
SPECIAL AGENT HANDBOOK



**SOCIAL SECURITY ADMINISTRATION
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS
Baltimore, Maryland 21235-6401**

October 2002

SPECIAL AGENT HANDBOOK



**SOCIAL SECURITY ADMINISTRATION
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS
Baltimore, Maryland 21235-6401**

This handbook contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This handbook is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

TABLE OF CONTENTS

Chapter 1 – Authority & Organization

001.000	Establishment of the Office of the Inspector General
001.010	Organizational Structure
001.020	Office of Investigations
001.030	<i>For Future Use</i>
001.040	Criminal Investigations Division
001.050	Policy and Administration Division
001.060	Forensic Intelligence and Analysis Division
001.070	<i>For Future Use</i>
001.080	Field Divisions
001.090	Nature of OI Investigations
001.100	Commonly Investigated Statutes
001.110	Oaths, Affirmations, & Law Enforcement Authority
001.120	Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority
001.130	Establishing Policy & Procedure
001.140	Certification of Review of the <i>Special Agent Handbook</i>
001.150	Liaison
001.160	Quality Assurance
001.170	National & Regional Fraud Alerts
001.175	Mutual Notification Agreement with the FBI
001.180	Mutual Assistance Agreement Authorizing Cooperation Among Offices of Inspectors General in the Execution of Search and Arrest Warrants

Chapter 1 – EXHIBITS

1-1	– Quality Standards for Investigations
1-2	– Attorney General Guidelines for OIGs with Statutory Law Enforcement Authority
1-3	– AIGI Policy Message
1-4	– Certification of Review of the <i>Special Agent Handbook</i>
1-5	– Sample Fraud Alert
1-6	– FBI Notification Letter
1-7	– Annual Certifications Checklist (Form OI-41)
1-8	– Annual Training Requirements (Form OI-41A)
1-9	– U.S. Government Interagency Agreement (Form 6-10 FMS 7600A) – Mutual Assistance Agreement

Chapter 2 – Responsibilities & Conduct

002.000	Standards of Ethical Conduct
002.010	Digest of Standards of Ethical Conduct
002.020	Supplemental Agency Regulations on Conduct

002.030	Conduct While on Official Duty
002.040	Outside Activities
002.050	Drug & Alcohol Use
002.060	Use of Official Vehicles
002.070	Surrender of Badge, Credential, & Firearm
002.080	Law Enforcement Availability Pay (LEAP)
002.090	Authority for LEAP
002.100	Eligibility for LEAP
002.110	Rules for LEAP
002.120	LEAP Reporting Requirements
002.130	Tracking Work Hours
002.140	Opting Out of Law Enforcement Availability Pay and Part-time Agent Program
002.150	Media Relations
002.160	Disclosure of Information
002.170	Congressional Inquiries

Chapter 2 – EXHIBITS

- 2-1 – [Certification for Home-to-Work Use of Official Government Vehicles \(OI-46\)](#)
 - 2-2 – [Availability Pay Certification \(OI-49\)](#)
 - 2-3 – [NICMS Time Module](#)
 - 2-4 – [Annual Certification of Availability Hours \(OI-50\)](#)
 - 2-5 – [Special Agent Part-time Employment Program](#)
-

Chapter 3 – Case Management

003.000	General
003.010	Policy
003.020	Receipt of Allegations from SSA
003.030	Divisional Responsibilities
003.040	Hotline & Field Division Responsibilities
003.045	SSA’s Fraud Information Tracking System (FITS)
003.050	Case Opening Procedures
003.060	Case Opening Priorities
003.070	Case Opening Guidelines
003.080	Case Numbering System
003.090	Guidelines for Administratively Closing Referrals of Potential Violations
003.100	Case Reviews
003.110	Case File Organization
003.120	Case File Table of Contents
003.130	Documenting Monetary Achievements
003.140	Documenting Arrests
003.150	Requests for Investigative Activities by Another Division (Collateral Investigations)
003.160	Reporting of Judgments & Court Ordered Restitution
003.170	Closing/Disposition of Investigative Files
003.180	Notification to SSA at the Conclusion of an Investigation
003.190	Monthly Verification of Statistics

003.200	Reopening of Previously Closed Cases
003.210	Quarterly Case Reviews by the Criminal Investigations Division
003.220	Special Interest Cases
003.230	Organizational Representative Payee Cases

Chapter 3 – EXHIBITS

3-1	– NICMS Case Opening Report (OI-1)
3-2	– Additional Subjects/Victims/Alias Data (OI-1A)
3-3	– Supervisory File Review Sheet (OI-20)
3-4	– Case File Arrangement and Closing Checklist (OI-31)
3-5	– NICMS Disposition Form (OI-9)
3-6	– Report of Court Ordered Restitution/Judgment (OI-68)
3-6A	– How to Use NICMs to Submit OI-68s
3-7	– Personal History Information Form (OI-19)
3-8	– Report of Investigation (OI-4)
3-9	– Report of Investigation – Disability (OI-4D)
3-10	– Report of Investigation – Cooperative Disability Investigations Program (OI-4C)
3-11	– FBI Laboratory Buccal Collection Kit Re-Order Form
3-12	– Methodology for Calculating Disability Program Savings in the CDI Program
3-13	– CJIS Fingerprinting Supply Requisition Form
3-14	– Request for Financial Forensic Assistance

Chapter 4 – Investigative Guidelines & Procedures

004.000	Types of Investigations
004.010	Program Fraud Investigations
004.020	Investigation of Representative Payees
004.030	Disability Investigations
004.040	Deceased Payee Investigations
004.050	Case Opening Guidelines for SSA Employee Investigations
004.055	Employee Case Notifications at Start of Investigation
004.060	Notifications for OIG Employee Allegations of Misconduct
004.065	Employee Case Notifications at Conclusion of the Investigation
004.070	Types of Employee Misconduct
004.075	Computer Assistance in Employee Investigations
004.080	Duty of Employee to Cooperate
004.085	Employee Misconduct with Prosecution Potential
004.090	Federal Employee Rights in Criminal Investigations
004.095	Federal Employee Rights in Non-Criminal Investigations
004.100	Waiver of Prosecution to Obtain Cooperation of Employee
004.105	Waiver of Disciplinary Action Against an Employee
004.110	Employee’s Right to Representation (Weingarten Rights)
004.120	Exculpatory and False Exculpatory Statements
004.130	Written Statements
004.140	Allegations of Misuse of Official Time by Union Officials
004.150	Updating the Status of Employee Cases in NICMS
004.160	Social Security Number (SSN) Misuse Investigations
004.170	Background Investigations

004.180	Reprisals Against SSA Employees
004.190	Investigation of Threats & Assaults Against SSA Employees
004.200	Protecting the Identity of Employee Allegers
004.210	Disclosure of Employee Identity
004.220	Pledges of Confidence
004.230	Avoidance of Informal Agreements
004.240	Confidential Informants
004.250	Confidential Sources
004.260	Searches of Government Property
004.270	Investigations in Foreign Countries
004.280	Audit Assistance in Criminal Investigations

Chapter 4 – EXHIBITS

4-1	– Federal Employee Advice of Rights (Form OI-15)
4-2	– Federal Employee Advice of Rights – Spanish (Form OI-15 S)
4-3	– Kalkines (Form OI-14)
4-4	– Kalkines – Spanish (Form OI-14 S)
4-5	– Report of Alleged SSA Employee Misconduct
4-6A	– Model Referral Letter to SSA – SSA Action Needed
4-6B	– Model Referral Letter to SSA – No SSA Action Needed
4-7	– Request for Information or Assistance (Form OI-56)
4-8	– Union Representative Advisory to SSA Employee (Form OI-80)
4-9	– Non-Criminal Background Investigation: Education
4-10	– Non-Criminal Background Investigation: Employment
4-11	– Non-Criminal Background Investigation: Neighborhood
4-12	– Confidential Informant Data (OI-27)
4-13	– Agreement to Provide Information (OI-27A)
4-14	– Confidential Informant Contact Record (OI-27B)
4-15	– Confidential Source Registration Card (OI-27C)
4-16	– Threat/Assault – Interview Worksheet
4-17	– Relevant Statutes
4-18	– AIMS, GAM 12.06
4-19	– Consent to Search Computers/Electronic Media
4-20	– Request for Audit and Financial Forensic Assistance memorandum
4-21	– Category 1 – Threat Notification Report (Form OI-95)

Chapter 5 – Investigative Project Management

005.000	Investigative Projects
005.010	Investigative Projects Originating in OI Headquarters
005.020	Request from Field Divisions to Establish Projects
005.030	Cooperative Disability Investigative Program
005.040	Fugitive Felon Program
005.050	SSN Misuse & Identity Theft
005.060	Deceased Auxiliary Beneficiary Project (BIC ‘D’) – National Operation Code “DA”
005.070	Residency Fraud
005.080	Homeland Security Projects

[005.085](#) Worksite Enforcement Operations
[005.090](#) Computer Research and Inquiries Team

Chapter 5 – EXHIBITS

- 5-0 – [Request for Approval to Establish Investigative Project](#)
 - 5-1 – [Guide to Third-Party Facilitator Investigations](#)
 - 5-2 – [Request for IAD IT Support](#)
 - 5-3 – [Request for Approval of Special Investigative Project](#)
-

Chapter 6 – Access to Social Security Information

[006.000](#) Introduction
[006.010](#) Disclosure of Records and Information by OIG Special Agents
[006.015](#) Disclosure of Tax Return Information
[006.020](#) Penalties for Unlawful Disclosure
[006.025](#) SSN Verification Policy
[006.030](#) Access Documentation
[006.040](#) Certifications
[006.050](#) Control of SSA’s Claim, Files, & Documents
[006.055](#) Payment Extracts
[006.060](#) Annotating “Special Message” Field of Benefit Records
[006.070](#) The Computer Matching and Privacy Protection Act
[006.080](#) Full Titles of Selected Acronyms
[006.090](#) Program Operations Manual Systems (POMS)
[006.100](#) Modernized System Operations Manual (MSOM)
[006.110](#) Query Master
[006.120](#) Initial Access to the SSA Mainframe
[006.130](#) Master File Query
[006.140](#) SS-5 Requests
[006.150](#) DECOR or EDCOR “No Match” Letters
[006.160](#) Policy for the Transportation of Personally Identifiable Information Outside of OIG Secure Space

Chapter 6 – EXHIBITS

- 6-0 – [Payment Extract Request Letter \(OI-85\)](#)
- 6-1 – [SSA Main Menu \(VTAM\)](#)
- 6-2 – [SSA Production \(Production\)](#)
- 6-3 – [SSA Menu \(Main\)](#)
- 6-4 – [Master File Query Menu \(MFQM\)](#)
- 6-5 – [Title II Menu \(T2SM\)](#)
- 6-6 – [Photocopy Request \(PEPH\)](#)
- 6-7 – [Detailed Office/Organization System \(DOORS\)](#)
- 6-8 – [Field Office Address & Phone Numbers \(FOADDRESS\)](#)
- 6-9 – [Representative Payee Main Menu \(RPMM\)](#)
- 6-10 – [RP Query Response Selection List \(RQSL\)](#)
- 6-11 – [CDR Selection Menu \(MCDR\)](#)

- 6-12 – [CDR Query Screen \(QCDR\)](#)
 - 6-13 – [Prison Systems/Fugitive Felons \(PFSM\)](#)
 - 6-14 – [Prison Systems Menu \(PSMU\)](#)
 - 6-15 – [Master File Query Menu \(MFQM\)](#)
 - 6-16 – [Abbreviated Account Query \(AACT\)](#)
 - 6-17 – [SSA Claims Control System Query \(SSACCS\)](#)
 - 6-18 – [Numident Query Sensitive Information \(NUMI\)](#)
 - 6-19 – [Numident \(NUMI\)](#)
 - 6-20 – [Alpha-Index Query \(ALPH\)](#)
 - 6-21 – [Data Exchange Query Menu \(DXQM\)](#)
 - 6-22 – [National Directory New Hire, Wage & Unemployment Menu \(NDNH\)](#)
 - 6-23 – [Systematic Alien Verification for Entitlement \(SAVE\)](#)
 - 6-24 – [Non-Immigrant Information & Alien Status Verification Display \(NIIS\)](#)
 - 6-25 – [Summary Earnings Query \(SEQY\)](#)
 - 6-26 – [Summary Earnings Report \(SEQR\)](#)
 - 6-27 – [Detail Earnings Query \(DEQY\)](#)
 - 6-28 – [Detail Earnings Report \(DEQR\)](#)
 - 6-29 – [Supplemental Security Income Queries \(SSQM\)](#)
 - 6-30 – [SSI Complete Record \(SSID\)](#)
 - 6-31 – [Payment History Update System Queries \(PHUS\)](#)
 - 6-32 – [Payment History by BIC \(PHU1\)](#)
 - 6-33 – [Miscellaneous Menu \(MISM\)](#)
 - 6-34 – [Routing Transit Number \(RTND\)](#)
 - 6-35 – [Final Financial Institution Listing \(RTN1\)](#)
 - 6-36 – [EIF Access by Name \(AEQY\)](#)
 - 6-36A – [EIF Access by EIN \(AEQY\)](#)
 - 6-37 – [EIF Response to Query \(AEQY\)](#)
 - 6-38 – [Consolidated Query \(CNOY\)](#)
 - 6-39 – [RP QUERY Response Selection List \(RQSL\)](#)
 - 6-40A – [Standard Query \(SQRY\)](#)
 - 6-40B – [Standard Query & Reply \(SQRY\)](#)
 - 6-41 – [Folder Query \(FOY1\)](#)
 - 6-42 – [Response Letter for SSN Queries](#)
 - 6-43 – [Annual Systems Security Certification and Acknowledgement](#)
 - 6-44 – [SSA Consent for Release of Information](#)
 - 6-45 – [Transportation of Personally Identifiable Information Outside of OIG Secure Space](#)
-

Chapter 7 – Investigative Operations & Support

- [007.000](#) Investigative Operations
- [007.010](#) Policy
- [007.020](#) Initiating Undercover Operations
- [007.030](#) Approval of Undercover Operations
- [007.040](#) Use of SSA Employees in Field or Undercover Operations
- [007.050](#) Monitoring Field or Undercover Operations
- [007.060](#) Reporting the Results of Undercover Operations
- [\(b\) \(7\)\(E\)](#) [REDACTED]
- [007.080](#) Mail Covers

007.090	Witness Identification of Subjects
007.100	Polygraph
007.110	Electronic Sources of Information
007.120	Electronic Device Forensic Examinations
007.130	Other Forensic Examination
007.140	Technical Investigative Equipment & Support
007.150	Radio Communications

Chapter 7 – EXHIBITS

7-1	– Tactical Plan: Surveillance, Undercover, Arrest (OI-17)
7-2	– Tactical Plan for Search Warrants
7-3	– Consent to Monitor Non-Telephone Conversations (OI-25AL)
7-4	– Action Memorandum (OI-42)
7-5	– Consent to Monitor Telephone Conversations (OI-25AL)
7-6	– Agreement Between SSA OIG & SSA Special Project Staff (OI-55)
7-6A	– USPS Procedures – Mail Cover Requests
7-6B	– Mail Cover Transmittal Letter (OI-71)
7-6C	– Request for Mail Cover (official USPS version)
7-7	– Photo Lineup Guidelines
7-8	– OI Standard Operating Procedures for Psychophysiological Detection of Deception
7-9	– OI Polygraph Examination Request Worksheet
7-10	– Request for NCIC/NLETS Records Check
7-11	– FinCEN Request for Information
7-12	– Guidelines for Suspected Child Pornography on Agency Networks
7-13	– Handwriting Sample (OI-29A)
7-14	– Handwriting Specimen (OI-29B)
7-15	– Radio Network User Registration Form
(b) (7)(E)	
[REDACTED]	
[REDACTED]	
7-18	– NCIC Data for USMS
7-19	– Policy for Law Enforcement Information Systems and Commercial Database Access and Law Enforcement Systems and Commercial Database Security Acknowledgement
7-20	– National Crime Information Center Information
7-21	– Non-SSA Internet Access Log
7-22	– Mobile Device Inventory Worksheet (Form OI-94)

Chapter 8 – Interception of Communications

008.000	Nonconsensual Monitoring
008.010	Accounting for Interception Devices
008.020	Electronic Tracking Devices
008.030	Dialed Number Recorded
008.040	Interception of Wire or Oral Communications
008.050	Consensual Telephone Monitoring
008.060	Request for Approval of Consensual Telephone Monitoring
008.070	Consensual Non-Telephone Monitoring

Chapter 8 – EXHIBITS

- 8-1 – [Report of Intercept \(OI-24A\)](#)
 - 8-2 – [Consent to Monitor Telephone Conversations \(OI-25L\)](#)
 - 8-3 – [Sample Request Memorandum \(OI-24\)](#)
 - 8-4 – [Consent to Monitor Non-Telephone Conversations \(OI-25L\)](#)
-

Chapter 9 – Confidential Expenditures

009.000	Purpose
009.010	Obtaining Confidential Funds
009.020	Disposition of Excess ATM Withdrawals
009.030	Confidential Expenditures
009.040	Expenditures for Confidential Informants
009.050	Approving Amounts by Officials
009.060	Funds Administration
009.070	Accountability Report
009.080	Periodic Unannounced Audits of Unexpended Confidential Fund Balances

Chapter 9 – EXHIBITS

- 9-1 – [Transaction Record of Each Advance of Return of Confidential Funds \(OI-28A\)](#)
 - 9-2 – [OIG Transmittal Register](#)
 - 9-3 – [Receipt for Payment to Informant \(OI-28B\)](#)
 - 9-4 – [Custodian's Activity Log for Confidential Funds \(OI-28\)](#)
 - 9-5 – [Accountability Report \(OI-28C\)](#)
-

Chapter 10 – Interviews, Investigative Notes, & Statements

010.000	Policy Directive
010.010	Purpose of Interviews
010.020	General Instructions
010.030	Definitions
010.040	Procedures
010.050	Advice of Rights
010.060	Conducting the Interview
010.070	Obtaining Descriptive Factors
010.080	Investigative Notes
010.090	Statements
010.100	Oath or Affirmation
010.110	Jurat
010.120	Special Situations

Chapter 10 – EXHIBITS

- 10-1 – [Personal History Form \(OI-19\)](#)
- 10-2 – [Report of Investigations \(OI-4\)](#)
- 10-3 – [Advice of Rights \(OI-13\)](#)
- 10-4 – [Advice of Rights – Non Custodial \(OI-13 NC\)](#)
- 10-5 – [Advice of Rights – Spanish \(OI-13 S\)](#)
- 10-6 – [Witness Statement \(OI-16A\) *](#)
- 10-7 – [Non-Custodial Advice of Rights Statements \(OI-16B\) *](#)
- 10-8 – [Full Miranda Statement \(OI-16C\) *](#)
- 10-9 – [Statement Continuation \(OI-16D\) *](#)
- 10-10 – [Statement Signature Page \(OI-16E\) *](#)

* OI-16 A-E forms are available in Spanish in Sharepoint.

Chapter 11 – Investigative Reports

- [011.000](#) General
- [011.010](#) Quality Standards
- [011.020](#) Policy
- [011.030](#) Investigative Reports
- [011.035](#) Submission of Reports/Documents
- [011.040](#) SSA Office of the Inspector General Facts Sheets
- [011.050](#) Reports of Employee Misconduct to Headquarter
- [011.060](#) Annual Report to the Attorney General

Chapter 11 – EXHIBITS

- 11-1 – [NICMS Case Opening Report \(OI-1\)](#)
- 11-2 – [Investigative Plan \(OI-2\)](#)
- 11-3 – [Report of Investigation \(OI-4\)](#)
- 11-3A – [Report of Investigation \(OI-4D\)](#)
- 11-3B – [Report of Investigation – Cooperative Disability Investigations Unit \(OI-4C CDI\)](#)
- 11-4 – [Prosecution Report \(OI-6\)](#)
- 11-4A – [Prosecution Report \(OI-6A\)](#)
- 11-5 – [Memorandum of Transmission \(OI-7\)](#)
- 11-6 – [Specialized Report of Investigation \(OI-5A\)](#)
- 11-7 – [NICMS Criminal & Administrative Disposition Form \(OI-9\)](#)
- 11-8 – [Investigative Checklist \(OI-34\)](#)
- 11-9 – [SSA OIG Fact Sheet \(OI-12L\)](#)
- 11-10 – [DAIGI Memorandum for Employee Misconduct Cases Involving OI SAs](#)

Chapter 12 – Inspector General Subpoenas

- [012.000](#) Authority
- [012.010](#) Subpoena Requests
- [012.020](#) Subpoena Service

012.030	Noncompliance
012.040	Subpoena Register

Chapter 12 – EXHIBITS

12-1	– OIG Subpoena
12-2	– IG Subpoena Transmittal Letter
12-2a	– IG Subpoena Transmittal Letter - Regular
12-2b	– IG Subpoena Transmittal Letter - Account Names Only
12-2c	– IG Subpoena Transmittal Letter - Right to Financial Privacy Act
12-2d	– IG Subpoena Transmittal Letter - Right to Financial Privacy Act (Deceased Sole Account Holder)
12-2e	– IG Subpoena Transmittal Letter - Right to Financial Privacy Act (Minor Son or Daughter Account Holder)
12-3	– Pre-approved Subpoena Language

Chapter 13 – Search & Seizure

013.000	Purpose
013.010	Policy
013.020	Protection Afforded by the U.S. Constitution
013.030	Search Warrants-General
013.040	Tactical Plan
013.050	Mandatory Briefing
013.060	Video Documentation
013.070	Execution of Search Warrants
013.080	Warrantless Searches
013.090	Abandoned Property
013.100	Vehicle Searches
013.110	Searches of Government Property

Chapter 13 – EXHIBITS

13-1	– Preparatory Checklist for Search Warrant Affidavit (OI-35)
13-2	– Search Warrant Supplies Inventory/Raid Kit (OI-36)
13-3	– Tactical Plan for Search Warrant (OI-18)
13-4	– Inventory Form (OI-23)
13-5	– Inventory Form (Attachment) (OI-23A)
13-6	– Consent to Search-Computer Generated (OI-26)
13-7	– Consent to Search-Handwritten (OI-26L)

Chapter 14 – Acquisition, Preservation, & Management of Evidence

014.000	General
-------------------------	---------

014.010	Federal Rules of Evidence
014.020	Admissibility, Relevancy & Competency of Evidence
014.030	Burden of Proof
014.040	Best Evidence Rule
014.050	Computer-Based Evidence
014.060	Evidence Management Procedures
014.070	Grand Jury Information

Chapter 14 – EXHIBITS

14-1	– Evidence/Property Report (OI-21)
14-2	– Description of Property Acquired (OI-21A)
14-3	– Chain of Custody (OI-21B)
14-4	– Inventory Form (OI-23)
14-5	– Inventory Form (Attachment) (OI-23A)

Chapter 15 – Criminal Procedure

015.000	General
015.010	Entrapment
015.020	Arrest Warrants-General
015.030	Indictment & Information
015.040	Arrest Warrants-Execution
015.050	Obtaining a Summons
015.060	Arrest Without a Warrant
015.070	Initial Appearance
015.080	Preliminary Hearing
015.090	The Arraignment
015.100	Transfer from the District for Plea & Sentencing (Rules of Criminal Procedure – Rule 20)
015.110	Removals (Rules of Criminal Procedure – Rule 40)
015.120	Declinations of Prosecution
015.130	Pretrial Diversion
015.140	Giglio Policy (Policy Regarding the Disclosure to Federal Prosecutors of Potential Impeachment Information Concerning SSA Office of the Inspector General Employees Who are Affiants and/or Witnesses in Federal Criminal Cases)

Chapter 15 – EXHIBITS

15-1	– Criminal Complaint
15-2	– Arrest Warrant
15-3	– Declination of Prosecution (OI-77)

Chapter 16 – Civil Monetary Penalties & Administrative Sanctions

016.000	Section 1129 – False Statements & Representation
016.010	Procedural Requirements Under Section 1129
016.020	Hearings & Appeals
016.030	Collectability
016.040	Injunctions & Testimonial Subpoenas
016.050	Civil Monetary Penalty Investigative Referrals
016.060	Civil Monetary Penalty Reports of Investigation
016.070	Post-Referral Activities
016.080	Collections
016.090	Section 1129A – Title XI of the Social Security Act
016.100	OIG Actions After Receipt of Potential Sanction Referrals
016.110	NICMS Entries for Administrative Sanctions Referrals
016.120	Section 1140 – Misuse of SSA Program Works, Emblems, and Symbols

Chapter 16 – EXHIBITS

16-1 – [Civil Monetary Penalty Authorities under Section 1129](#)

Chapter 17 – Victim & Witness Assistance Program

017.000	General
017.010	Authority
017.020	Policy
017.030	Definitions
017.040	Responsibilities
017.050	Implementation with Respect to Confidential Informants
017.060	Victim & Witness Awareness Training

Chapter 17 – EXHIBIT

17-1 – [Information for Victims & Witnesses of Crime](#)

Chapter 18 – General Legal Matters

018.000	The Right to Financial Privacy Act of 1978
018.010	Exclusions & Limitations
018.020	Access to Records
018.030	Exceptions
018.040	Delayed Notification
018.050	Transfer of Records
018.060	Policy Regarding Notice to Executor or Administrator of Estate When Requesting Records of a Deceased Beneficiary
018.070	<i>Touhy</i> Regulations
018.080	Federal Tort Claims Act
018.090	Liability of Federal Officers

018.100	Duty of Care While in Official Custody
018.110	Motor Vehicles
018.120	Representation
018.130	Legal Considerations Regarding the Use of Text Messaging

Chapter 18 – EXHIBITS

18-1	– Certificate of Compliance with the Right to Financial Privacy Act of 1978 (OI-57)
18-2	– Statement of Customer Rights Under Right to Financial Privacy Act of 1978 (OI-58)
18-3	– Customer Consent & Authorization for Access to Financial Records (OI-59)
18-4	– Customer Notice (OI-60)
18-5	– Transmittal Letter (Right to Financial Privacy Act) to Financial Institution
18-6	– Transmittal Letter to Customer
18-7	– Instructions for Completing & Filing the Enclosed Motion & Sworn Statement (OI-61A)
18-8	– Motion for Order Pursuant to Customer Challenge Provisions of the Right to Financial Privacy Act of 1978 (OI-61)
18-9	– Sworn Statement of Movant
18-10	– Transfer of Records to Another Agency or Department
18-11	– Notice to Customer for Transfer of Records
18-12	– Transmittal Letter to Financial Institution (Account Information Only Under Right to Financial Privacy Act)

Chapter 19 – Freedom of Information & The Privacy Act

019.000	The Freedom of Information Act
019.010	Policy Statement
019.020	Methodology
019.030	Information Protected from Disclosure
019.040	Contact with Persons Seeking Records Under the Freedom of Information Act
019.050	The Privacy Act of 1974
019.060	Privacy Act Requests
019.070	Privacy Act Violations

Chapter 20 – Training Policy

020.000	General Policy
020.010	Responsibilities
020.020	Payment
020.030	Training Database
020.040	On-the-Job Training & the Mentoring Program
020.050	Individual Development Plan
020.060	Field Division In-Service Training

Chapter 20 – EXHIBITS

- 20-1 – [Training Nomination & Authorization \(HHS-350\)](#)
 - 20-2 – [On-the-Job Training Guide](#)
 - 20-3 – [Individual Development Plan](#)
 - 20-4 – [Statement of Experience and Training](#)
-

Chapter 21 – Firearms Policy and Training

- [021.000](#) Authority to Carry Firearms
- [021.010](#) General Conduct
- [021.020](#) Carrying Issued Weapons
- [021.025](#) Carrying of Back-up Weapons
- [021.030](#) Use of Shotguns
- [021.040](#) Firearms Inventory Control & Safekeeping
- [021.050](#) Types of Firearms & Ammunition
- [021.060](#) Basic Firearms Training
- [021.070](#) Firearms Instructors
- [021.080](#) Firearms Qualification Standards
- [021.090](#) Weapons Issuance & Security
- [021.100](#) Permits to Carry Firearms
- [021.110](#) Report of Shooting Incident

Chapter 21 – EXHIBITS

- 21-1 – [Shotgun Sign-out Log](#)
-

Chapter 22 – Occupational Health & Wellness

- [022.000](#) General Policy
- [022.010](#) Physical Requirements & Medical Standards
- [022.020](#) Pre-Employment Physical Examinations
- [022.030](#) Informing Applicants of the Mandatory Physical Examination Program
- [022.040](#) Scheduling Pre-Employment Physicals
- [022.050](#) Review by Public Health Service Medical Officer
- [022.060](#) Mandatory Periodic Physical Examinations
- [022.070](#) Scheduling of Periodic Physical Examinations
- [022.080](#) Reporting the Results of Periodic Physical Examinations
- [022.090](#) Exposure Control Plan
- [022.100](#) Office of the Inspector General Health Enhancement Program
- [022.110](#) Physical Conditioning Under the Office of the Inspector General Health Enhancement Program
- [022.120](#) Requesting Approval for Workday Conditioning Activities
- [022.130](#) Administration of the Fitness Assessment

Chapter 22 – EXHIBITS

- 22-1 – [Physical Requirements for SSA OIG Criminal Investigators](#)

22-2 – [SSA OIG Fitness Evaluation Report](#)

22-3 – [SSA OIG Fitness Norms](#)

Chapter 23 - Administrative Support Functions

023.000	General
023.010	Property Management
023.020	Administrative Filing System
023.030	Files to be Considered for Establishing Each Fiscal Year
023.040	Records Disposition Schedules
023.050	Personnel Management Information and Procedures Guidance
023.060	Employee Transfers and Relocations
023.070	Government Vehicle Fleet Management

Chapter 23 – EXHIBITS

23-1 – [Personal Custody Property Record/Hand Receipt \(OI-52\)](#)

Chapter 24 - Use-of-Force

024.000	Consideration for Use of Force
024.010	Liability
024.020	Basic Use-of-Force Training
024.030	Use-of-Force Instructors
024.040	Reporting Use of Force Incidents (Shooting Incidents)
024.050	Incidents Involving Less-Than-Lethal Force
024.060	Post-Incident Procedures
024.070	Administrative Inquiry
024.080	Emergency, Interim Legal Representation of Federal Law Enforcement Officials involved in “Critical Incidents”

Revised 10/17/07
Revised 12/17/09
Revised 9/29/10
Revised 1/25/11
Last update 6/21/11
Revised 8/17/11
Revised 9/7/11
Revised 9/13/11
Revised 9/22/11
Revised 10/19/11
Revised 1/22/13
Revised 4/24/13

AUTHORITY AND ORGANIZATION

Office of the Inspector General Mission Statement

By conducting independent and objective audits, evaluations, and investigations, we improve the Social Security Administration (SSA) programs and operations and protect them against fraud, waste, and abuse. We provide timely, useful, and reliable information and advice to Administration officials, Congress, and the public.

Vision and Values

We are agents of positive change striving for continuous improvement in SSA's programs, operations, and management by proactively seeking new ways to prevent and deter fraud, waste, and abuse. We are committed to integrity and to achieving excellence by supporting an environment that encourages employee development and retention, and fosters diversity and innovation, while providing a valuable public service.

001.000 Establishment of the Office of the Inspector General

- A.** The Social Security Administration (SSA) Office of the Inspector General (OIG) was established on April 1, 1995, pursuant to Public Law 103-296, known as the *Social Security Independence and Program Improvements Act of 1994*. General OIG authority is established under the Inspector General Act of 1978, as amended.
- B.** OIG has a statutory responsibility to protect the integrity of SSA's programs and operations affecting millions of beneficiaries; and to ensure that the programs are administered with maximum economy and efficiency.
- C.** OIG is also responsible for conducting reviews of SSA's management activities, and monitoring SSA's programs to ensure that effective internal controls are in place.
- D.** In addition, OIG participates in coordinating Government-wide activities to reduce fraud, waste, and abuse; and to improve management process.

001.010 Organizational Structure

- A.** SSA OIG is headed by an Inspector General (IG), appointed by the President with the advice and consent of the United States Senate. By statute, the IG oversees and is responsible for:
1. auditing and investigating matters affecting SSA's programs and operations;
 2. reviewing proposed and existing laws and regulations bearing upon the SSA;
 3. establishing and implementing policies to promote economy and efficiency and to prevent fraud, waste, and abuse; and
 4. appointing an Assistant Inspector General for Investigations (AIGI) and an Assistant Inspector General for Audit.
- B.** The AIGI supervises the performance of investigative activities and inquiries relating to SSA's programs and operations. Two Deputy Assistant Inspectors General for Investigations advise and assist the AIGI on all SSA OIG investigations and inquiries.
- C.** In addition to the Office of Investigations (OI), the OIG has three other major components: Office of Audit (OA), Office of Counsel to the Inspector General (OCIG), and the Office of Communications and Resource Management (OCRM).
1. OA conducts comprehensive financial and performance audits of SSA's programs and operations; and makes recommendations to ensure that program objectives are achieved effectively and efficiently.
 2. OCIG provides legal advice and counsel to the IG and senior staff on various matters, including
 - a. statutes, regulations, and legislative and policy directives governing the administration of the SSA's programs;
 - b. investigative procedures and techniques; and
 - c. legal implications and conclusions to be drawn from audit and investigative material.

Section 4(a) of the Inspector General Act of 1978, as amended, requires the IG to review existing and proposed legislation and regulations, and to make recommendations concerning the possible effects on the economy and efficiency of the administration of the Agency's programs.

OCIG is responsible for the implementation of the Civil Monetary Penalty (CMP) program. OCIG also manages OIG public and media relations, and congressional liaison.

3. OCRM provides administrative and management support and coordinates resource management needs for OIG components by providing budgetary, administrative, facilities and equipment, human resources, and information management. In addition to these functions, OCRM oversees the Allegation Management and Fugitive Enforcement Division (AMFED).

001.020 Office of Investigations

- A.** OI protects the integrity of SSA’s programs by investigating allegations of fraud, waste, and abuse. These include investigations of grant and contract fraud by unscrupulous individuals, as well as violations by SSA’s employees and those who attempt to secure benefits illegally.
- B.** Investigations conducted by OI can result in criminal or civil prosecutions and CMPs against wrongdoers, and can act as a deterrent against those contemplating fraud against SSA and its beneficiaries.
- C.** OI also proposes systemic changes for remedying program flaws detected during investigations to prevent future fraudulent activities. Special fraud alerts are issued to warn SSA and others of illegal schemes that deplete the Social Security trust funds or victimize beneficiaries.
- D.** OI Headquarters (HQ) consists of three divisions, and each is headed by a Special Agent-in-Charge (SAC) or Director. These divisions are: Criminal Investigations Division (CID), Policy and Administration Division (PAD), and Intelligence and Analysis Division (IAD).

001.030 For Future Use

001.040 Criminal Investigations Division (CID)

- A.** CID is located at SSA OIG/OI HQ and reports to the AIGI through the DAIGI. CID is comprised of four Assistants to the Special Agents-in-Charge (ATSACs) who are under the supervision of a SAC.
- B.** CID manages the day-to-day coordination of the investigative and administrative information flow between OI HQ and the field divisions (FD).
- C.** The division is comprised of five teams:
 - 1.** Investigative Operations Team
 - 2.** Controls and Liaison Team
 - 3.** Investigative Management Information Team
 - 4.** Cooperative Disability Investigations
 - 5.** Digital Forensics Team
- D.** CID’s responsibilities include:
 - 1.** Serving as the conduit for HQ oversight and operational field support to the FDs, to include:
 - a.** Management and tracking of national investigations.

- b. Management and tracking of national incidents or “high-profile” investigations.
2. HQ reporting and tracking of threat investigations involving threats or assaults made against SSA employees or facilities.
3. Management of the SSA employee integrity and employee fraud program, which includes monitoring and reporting of all SSA employee fraud or misconduct investigations.
4. Processing all requests for undercover operations and/or consensual electronic monitoring operations, as well as administering oversight for FDs’ reporting of confidential funds expenditures.
5. Overseeing the OIG HQ function for the National CDI Program.
6. Preparing recurring (Quarterly and Semi-annual) and “ad hoc” management information reports for OI senior executives and management staff, to include managing OI’s quarterly case file review process.
7. Ensuring the functionality of the OIG’s National Investigative Case Management System (NICMS), to include validating the accuracy and utility of system information, as well as the development and handling of NICMS statistical information reports.

001.050 Policy and Administration Division (PAD)

- A. PAD is located at SSA OIG/OI HQ and reports to the AIGI through the DAIGI. PAD is responsible for budget, staffing plans, training, procurement, personnel issues, and general administrative matters.
- B. The division is responsible for identifying and procuring special technical investigative equipment for use by OI personnel.
- C. The division is responsible for coordination with the Federal Law Enforcement Training Center and the Inspector General Criminal Investigator Academy.
- D. PAD heads OI’s effort to ensure that the OIG, in conjunction with SSA, is prepared to continue operations in the event of natural disasters, terrorist activities, or other disruptive events.

001.060 Intelligence and Analysis Division (IAD)

- A. IAD is located at SSA OIG/OI HQ and reports to the AIGI through the DAIGI. This division is composed of teams of Investigations Analysts, Forensic Specialists, Information Technology (IT) Specialists, and Special Agents under the supervision of a SAC/Director. IAD is composed of two teams:
 1. Analytics Team
 2. Field Support Team (FST)

- B.** IAD's primary responsibility is to identify and target for investigation SSA's programs and operations that are potentially vulnerable to widespread fraud and abuse. Its success is dependent on numerous sources of information and support from SSA and other OIG components. The approach IAD will use to accomplish its mission includes:
1. analysis of individual fraud cases, hotline allegations, audit reports, and reports on regional fraud committee initiatives;
 2. proactive use of computer searches and matches to identify repetitious fraudulent transactions on SSA systems perpetrated by employees or the public;
 3. intelligence developed from cooperative efforts with other law enforcement agencies; and
 4. forensic tools.
- C.** IAD serves as the IG's fraud and abuse intelligence-gathering component. To successfully accomplish this, IAD shall:
1. effect liaison with other SSA components to keep abreast of their concerns regarding fraud;
 2. coordinate with other Federal, State, and local law enforcement agencies to identify areas of mutual concern;
 3. coordinate with SACs to establish interagency and intra-agency task forces; and
 4. prepare Management Implication Reports (MIR) on vulnerabilities in SSA's programs or operations.
- D.** The IAD SAC/Director serves as OI's primary liaison to OIG/OA. When a field division (FD) has identified an administrative control or operational deficiency that may need audit attention, the FD SAC should forward the identified issue via memorandum to the IAD SAC/Director. IAD reviews, approves, and submits suspected administrative control or operational deficiencies identified by field personnel to OA for inclusion in the Audit Work Plan. This activity should not be confused with requesting audit assistance with an open investigation (see Section 004.280).
- E.** IAD also serves as OI's coordinator of national special projects, and assists field offices with the development of local projects. Proposals for investigative projects or operations with national implications should be submitted for review via memorandum from the FD SAC to the IAD SAC/Director.

001.070 **For Future Use**

001.080 **Field Divisions**

- A.** OI also consists of FDs with subordinate offices located throughout the United States. Each FD is headed by a SAC, who reports directly to the DAIGI.

- B.** Assistant Special Agents-in-Charge (ASACs) and Resident Agents-in-Charge (RACs) assist in the supervision of the FD. Some offices have an ASAC or RAC on-site. Other offices receive supervision from off-site ASACs or RACs.
- C.** FD personnel are expected to communicate with HQ components through their chain of command. Special Agents may contact CID desk officers directly when situations require immediate attention.
- D.** Resident Agents (RA) are the senior, non-supervisory special agents in offices without an on-site RAC. The RA is responsible for activities such as property management, evidence control, case assignment, file management, and leave reporting. The RA reports to either an ASAC or RAC within the FD.
- E.** The FDs are responsible for conducting investigations in assigned geographical areas. Currently, the FDs and the States and territories they cover are:

Atlanta FD: Alabama, Florida, Georgia, Kentucky, Mississippi, North Carolina, South Carolina, and Tennessee

Boston FD: Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont

Chicago FD: Illinois, Indiana, Michigan, Minnesota, Ohio, and Wisconsin

Dallas FD: Arkansas, Louisiana, New Mexico, Oklahoma, and Texas

Denver FD: Colorado, Montana, North Dakota, South Dakota, Utah, and Wyoming

San Francisco FD: Arizona, California, Hawaii, Nevada, American Samoa, Guam, and the Northern Mariana Islands

New York FD: New Jersey, New York, Puerto Rico, and the Virgin Islands

Philadelphia FD: Delaware, Maryland, Pennsylvania, Virginia, West Virginia, and the District of Columbia

Seattle FD: Alaska, Idaho, Oregon, and Washington

Kansas City FD: Iowa, Kansas, Missouri, and Nebraska

001.090 Nature of OI Investigations

- A.** OIG/OI policy is to concentrate its resources on conducting criminal investigations relating to the programs and operations of SSA. These investigations include the following:
 - 1.** allegations of employee misconduct/criminal activity;
 - 2.** allegations brought forward by employees;

3. program fraud cases (Title II – Federal Old-Age, Survivors, and Disability Insurance; and Title XVI – Supplemental Security Income for the Aged, Blind, and Disabled);
 4. enumeration cases (enumeration is the process of establishing legitimate Social Security numbers (SSN) and maintaining records established thereunder); and
 5. SSN cases. In number cases, someone misuses an SSN to perpetrate fraud outside of the SSA programs by using bogus SSNs for bank loans, credit applications, identity documents, etc. Many of these cases are worked jointly with other law enforcement agencies.
- B. OI will also perform other investigations and functions necessary to carry out the OIG mission.
- C. OI investigations will be conducted in accordance with the *Quality Standards for Investigations* issued by the Council of Inspectors General on Integrity and Efficiency (CIGIE) ([see Exhibit 1-1](#)).

001.100 Commonly Investigated Statutes

- A. The following are statutes commonly investigated by OI alone or jointly with other agencies.
- 18 U.S.C. § 2 Aiding and Abetting
 - 18 U.S.C. § 201 Bribery of a Public Official
 - 18 U.S.C. § 208 Conflict of Interest
 - 18 U.S.C. § 287 Fraudulent Claims
 - 18 U.S.C. § 371 Conspiring to Defraud the United States
 - 18 U.S.C. § 510 Forgery
 - 18 U.S.C. § 641 Embezzlement and Theft of Government Property
 - 18 U.S.C. § 1001 False Statements or Entries
 - 18 U.S.C. § 1028 Fraud in Connection with Identification Documents
 - 18 U.S.C. § 1029 Fraud in Connection with Access Devices
 - 18 U.S.C. § 1030 Computer Fraud
 - 18 U.S.C. § 1341 Mail Fraud
 - 18 U.S.C. § 1343 Wire Fraud
 - 18 U.S.C. § 1344 Bank Fraud
 - 42 U.S.C. § 408 Social Security Fraud
 - 42 U.S.C. § 1383a Supplemental Social Security Income Fraud
- B. The list is representative and not intended to be all-inclusive. Employees should consult current legal publications for cites, annotations, case law, and other relevant statutes for additional information. Questions should be directed to the OCIG at HQ, through the employee’s SAC and Regional ASAC.

001.110 Oaths, Affirmations, and Law Enforcement Authority

OI SAs have the authority to administer oaths and affirmations in connection with an investigation (*see Chapter 10*). Other law enforcement authority is delegated by the Attorney General through Guidelines adopted in accordance with the Homeland Security Act of 2002. The complete Attorney General Guidelines are included as [Exhibit 1-2](#) at the end of this chapter.

- A. Explicit authority to administer oaths and affirmations is given in 5 U.S.C. Appendix 3, Section 6 (a)(5).
- B. General authority to administer oaths and affirmations is given in 5 U.S.C. § 303.
- C. The Homeland Security Act of 2002 provides in part that the Attorney General may grant certain law enforcement authority to the various federal Offices of Inspectors General (OIG), including SSA OIG. The authority applies to those offices of Presidentially appointed Inspectors General with law enforcement powers received from the Attorney General under section 6(e) of the Inspector General Act of 1978 (IG Act), as amended. In accordance with the provisions of the Act, the Attorney General has authorized the SSA OIG Inspector General, the Assistant Inspector General for Investigations, and any Special Agent supervised by the Assistant Inspector General of that OIG to:
 - 1. carry a firearm while engaged in official duties as authorized under the Act or other statute, or as expressly authorized by the Attorney General;
 - 2. make an arrest without a warrant while engaged in official duties as authorized under the Act or other statute, or as expressly authorized by the Attorney General, for any offense against the United States committed in the presence of such individual, or for any felony cognizable under the laws of the United States if such individual has reasonable grounds to believe that the person to be arrested has committed or is committing such felony; and
 - 3. upon probable cause to believe that a violation has been committed, seek and execute warrants for arrest, search of a premises, or seizure of evidence issued under the authority of the United States.
- D. Individuals exercising law enforcement authorities under section 6(e) may exercise those powers only for activities authorized under the IG Act, or other statute, or as expressly authorized by the Attorney General. Section 6(e) does not, of itself, provide plenary authority to make arrests for non-Federal criminal violations. Legal authority for officers to respond to such offenses generally depends on state law. A Federal agency may, however, as a matter of policy, permit its officers to intervene in serious criminal conduct that violates State law, or in emergency situations under certain circumstances. The SSA OIG has adopted such a policy (*see Chapter 21*).

001.120 Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority

- A. The Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority cover a wide array of activities that an OIG must undertake. If the Attorney General determines that an Office of Inspector General exercising law enforcement powers under section 6(e), or any individual exercising such powers, has failed to comply with these Guidelines, the Attorney General may rescind or suspend exercise of law enforcement authorities for that office or individual.
- B. The Guidelines include the following:

1. Law Enforcement Training and Qualifications (Basic and Refresher Training, Firearms Training and Qualification Requirements, Deadly Force Policy)
2. Range of Law Enforcement Powers (to carry firearms, make arrests, seek and execute warrants, etc.)
3. Adherence to Attorney General Guidelines (General Crimes, Racketeering Enterprise, Terrorism Enterprise, Use of Confidential Informants, Monitoring of Verbal Communications, and any other Attorney General Guidelines applicable to criminal investigative practices)
4. Notification and Consultation Requirements with Respect to Allegations of Criminal Violations (Mutual Notification Requirements, Consultation with Prosecutors)
5. Use of Specialized Investigative Procedures and Techniques (Court-Ordered Electronic Surveillance, Undercover Investigative Operations, Especially Sensitive Targets, Consensual Monitoring in Certain Situations)
6. Prosecutor Concurrence for Certain Techniques (participation in criminal activities, legal privilege of confidentiality, payments to a source in excess of \$25,000, use of a member of the news media)
7. Relations with the News Media (28 C.F.R. § 50.2)
8. Reporting Requirements (number of federal investigations initiated, undercover operations undertaken, times electronic surveillance used, and significant and credible allegations of abuse of authorities conferred by 6(e)(1) of the IG Act)
9. Peer Reviews (to ascertain whether adequate internal safeguards and management procedures exist to ensure that the law enforcement powers conferred by the 2002 amendments to the IG Act are properly exercised)
10. No Third-Party Rights Created

001.130 Establishing Policy and Procedure

- A. Official OIG OI policy and procedural instructions, including the instructions in this *Handbook*, may be issued only under the authority of:
 1. the IG or his/her designee; or
 2. the AIGI or his/her designee.
- B. Policy is issued via three methods:
 1. Written revisions to the *Special Agent Handbook* (SAH) – changes made are transmitted to all holders of the SAH.

2. AIGI Memorandum – this form is used when it is necessary to send supportive or informational documents to provide background on the policy.
 3. AIGI Policy Messages – policy implemented in this form is through the use of electronic mail messages (see [Exhibit 1-3](#)).
- C. The SAH is available electronically on the OIG SharePoint site. The electronic SAH will be updated any time a policy change is announced.
- D. Limits on authority to issue OI policy and procedural instructions are necessary to assure consistency. They do not apply to purely informational issuances and are not meant to impede routine communications.

001.140 Certification of Review of Selected Documents and Policies

- A. An employee’s knowledge of OI policies and procedures is essential to maintaining an efficient organization. Accordingly, each OI employee is required to annually review and certify that he/she is familiar with the contents of selected administrative policies and other documents. Additionally, SAs are required to complete specific training activities in order to remain knowledgeable and possess current skills or proficiencies. The [annual certification documents](#) attesting to the employee’s compliance will be filed in either the employee’s SF-7B extension file or in a binder containing the records of certification.
- B. Documents to be placed in the employee’s SF-7B extension file (two or six part folders) include:
- Left Side of File (Top to Bottom Order)
 1. Documents such as those relating to awards, approved suggestions, leave restrictions, letters of commendation as well as an employee’s written comments concerning records contained in the file are also placed in the SSA 7B Employee Record Extension File.
 2. Individual Development Plan (see [Chapter 20](#), 020.050)
 3. Career Individual Development Plan (Optional) ([Form EDU-5000](#))
 - Right Side of File (Top to Bottom Order)
 1. Performance Plans
 2. Position Description
- C. For a complete listing of records supervisors are authorized to maintain in the SSA-7B Employee Record extension File and their respective retention periods and those records which are not authorized, review the Office of Personnel’s Personnel Policy Manual, SSA-7B Employee Record Extension File, S293_4 (http://personnel.ba.ssa.gov/ope/pmisps/virtuallib/S293_4.htm).

Note: The COOP Form/Emergency Contact Form in Metastorm is OI’s electronic version of the SSA-7B.

- D. A second file (in the form of a large three-ring binder) will be established in each office headed by a SAC or RAC. This file will consist of separate sections for each employee in the office. Each employee section in the file will contain copies of documents that are to be reviewed according to a set schedule. SACs or RACs are responsible for ensuring that the employees under their supervision sign and date each form in accordance with the schedule and to indicate

on the Annual Certifications Checklist (Form OI-41) that the employee signed to acknowledge a review of the document. The documents to be included in this file include:

- Certification of Review of the OIG COOP and Emergency Preparedness Plans (Form OI-44)
- Review of the SAH Acknowledgement (Form OI-45)
- LEAP Authorization (Form OI-49)
- Home to Work Driving Authority (Form OI-46)
- Request for Workday Conditioning Activities (Form OI-48)
- Outside Activities Request Form (if applicable) (Form SSA-520)
- Lautenberg Amendment Certification (Form OI-82A)
- Law Enforcement Systems and Commercial Database Security Agreement (Form OI-88)

- E.** In addition to ensuring completion of document and policy reviews, OI managers shall use form OI-41A to track employee progress in meeting training requirements.
- F.** When an employee transfers, it is the responsibility of the losing office to forward the employee's certification documents and SF-7B extension file and certification documents to the employee's new office.

001.150 Liaison

- A.** SAs are expected to establish cooperative and professional relationships with other Federal and local law enforcement agencies.
- B.** Matters within the investigative jurisdiction of another law enforcement agency will be promptly forwarded from the SAC to an appropriate official within the other agency. However, certain information protected by Federal law, such as the Privacy Act, may only be disclosed as permitted by Federal statutes and regulations (see *Chapter 6*).
- C.** Occasionally, the working relationship with another agency may be expressed in a mutually agreed upon formal document such as a Memorandum of Understanding (MOU).
 - 1.** Only the IG can enter into an MOU committing the involvement and/or resources of more than one OIG component.
 - 2.** The IG or the AIGI may enter into an MOU with another governmental (or private sector) entity for the purpose of delineating responsibilities in handling particular cases or projects of mutual interest. Any SAC seeking such an MOU should convey the proposal to the AIGI via memorandum.
 - 3.** OCIG must review all proposed MOUs.
 - 4.** MOUs affecting OI operations are maintained in the administrative files of OI, under file 001.150.
 - 5.** At the local level, SACs may enter into less formal agreements on working relationships and arrangements concerning joint investigative activity with other agencies.

001.160 **Quality Assurance**

- A. Quality assurance reviews are designed to measure progress, ensure uniformity, and provide employees with a means of expressing satisfaction or concerns.
- B. Reviews of OI FDs will be conducted by the OIG's Office of Quality Assurance and Professional Responsibility every three years to ensure that professional standards and OIG policies are followed.

001.170 *For Future Use*

001.175 **Mutual Notification Agreement with the FBI**

- A. The Attorney General Guidelines state that the FBI has jurisdiction in all matters involving fraud against the Federal government, and shares jurisdiction with the OIG in the investigation of fraud against the OIG's agency. In such areas of concurrent jurisdiction, the OIG and the FBI agree to notify each other **promptly** upon the initiation of any criminal investigation or when new subjects are added to an investigation. Absent exigent circumstances, "promptly" shall be considered to be within 30 calendar days. Notification by the OIG shall be in writing and addressed to the FBI in the district in which the investigation is being conducted. In investigations where allegations arise that are beyond the scope of the OIG's jurisdiction, the OIG will immediately notify the appropriate investigative agency and the appropriate prosecutive authority of the allegations.
- B. All FD SACs are required to identify each FBI SAC within each OI FD and to establish procedures to follow with regard to the mutual notification agreement. At a minimum, each FD SAC must notify the FBI SAC in writing of the procedures described in paragraph C of this section. Such agreements shall be renewed only when there is a change of SAC in OI or the FBI. Otherwise, the established notification agreement between OI and the FBI remains in effect.
- C. In order to reduce the paperwork involved and create a more uniform process in making case opening notifications to the FBI, on a monthly basis, CID will notify the FBI Headquarters, Public Corruption Unit, of all case openings and new subjects added to open investigations. The monthly notification will be made electronically via the secure LEO.gov email service accessed through the FBI's Law Enforcement Enterprise Portal (FBI LEEP). The FBI will electronically notify OI of any cases in which the OIG has concurrent jurisdiction. FBI Headquarters will provide the case opening information to all appropriate responsible FBI components/offices. To ensure appropriate routing, each FD SAC will ensure that the Federal jurisdiction is annotated in NICMS on all cases opened within their FD.
- D. All FD SACs are required to submit a memorandum to the AIGI reporting that the mutual notification agreements are in place by September 30th of each year. The memorandum must identify each FBI SAC by name and location and include the date the FD SAC advised the FBI SAC of the procedures described in paragraph C of this section.

001.180 Mutual Assistance Agreement Authorizing Cooperation Among Offices of Inspectors General in the Execution of Search and Arrest Warrants

- A.** Attorney General Order No. 3168-2010 dated June 28, 2010, authorizes special agents of each OIG otherwise authorized to exercise powers under subsection 6(e)(1)(C) of the IG Act (this includes the SSA OIG), to seek and execute warrants issued under the authority of the United States for arrest, search of premises, or seizure of evidence. This authorization shall extend to the number of agents that the loaning IG, or, at his discretion the Assistant Inspector General for Investigations reporting to him, deems appropriate.
1. Agents of the loaning IG shall operate under the direction of the IG to whom they are providing assistance.
 2. The loaning IG shall not direct agents as they assist the requesting IG.
- B.** Assistance provided by one IG to another pursuant to the authority granted in this order must comply with procedures to be established by the Council of Inspectors General on Integrity and Efficiency (CIGIE). Questions about CIGIE procedures should be directed through a CID desk officer for ultimate presentation to the DAIGI of Field Operations for discussion with the head of the CIGIE Investigations Committee.
- C.** Such assistance is authorized only for the purpose of supporting a specified search or arrest operation. Assistance is not authorized for other investigative activities. The duration of the assistance shall be agreed upon by both IGs and generally should not exceed five days. The IGs shall memorialize this agreement and the other terms of the loan in writing.
- D.** The formal guidance issued by the Department of Justice applies when participating OIGs do not already share jurisdiction. In situations where there is a joint investigative and nexus to each OIG's mission (e.g., where OIGs have legal jurisdiction over the subject of the investigation, mutual support would already be available through a joint investigation), a formal written agreement is unnecessary.
- E.** Reimbursement of expenses shall be decided prior to providing assistance in instances where OI does not share jurisdiction with the requesting agency, or when OI requests assistance from another OIG that does not share jurisdiction in the matter under investigation. If reimbursement will be sought or provided, the OI supervisor in charge of the area in which the investigative activity will occur is responsible for completing the Mutual Assistance Agreement ([Exhibit 1-5](#)) prior to providing, or requesting, any assistance.
- F.** The OI supervisor referred to in section E. is responsible for contacting OTRM for approval of the Mutual Assistance Agreement. The OI supervisor must be prepared to provide the following are the budget data needed for creating an interagency /reimbursable agreement for borrowing/lending, respectively, criminal investigators between OIGs:
- Subobject class code;
 - Common Account Number,(optional);
 - Agency Employer Identification Number;
 - DUNS or Business Partner Number;
 - Treasury Account Symbol;
 - Trading Partner Code;

- Agency Location Code;
- Estimated agreement amount;
- Authority (can be The Inspector General Act);
- Name, title, and telephone number of authorized official signing the agreement;
- Name, title, address, telephone number and email address of the Program Official;
- Name, title, address, telephone number and email address of the Funding Official; and
- Name, title, address, telephone number and email address of the Finance Official.

Chapter 1 — **EXHIBITS**

[1-1 — “Quality Standards for Investigations”](#)

[1-2 — Attorney General Guidelines for OIGs with Statutory Law Enforcement Authority](#)

[1-3 — AIGI Policy Message](#)

[1-4 — Sample Fraud Alert](#)

[1-5 — U.S. Government Interagency Agreement \(Form 6-10 FMS 7600A\) – Mutual Assistance Agreement](#)

Council of Inspectors General on Integrity and Efficiency

**QUALITY
STANDARDS
FOR
INVESTIGATIONS**

NOVEMBER 2011

<https://www.ignet.gov/sites/default/files/files/invstds2011.pdf>



**ATTORNEY GENERAL GUIDELINES
FOR OFFICES OF INSPECTOR GENERAL WITH
STATUTORY LAW ENFORCEMENT AUTHORITY**

I. PURPOSE

These Guidelines, required by section 6(e)(4) of the Inspector General Act of 1978 (the “Act”), as amended in 2002, govern the exercise of law enforcement authorities for those Offices of Inspector General that have been granted statutory law enforcement authorities pursuant to that Act. These Guidelines replace the Memorandum of Understanding under which the Department of Justice deputized certain Office of Inspector General investigators as Special Deputy United States Marshals and that described the training and operational requirements applicable to the deputized Office of Inspector General investigators.

II. BACKGROUND

The Department of Justice has primary responsibility for enforcement of violations of federal laws by prosecution in the United States district courts. The Federal Bureau of Investigation is charged with investigating violations of federal laws. Offices of Inspector General have primary responsibility for the prevention and detection of waste and abuse, and concurrent responsibility for the prevention and detection of fraud, within their agencies and their agencies programs. The Inspector General Act of 1978, 5 U.S.C., App 3, established criminal investigative offices of presidentially appointed Inspectors General. However, prior to enactment of section 812 of the Homeland Security Act of 2002 (Pub. L. No. 107-296), the Inspector General Act did not provide firearms, arrest, or search warrant authorities for investigators of those offices.¹ The Inspectors General of the various executive agencies rely on Memoranda of Understanding with the Department of Justice that provided temporary grants of law enforcement powers through deputations. As the volume of investigations warranting such police powers increased, deputations were authorized on a “blanket,” or office-wide, basis.

With the enactment of section 6(e) of the Inspector General Act, the Attorney General, after an initial determination of need, may authorize law enforcement powers for eligible personnel of each of the various offices of presidentially appointed Inspectors General. The determination of need hinges on the respective office meeting the three prerequisites enumerated in section 6(e)(2). Those Offices of Inspector General listed in section 6(e)(3) of the Act are exempt from the requirement of an initial determination of need by the Attorney General.

Offices of Inspector General receiving law enforcement powers under section 6(e) must exercise those authorities in accordance with Guidelines promulgated by the Attorney General. This documentation sets forth the required Guidelines.

¹ Certain Offices of Inspector General had (prior to 2002) and continue to have OIG-specific grants of authority under which they exercise law enforcement powers.

Exhibit 1-2

III. APPLICATION OF GUIDELINES

These Guidelines apply to qualifying personnel in those offices of presidentially appointed Inspectors General with law enforcement powers received from the Attorney General under section 6(e) of the Inspector General Act of 1978, as amended. Qualifying personnel include the Inspector General, the Assistant Inspector General for Investigations under such Inspector General, and all special agents supervised by the Assistant Inspector General for Investigations, provided that those individuals otherwise meet the training and qualifications requirements contained in these Guidelines. These mandatory Guidelines do not limit Offices of the Inspector General from exercising any statutory law enforcement authority derived from a source other than section 6(e). These Guidelines may be revised by the Attorney General, as appropriate. These Guidelines may be supplemented by agency-specific agreements between an individual Office of Inspector General and the Attorney General.

If the Attorney General determines that an Office of Inspector General exercising law enforcement powers under sections 6(e), or any individual exercising such authorities, has failed to comply with these Guidelines, the Attorney General may rescind or suspend exercise of law enforcement authorities for that office or individual.

IV. LAW ENFORCEMENT TRAINING AND QUALIFICATIONS

A. Basic and Refresher Training

Each Office of Inspector General must certify completion of the Basic Criminal Investigator Training Program at the Federal Law Enforcement Training Center by each Inspector General, Assistant Inspector General of Investigations, and Special Agent/Investigator who will be exercising powers under these Guidelines. As an alternative, this training requirement may be satisfied by certification of completion of a comparable course of instruction to the Federal Law Enforcement Training Center Basic Criminal Investigator Training Program. Additionally, the Office of Inspector General will provide periodic refresher training in the following areas: trial process; federal criminal and civil legal updates; interviewing techniques and policy; law of arrest, search, and seizure; and physical conditioning/defensive tactics. The specifics of these programs should conform as much as practicable to standards such as those set at the Federal Law Enforcement Training Center or the Federal Bureau of Investigation Training Academy at Quantico, Virginia.

B. Firearms Training and Qualification Requirements

All individuals exercising authorities under section 6(e) must receive initial and periodic firearms training and qualification in accordance with Federal Law Enforcement Training Center standards. This training will focus on technical proficiency in using the firearms the Special Agent will carry, as well as the policy and legal issues involved in the use of deadly force. The initial training for this requirement must be met by successful completion of an appropriate course of training at the Federal Law Enforcement Training Center or an equivalent course of instruction (that must include policy and law concerning the use of firearms, civil liability, retention of firearms and other tactical training, and deadly force policy).

In addition to basic firearms training, each covered Office of Inspector General will implement a program of quarterly firearms qualifications by all individuals exercising authorities under section 6(e). Such program will be conducted in accordance with recognized standards.

Exhibit 1-2

C. Deadly Force Policy

The Offices of Inspector General will abide by the deadly force policy established by the Department of Justice.

V. RANGE OF LAW ENFORCEMENT POWERS

Section 6(e) of the Act provides that the Attorney General may authorize covered individuals to:

1. carry a firearm while engaged in official duties as authorized under this Act or other statute, or as expressly authorized by the Attorney General;
2. make an arrest without a warrant while engaged in official duties as authorized under this Act or other statute, or as expressly authorized by the Attorney General, for any offense against the United States committed in the presence of such individual, or for any felony cognizable under the laws of the United States if such individual has reasonable grounds to believe that the person to be arrested has committed or is committing such felony, and
3. upon probable cause to believe that a violation has been committed, seek and execute warrants for arrest, search of a premises, or seizure of evidence issued under the authority of the United States.

Individuals exercising law enforcement authorities under section 6(e) may exercise those powers only for activities authorized under the Inspector General Act of 1978 or other statute, or as expressly authorized by the Attorney General².

The Inspector General of each agency covered by these Guidelines, any Assistant Inspector General for Investigations under such Inspector General, and any special agent supervised by such an Assistant Inspector General are authorized to carry their firearms while off-duty when the Inspector General determines that they need to do so for operational or safety reasons.

The possession of firearms on aircraft while on official duty shall be governed by Transportation Security Administration guidelines and common carrier regulations applicable to the transport of firearms.

VI. ADHERENCE TO ATTORNEY GENERAL GUIDELINES

In addition to any other Department of Justice directives or guidance referenced in these Guidelines, Offices of Inspector General will adhere to the Attorney General's Guidelines on General Crimes, Racketeering Enterprise, and Terrorism Enterprise Investigations; the Attorney General's Guidelines Regarding the Use of Confidential Informants, the Attorney General's Memorandum on Procedures for Lawful, Warrantless Monitoring of Verbal Communications;

2. Section 6(e) does not, of itself, provide plenary authority to make arrests for non-federal criminal violations. Legal authority for officers to respond to such offenses generally depends on state law. A federal agency may, however, as a matter of policy, permit its officers to interview in serious criminal conduct that violates state law under certain circumstances.

Exhibit 1-2

any other Attorney General Guidelines applicable to criminal investigative practices; and updated or amended versions of any of the aforementioned documents.

VII. NOTIFICATION AND CONSULTATION REQUIREMENTS WITH RESPECT TO ALLEGATIONS OF CRIMINAL VIOLATIONS

The Inspector General Act directs expeditious reporting to the Attorney General whenever an Office of Inspector General has reasonable grounds to believe there has been a violation of federal criminal law.

A. Offices of Inspector General/Federal Bureau of Investigation Mutual Notification Requirements

As the primary investigative arm of the Department of Justice, the Federal Bureau of Investigation has jurisdiction in all matters involving fraud against the Federal Government, and shares jurisdiction with the Offices of Inspector General in the investigation of fraud against the Office of Inspector General's agency. In areas of concurrent jurisdiction, the Offices of Inspector General and the Federal Bureau of Investigation must promptly notify each other in writing upon the initiation of any criminal investigation. The notification requirement is a continuing obligation when new subjects are added to an investigation. Absent exigent circumstances, "promptly" shall be considered to be within 30 calendar days. Notification by the Offices of Inspector General shall be in writing and addressed to the Federal Bureau of Investigation in the district in which the investigation is being conducted. Notification by the Federal Bureau of Investigation shall be in writing and addressed to the appropriate regional office of the Office of Inspector General. Notifications shall include, at a minimum and where available, (a) subject name, date of birth, social security number, and (b) any other case-identifying information including, but not limited to, (i) the date the case was opened or the allegation was received, and (ii) the allegation that predicated the case. For investigations in which allegations arise that are beyond the scope of the Office of Inspector General's jurisdiction, the Office of Inspector General will immediately notify the appropriate investigative agency of the allegations.

B. Consultation with Prosecutors

In all criminal investigations, a federal prosecutor must be consulted at an early stage to ensure that the allegations, if proven, would be prosecuted. Such consultation will also ensure coordination of investigative methods.

VII. USE OF SPECIALIZED INVESTIGATIVE PROCEDURES AND TECHNIQUES

A. Court-Ordered Electronic Surveillance

Court-authorized interception of wire, oral, or electronic communications are among the most intrusive investigative techniques currently available to law enforcement. The rigors of the approval process, expenditures of financial and manpower resources, and the probability of challenges by the defense bar make this technique subject to intense scrutiny. Surreptitious electronic surveillance using closed-circuit television presents similar considerations. Accordingly, any investigation involving the interception of communications pursuant to 18

Exhibit 1-2

U.S.C. 2510, *et seq.*, electronic surveillance using closed-circuit television in situations where a warrant is required, or any other court-ordered electronic surveillance, shall be conducted only after consulting with the Federal Bureau of Investigation may choose to join the investigation, but is not required to do so. However, in an instance in which the Office of Inspector General intends to engage in court-authorized electronic surveillance without the participation of the Federal Bureau of Investigation, one of the following federal investigative agencies must participate in the investigation and supervise the application for and use of the surreptitious electronic surveillance: the Drug Enforcement Administration; Bureau of Alcohol, Tobacco, Firearms, and Explosives; DHS – Homeland Security Investigations; United States Postal Service; United States Secret Service; or Internal Revenue Service.

B. Undercover Investigative Operations

The Attorney General’s Guidelines on Federal Bureau of Investigation Undercover Operations (the “Undercover Guidelines”) ensure that the Federal Bureau of Investigations considers the efficacy, as well as the legal and policy implications, of every proposed undercover operation, and ensure that the use of the undercover investigative technique is subject to a management on-site review and oversight on a regular basis. It is the intent of this provision that undercover operations conducted by the Offices of Inspector General be subject to the same standards that govern the use of this investigative technique by the Federal Bureau of Investigation.

Accordingly, the community of Inspectors General granted law enforcement powers under section 6(e) of the Inspector General Act shall establish an Undercover Review Committee (the Committee) composed of 6 senior headquarters managers selected by the community of Inspectors General, with no two members of the Committee being employed by the same Office of Inspector General, for the purpose of reviewing undercover operations involving sensitive circumstances³ in investigations that are not being conducted jointly with the Federal Bureau of Investigation. The Committee shall also include such representatives from the litigating sections of the Criminal Division of the Department of Justice as are designated by the Assistant Attorney General of the Criminal Division. If an undercover investigation being conducted by an Office of Inspector General that is not represented on the Committee, a representative of that Office of Inspector General who is a senior management official shall be added as a full member of the Committee to review that undercover operation. The Federal Bureau of Investigation may designate a representative to participate in the Committee in a consultative role.

Before conducting an undercover operation lasting longer than six months, or involving any of the sensitive circumstances set forth in the Undercover Guidelines, the Office of Inspector General must first notify the Federal Bureau of Investigation. The Federal Bureau of Investigation may choose to join the investigation, in which case the undercover operation would be subject to review by the Criminal Undercover Operations Review Committee of the Federal Bureau of Investigation. If the Federal Bureau of Investigation opts not to join the case, the undercover operation will be reviewed by the Committee. No undercover operation involving sensitive circumstances may be conducted without the approval of one of these committees.

3. “Sensitive circumstances” are set forth in the Undercover Guidelines, and include investigations involving certain public officials, a significant risk of violence, authorized criminal activity, operations of a proprietary business, the risk for significant civil liability, and other circumstances as defined in those Guidelines.

Exhibit 1-2

The approval for each undercover operation involving sensitive circumstances must be renewed for each six month period, or less, during which the undercover operation is ongoing. The standards of the Committee for approval of the undercover operation shall operate in the same fashion as the Criminal Undercover Operations Review Committee as outlined in the Undercover Guidelines.

Each Office of Inspector General whose law enforcement effort contemplates the use of the undercover investigative technique in investigations not involving the sensitive circumstances set forth above shall establish procedures that are consistent with the procedures established for such undercover investigations not involving sensitive circumstances as are set forth in the Undercover Guidelines.

C. Especially Sensitive Targets

1. Upon notification pursuant to Part Vii, Subpart VII, Subpart A of these Guidelines, or otherwise the Federal Bureau of Investigation may choose to join, but would not be required to join, any investigation that involves:
 - (a) especially sensitive targets, including a member of Congress, a federal judge, a member of the executive branch occupying a position for which compensation is set at the Executive Level IV or above, or a person who has served in such capacity within the previous two years;
 - (b) a significant investigation of a public official for bribery, conflict of interest, or extortion relating to the official's performance of duty;
 - (c) a significant investigation of a federal law enforcement official acting in his or her official capacity; or
 - (d) an investigation of a member of the diplomatic corps of a foreign country.
2. Investigations involving certain other classes of persons may result in serious security concerns, especially regarding the operation of the Federal Witness Security Program. Therefore an Office of the Inspector General investigation will be coordinated with the Office of Enforcement Operations of the Criminal Division, Department of Justice, when the investigation:
 - (a) involves a person who is or has been a member of the Witness Security Program if that fact is known by the Office of Inspector General;
 - (b) involves a public official, federal law enforcement officer, or other government employee who is or has been involved in the operation of the Witness Security Program;
 - (c) involves the use or targeting, in an undercover capacity, of a person who is in the custody of the Federal Bureaus of Prisons or the United States Marshals Service, or in under Federal Bureau of Prisons' supervision; or
 - (d) involves the use or targeting, in an undercover capacity, of the Federal Bureau of Prisons employee, if any part of the activity will occur within the confines of, or otherwise would

Exhibit 1-2

be likely to affect the security of, a Bureau of Prisons-administered facility.

Investigations that require coordination with the Office of Enforcement Operations pursuant to Party VIII, Subpart C.(2)(a)-(d) may be conducted without the participation of the Federal Bureau of Investigation. In such instances, notification of the investigation should not be made to any other agency without the explicit approval of the Office of Enforcement Operations.

D. Consensual Monitoring in Certain Situations

Consensual monitoring of conversations in some circumstance can present unusual problems. Accordingly, if the Office of Inspector General contemplates the use of consensual monitoring involving a consenting or non-consenting person in the custody of the Bureau of Prisons or the United States Marshals Service, the use of any type of consensual monitoring in the investigation, whether telephonic or non-telephonic, must be coordinated with the Office of Enforcement Operations at the Department of Justice.

Consistent with the Attorney General's Memorandum on Procedures for Lawful, Warrantless Monitoring of Verbal Communications, the use of any non-telephonic consensual monitoring in an Office of Inspector General investigation requires the prior approval of the Director or an Associate Director of the Office of Enforcement Operations if any of the following sensitive circumstances are present:

- (a) the monitoring relates to an investigation of a member of Congress, a federal judge, a member of the Executive Branch occupying a position for which compensation is set at Executive Level IV or above, or a person who has served in such capacity within the previous two years;
- (b) the monitoring relates to an investigation of the Governor, Lieutenant Governor, or Attorney General of any State, or Territory, or a judge or justice of the highest court of any State or Territory, and the offense investigated is one involving bribery, conflict of interest, or extortion relating to the performance of his or her official duties;
- (c) any party to the communication is a member of the diplomatic corps of a foreign country;
- (d) any party to the communication is or has been a member of the Witness Security Program and that fact is known to the agency involved or its officers;
- (e) the consenting or non-consenting person is in the custody of the Bureau of Prisons or the United States Marshals Service; or
- (f) the Attorney General, Deputy Attorney General, Associate Attorney General, any Assistant Attorney General, or the United States Attorney in the district where an investigation is being conducted has requested the investigating agency to obtain prior written consent before conducting consensual monitoring in a specific investigation.

IX. PROSECUTOR CONCURRENCE FOR CERTAIN TECHNIQUES

The use and control of informants, sources, and cooperating witnesses is recognized by the courts as lawful and often essential to the effectiveness of properly authorized law enforcement

Exhibit 1-2

investigations. However, certain guidelines must be applied because the use of informants and cooperating witnesses may involve intrusion into the privacy of individuals, or cooperation with individuals whose reliability and motivation can be open to question. In the following situations, *inter alia*, the prior concurrence of a federal prosecutor must be obtained to avoid problems such as entrapment, danger to the public, and abuse of police authority:

1. when an informant is authorized to participate in criminal activities;
2. when an informant or cooperating witness is a person entitled to claim a federally recognized legal privilege of confidentiality, such as an attorney, member of the clergy, or psychiatrist;
3. when aggregate payments for services or expenses to be made to a source who could be a witness in a legal proceeding exceed \$25,000; or
4. when the use of any member of the news media as a source is planned (and in such a situation the prior written approval of a federal prosecutor must be obtained).

X. RELATIONS WITH THE NEWS MEDIA

The Department of Justice has issued guidelines that prescribe policy and instructions concerning the release of information by Department of Justice employees relating to criminal and civil proceedings (see 28 C.F.R. 50.2). Office of Inspector General personnel must familiarize themselves with and follow these guidelines. In addition, in the course of joint investigations between an Office of Inspector General and the Federal Bureau of Investigation, wherever a “news release” would be permitted pursuant to the guidelines noted above, the Office of Inspector General must coordinate the release with the Federal Bureau of Investigation and the Department of Justice.

XI. REPORTING REQUIREMENTS

Each Office of Inspector General shall make an annual written report to the Attorney General due on November 1 of each year, detailing the investigative and prosecutive activities of that Office of Inspector General. The report shall, at a minimum, contain information on the number of (1) federal criminal investigations initiated, (2) undercover operations undertaken, and (3) times any type of electronic surveillance was used. Additionally, the report shall provide information on all significant and credible allegations of abuse of authorities conferred by section 6(e)(1) of the Inspector General Act by Office of Inspector General investigative agents and what, if any, actions were taken as a result. The names of the agents need not be included in such report.

XII. PEER REVIEWS

In accordance with section 6(e)(7) of the Inspector General Act, covered Offices of Inspector General must implement a collective memorandum of understanding, in consultation with the Attorney General, under which each Office of Inspector General will be periodically reviewed by another Office of Inspector General or a committee of Offices of Inspector General. Reviews should occur no less often than once every 3 years. The purpose of the review is to ascertain whether adequate internal safeguards and management procedures exist to ensure that the law enforcement powers conferred by the 2002 amendments to the Inspector General Act are properly

Exhibit 1-2

exercised. Results of the review will be communicated to the Attorney General, as well as to the applicable Inspector General.

XIII. NO THIRD-PARTY RIGHTS CREATED

These Guidelines are adopted for the purpose of the internal management of the Executive Branch. These Guidelines are not intended to, do not, and may not be relied upon to, create any rights, substantive or procedural, enforceable at law or in equity by any party in any matter civil or criminal, nor do these Guidelines place any limitations on otherwise lawful investigative or litigation prerogatives of the Department of Justice or otherwise lawful investigative prerogatives of the covered Offices of Inspector General.

Signed/

December 8, 2003

John Ashcroft
Attorney General

Exhibit 1-3



SAMPLE

AIGI Policy Message # FY 2008-1

FILE: 000.000
001.130

Policy messages are numbered using the fiscal year in which the policy is issued followed by a sequential number. The file number reflects the section of the Special Agent Handbook affected by the policy change and the administrative file number for policy changes (001.130).

Policy messages originate from the Executive Officer. The names at the bottom of the message indicate the OI senior manager, either the AIGI or DAIGI, who approved the policy.



FRAUD ALERT

ACTIVITY OR EVENT REPORTED

The body of this document contains a narrative description of the activity or event that OI headquarters staff believes is of sufficient importance to all OI agents nationwide and other SSA components.

Confidential — Sensitive Information

OIG Fraud Alert No. __ - FY 200__

Issued MM/DD/YY

Exhibit 1-5

Mutual Assistance Agreement (click on icon)



Sample OIG
Assistance Agreement.

RESPONSIBILITIES AND CONDUCT

002.000 Standards of Ethical Conduct

- A.** The *Standards of Ethical Conduct for Employees of the Executive Branch*, codified at Title 5, Code of Federal Regulations, Part 2635, apply to all Federal employees of the Executive Branch of Government, except for members of the armed services. Violations of these standards can lead to disciplinary action up to and including removal from the Federal service. All Office of Investigations (OI) Special Agents (SA) must be familiar with these standards not only as they apply to themselves, but also their applicability to employee violations under investigation.
- B.** Questions regarding the applicability or interpretation of these standards should be directed to the Office of Counsel to the Inspector General (OCIG) at Headquarters (HQ).

002.010 Digest of Standards of Ethical Conduct

- A.** Public service is a public trust. To ensure that every citizen can have complete confidence in the integrity of the Federal Government and the Office of the Inspector General (OIG), each OI employee shall respect and adhere to the principles of ethical conduct set forth in the *Standards of Ethical Conduct for Employees of the Executive Branch*, as well as any supplemental agency regulations.
- B.** OI employees shall apply the principles in the *Standards of Ethical Conduct* noted above in determining whether their conduct is proper.
- C.** OI employees will:
 - 1.** Obey Federal, State, and local laws.
 - 2.** Observe and comply with all applicable standards of conduct established by appropriate authority.
 - 3.** Follow the instructions of supervisors and other management officials in their line of authority, as well as written directives concerning the conduct of official business.
 - 4.** Put forth an honest effort in the performance of their duties.
 - 5.** Act impartially and not give preferential treatment to any private organization or individual.

6. Protect and conserve Federal property and not use it for other than authorized activities or official business.
7. Disclose waste, fraud, abuse, and corruption to appropriate authorities.
8. Satisfy in good faith their obligations as citizens, including all just financial obligations, especially those such as Federal, State, or local taxes that are imposed by law.
9. Avoid actual conflicts of interest or any actions creating the appearance of a conflict of interest or impropriety.
10. Advise their supervisor in writing promptly if they have been arrested, held for investigation or questioning, or if charges of any kind have been brought against them.

D. OI employees will not:

1. Hold financial interests that conflict with the conscientious performance of duty.
2. Engage in financial transactions using non-public Government information or allow the improper use of such information to further any private interest.
3. (Except as permitted by subpart B of the *Standards of Ethical Conduct*) Solicit or accept any gift or other item of monetary value from any person or entity seeking official action from doing business with, or conducting activities regulated by, the Social Security Administration (SSA) or whose interests may be substantially affected by the performance or non-performance of the OI employee's duty.
4. Knowingly make unauthorized commitments or promises of any kind purporting to bind the Federal Government.
5. Engage in outside employment or activities, including seeking or negotiating for employment, that conflict with official Government duties and responsibilities.

E. In addition to the standards of ethical conduct noted in Section 002.010, there are conflict of interest statutes that prohibit certain conduct. Criminal conflict of interest statutes of general applicability to all employees; e.g., 18 U.S.C. §§ 201, 203, 205, 208, and 209, must be taken into consideration in determining whether conduct is proper.

F. OI employees must abide by the Department of Justice's "[Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender Identity](#)". This guidance applies to Federal law enforcement officers performing Federal law enforcement activities, including those related to national security and intelligence, and defines the circumstances in which Federal law enforcement officers and state and local law enforcement officers while participating in Federal law enforcement task forces may take into account a person's race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity.

002.020 Supplemental Agency Regulations on Conduct

- A. In addition to the standards of ethical conduct noted in Section 002.010, all OI employees shall comply with any supplemental regulations governing employee conduct issued by SSA.
- B. A violation of the standards of ethical conduct or of supplemental agency regulations may be cause for corrective or disciplinary action to be taken under applicable Government-wide regulations or agency procedures. Such actions may be in addition to any action or penalty prescribed by law.

002.030 Conduct While on Official Duty

- A. The general reputation, credibility, and professional image of the OIG and OI depend on the actions of each member of the organization. Daily contact by OI SAs and other OI employees with the public, Government agencies, law enforcement personnel, United States Attorneys, courts, and others is an opportunity to create and maintain a professional image and reputation.
- B. Below are some guidelines which should be followed at all times. OI SAs:
 - 1. Will exercise SA authority only in connection with matters of official interest to the OIG.
 - 2. Will not engage in the abuse of investigative authority or unnecessary interference in the operations of others during the conduct of an investigation.
 - 3. Will not display or use badges, credentials, firearms, restraint devices, or any other law enforcement equipment **except in the line of duty**. Unauthorized use is a serious matter and can result in disciplinary action, including removal from Federal service.
 - 4. Will avoid expressing personal opinions on controversial, social, or political matters while on official business.
 - 5. Will cooperate to the fullest extent permitted by law with other law enforcement agencies conducting investigations with OI.

002.040 Outside Activities

- A. Outside activities, including outside employment, are governed by Federal regulation and require a prior written request to, and approval by, OI management. Detailed guidance on outside activities and the policy and procedures covering all OIG employees is contained in the *OIG Administrative Policies and Procedures Manual*.
- B. Examples of outside activities requiring prior written approval include:
 - 1. Certain types of professional and consultative services.
 - 2. Certain teaching, lecturing, writing, editing, and certain office-holding activities in professional societies.

3. All activities for which OI employees are financially compensated and which are considered employment or business.
 4. All legal services and all outside law enforcement activities, including volunteer work, with the exception of temporary legal services to relatives (for example, drawing a will or handling a traffic violation, eviction notice, or mortgage transaction).
- C. Employees of OI should request prior approval of any activity that could cause embarrassment to, or call into question, the integrity or objectivity of the OIG. When in doubt about the appropriateness of an outside activity, an employee should submit a written request for approval.
- D. The following are some examples of outside activity situations where approval will generally be denied, except in exceptional circumstances:
1. Any outside activity when the OI employee is receiving Law Enforcement Availability Pay (LEAP).
 2. All outside law enforcement activities or positions involving the carrying of firearms.
 3. All outside investigative or detective work.
 4. Any outside employment requiring more than 1,040 hours per year, or more than an average of 20 hours per week if the employment is temporary or seasonal.
 5. Any ownership or substantial interest in a business where the business could become involved in matters falling within the jurisdiction of the OIG.
- E. Because of the increased likelihood of a conflict of interest, or the appearance of a conflict, in the outside activities of OI HQ employees and all OI management personnel, approval for outside activities will be granted only where there is a minimal risk of a potential conflict. Most professional and consultative services to the general public will not be approved except in special circumstances.

002.050 **Drug and Alcohol Use**

- A. OI's alcohol and drug use policies are formed on the premise that OI must maintain maximum operational readiness and effectiveness as a law enforcement agency.
- B. OI's law enforcement mission requires that OI employees engage in activities that require the ability to think and react quickly, free of any impairment attributable to the use of alcohol or drugs. Such activities include, but are not limited to:
1. Carrying and using firearms.
 2. Executing search warrants.
 3. Operating motor vehicles while on Government business.
 4. Dealing with other Government agencies, including other law enforcement agencies.

5. Dealing with the public.
- C.** Each OI employee engaging in any such activity represents OI as an organization and consequently shares with fellow employees the responsibility to:
1. perform effectively in all situations, including those that pose the threat of physical injury to any person or of loss or destruction of essential evidence; and
 2. maintain the good reputation of OI as an organization.
- D.** Administrative sanctions may be imposed against OI employees who, without authorization, consume alcoholic beverages while on duty on Government premises or while in duty status, or who are under the influence of alcohol when reporting for duty or while in duty status.
- E.** In addition, it is OIG OI policy that OI employees will refrain from consuming alcoholic beverages:
1. prior to reporting for duty on a workday, whether or not on approved leave beforehand; and
 2. at any time during the workday, including lunch breaks or other work breaks.
- F.** Administrative sanctions may be imposed against OI employees who violate this prohibition, whether or not their performance or capacity to perform is impaired.
- G.** (b) (7)(E) [REDACTED]
[REDACTED]
[REDACTED]
- H.** The exception in Section 002.050 may be authorized by:
1. the Assistant Inspector General for Investigations (AIGI),
 2. a Deputy Assistant Inspector General for Investigations (DAIGI),
 3. a Special Agent-in-Charge (SAC), or
 4. an Assistant Special Agent-in-Charge (ASAC).
- I.** It is the personal responsibility of each OI employee to remove himself/herself from the official operation under Section 002.050 if he/she becomes impaired due to the consumption of alcohol.
- J.** All OI employees must be aware that certain legal drugs and medications may impair their ability to function.
- K.** Any OI employee who is (or may reasonably expect to be) armed in the course of the workday and who senses (or reasonably anticipates) impairment attributable to legal drug use must:

1. report that condition to his/her supervisor; and
 2. request leave or assignment to other duties.
- L.** OI prohibits the use of illegal drugs by any OI employee at any time.
1. Sanctions may be imposed against OI employees who violate this prohibition, whether or not their performance or capacity to perform is impaired.
 2. OI employees who abuse alcohol or drugs, or who feel that they may have an alcohol or drug-related problem, are encouraged to seek corrective professional help.
- M.** All OI employees have access to an employee counseling service office which can help them obtain appropriate assistance.

002.060 Use of Official Vehicles

The use of Government vehicles (GOV) for transportation between an employee's residence and workplace (official duty station – ODS) is essential for the safe and efficient performance of criminal law enforcement duties by investigative personnel. It is the policy of the OIG to permit home-to-work transportation if certain conditions are met. All OIG fleet users and oversight officials will comply with the provisions of internal control and record keeping as set forth in this section.

- A.** SAs and Supervisory SAs may be certified home-to-work use of an official GOV provided that:
1. Such use is essential for the safe and efficient performance of criminal law enforcement duties.
 2. Their duties require that they are continually available for communications and recall to duty, and/or that their duties would be rendered inefficient or unsafe without home-to-work transportation.
 3. The activities performed by these personnel would be adversely affected by the lack of home-to-work transportation.
 4. The distance from the Special Agent's residence to their official duty station does not exceed 60 miles. If the distance does exceed 60 miles, it is the responsibility of the Special Agent to find alternate secure parking for the GOV within the 60 mile radius.
 - a. Alternate secure parking may include a local police department, fire department or municipal government facility.
 - b. Those SA's whose current residence to ODS mileage does not meet this requirement as of January 1, 2014 are grandfathered.
- B.** SACs (for their FDs) and the AIGI or the DAIGI (for SACs) will review the duties and activities of personnel under their commands on a continuing basis. Those personnel whose duties or activities do not conform to the criteria for granting home-to-work driving authority will be decertified.

- C.** Certification for home-to-work use of an official GOV for performance of criminal law enforcement duties will be documented on form OI-46 ([see Exhibit 2-1](#)). The employee's supervisor will be the certifying official on the form. Current certifications must be maintained in a master file (see section 001.140C) at the issuing office and renewed on or about October 1 of each year.
- D.** SACs are responsible for annually notifying the DAIGI when the certification process is complete. This notification is due by December 31st of each year.
- E.** Employees certified for home-to-work use of an official GOV are responsible for the security of the vehicle. GOVs must not be left in areas where there is a high probability that the vehicle will be vandalized or stolen. Security of all equipment provided by the government is the responsibility of the agent assigned to the vehicle. Equipment assigned to an employee for official use shall not be left in a GOV in plain view. Sensitive property such as firearms or radios should not be left unattended in a vehicle. The person to whom the vehicle is assigned is responsible for reporting any damage done to the vehicle to his/her supervisor in writing within 48 hours from the time the damage is first noticed. The information must be forwarded to the ^OIG PAD mailbox within 10 days of the incident.
- F.** Each FD will maintain control over the use of the GOV as follows:
- 1.** The SAC or his/her designee will ensure that a separate folder is maintained for each vehicle assigned.
 - 2.** The folder will contain copies of all documents for that vehicle. At a minimum, copies of maintenance bills or other charges and vouchers used to maintain the vehicle will be included.
- G.** In accordance with 31 U.S.C. § 1349, any employee who willfully misuses a passenger motor vehicle owned or leased by the United States Government shall be suspended for at least one month, and when circumstances warrant, for a longer period or summarily removed from office. Title 31 U.S.C. § 1344 requires that Federal funds for passenger motor vehicles be used only to provide transportation for official purposes.
- H.** Vehicles leased from the General Services Administration (GSA) Fleet Management Centers come with a "Motor Vehicle Accident Reporting Kit." Drivers of these vehicles are expected to be knowledgeable of and comply with the information contained in the operator instructions and the accident reporting kit. The kit contains instructions on what to do in case of an accident, forms, and proof of insurance for operators of GSA owned vehicles. If an accident occurs, appropriate information needed to complete the forms should be exchanged. The agent should cooperate fully with local authorities in providing complete and truthful information, but opinions as to the fault or liability should be left for the local authorities and/or a judge if and when a claim is filed.
- I.** Any OI employee involved in a motor vehicle accident, or an incident where damage to the vehicle has occurred, to a GSA owned or a commercially leased vehicle must provide to their immediate supervisor a memorandum explaining the circumstances surrounding the accident, a copy of the police report, photos of all vehicles involved, and the SF-91 (GSA Accident Report). The supervisor will forward the signed documents to the ^OIG PAD mailbox within 10 business

days of the accident. Once repair estimate(s) are obtained, copies must be forwarded to the same mailbox. All documentation will be provided to the appropriate DAIGI for review. Upon review, the DAIGI will determine activation of the OI Accident Review Board (ARB). The ARB will consist of at least three Headquarters personnel at the GS-14 level or above. The ARB will review the documents and will make a recommendation to the DAIGI for action regarding the accident. The DAIGI will be the deciding official on any action taken. Upon the rendering of a decision by the DAIGI, the designated ARB Chairperson will be responsible for notifying the field division of any remedial actions required. OI personnel found to be operating a GOV in an inappropriate manner may be subject to loss of GOV privileges and disciplinary action. PAD will report the accident to the OIG Safety Officer located in the Office of Communications and Resource Management. Additionally, OI employees must report all maintenance/repairs to OI HQ, via the ^OIG PAD mailbox, prior to having the work completed.

- J.** OI personnel are called upon to make judgments pertaining to traffic laws, pursuit driving, and the use of emergency lights and sirens in the performance of their duties. The paramount consideration in making these judgments will be safety.
1. OI personnel should observe traffic laws in the performance of their duties. Situations may arise that will necessitate operating under emergency vehicle laws. Safety will be the agent's paramount consideration while operating under these laws.
 2. High-speed driving is prohibited unless a life is believed to be in jeopardy. When necessary, it must be undertaken with prudence and regard for the safety of all concerned. Safety is paramount, not capture.
 3. It is not practicable to frame exact guidelines to cover all situations in which emergency lights and siren must be used. It must be stressed that they are for use in emergency situations only. An SA must be able to justify their use.
 4. SACs are responsible for briefing SAs who work within their FD on the applicable laws concerning the use of emergency lights and siren, as well as the limitations of "Peace Officer Status" within their respective states. This briefing may be verbal or written.
 5. The use of emergency lights or siren by an SA must be reported to his/her SAC or ASAC each time the equipment is activated. This notification shall be in the form of a memorandum in which the SA shall describe the circumstances surrounding the decision to activate the lights or siren. The notification must be made within 24 hours of the event.
- K.** Unless waived by the issuing authority, the driver of a Government vehicle is personally responsible for paying for any parking ticket issued to the vehicle while in the driver's control and custody.
- L.** The safe operation of a GOV in the performance of Government business is the responsibility of the agent and must be given appropriate attention at all times. Texting-while-driving by an SSA OIG special agent is only permitted as a tool of last resort in law enforcement, national security, or emergency situations when texting is the only method the agent can use to communicate.
1. Agency employees should be familiar with and comply with all Federal, state, local, and agency motor vehicle safety requirements and policies, including the agency's policy on text messaging as outlined in this policy

002.070 Surrender of Equipment

- A.** Special Agents (SA) who are suspended for any reason or placed on administrative leave (due to a pending disciplinary action) are required to surrender the following items to their supervisor prior to serving the suspension/leave:
- Special Agent Credential with badge
 - Belt badge
 - HSPD-12 badge (PIV Card),
 - Firearm
 - Government-issued vehicle
 - Passport (because passports are retained in Headquarters, the Policy and Administration Division (PAD) should be notified that the passport is not to be released if requested by the SA)
 - Office keys/access cards (if applicable)
- B.** The following items should be surrendered after discussion with the Deputy Assistant Inspector General for Investigations (DAIGI):
- Blackberry
 - Laptop
- C.** The supervisor shall conduct an inventory of the vehicle at the time of the surrender to document items in the vehicle, to include emergency lights, emergency kit, etc. The supervisor will notify PAD via the PAD Mailbox, ^OIG PAD, if the Blackberry has been surrendered and service will be suspended.
- D.** If for any reason the supervising Special Agent-in-Charge (SAC) believes that the SA should not be required to surrender any of the above items, the SAC may request, in writing, that the Assistant Inspector General for Investigations (AIGI) waive the requirement of subsection A and B above. Such request shall set forth the reasons for the waiver.
- E.** Notwithstanding subsections A and B above, if the SAC, DAIGI, AIGI, or Inspector General (IG) determines that it is in the best interests of the OIG to require an SA to surrender any of these items at any time, the SAC, DAIGI, AIGI, or IG will issue a written memorandum to that effect, and the SA must surrender these items to his or her supervisor or any OI management official.
- F.** After serving a suspension, returning from administrative leave, or surrendering these items under authority of subsections A, B, or E above, the SA shall write a memorandum to the SAC requesting the return of the specified items.

002.080 Law Enforcement Availability Pay (LEAP)

- A.** Availability pay is the 25 percent premium pay granted in the Law Enforcement Availability Pay (LEAP) Act of 1994. It is paid to ensure the “availability” of criminal investigators for unscheduled duty in excess of their 40-hour basic workweek. LEAP will be considered as part of basic pay for the computation of retirement benefits, lump sum annual leave, life insurance, and the value of subsistence and quarters where applicable.

- B.** Availability means that a criminal investigator shall be either performing official duties during unscheduled duty hours or, based on the needs of the OIG, is requested by management to be generally and reasonably accessible to perform specific official duties or assignments during unscheduled duty hours.
- C.** Criminal Investigator refers to a law enforcement officer as defined under Section 5541(3) of Title 5, United States Code, who is required to:
- 1.** Possess knowledge of investigative techniques, laws of evidence, rules of criminal procedure, and precedent court decisions concerning admissibility of evidence, constitutional rights, search and seizure, and related issues.
 - 2.** Recognize, develop, and present evidence that reconstructs events, sequences, and time elements for presentation in various legal hearings and court proceedings.
 - 3.** Demonstrate skills in applying surveillance techniques, undercover work, and advising and assisting the United States Attorney in and out of court.
 - 4.** Demonstrate the ability to apply the full range of knowledge, skills, and abilities necessary for cases that are complex and unfold over a long period.
 - 5.** Possess knowledge of criminal laws and Federal rules of procedure that apply to cases involving crimes against the United States.
 - 6.** Possess the ability to follow leads that indicate a crime will be committed rather than initiate an investigation after a crime is committed.
- D.** Unscheduled duty hours are those hours a criminal investigator works, or is determined by the agency to be available for work, which are not a part of the 40 hours in the basic workweek or not regularly scheduled.
- E.** Administrative workweek means a period of seven consecutive calendar days designated in advance by the head of an agency.
- F.** Regular workday means each day in the basic workweek during which the investigator works at least four hours that are not regularly scheduled overtime hours, unscheduled duty hours, or hours spent on approved training, travel, leave, or an excused absence with pay for relocation purposes.

002.090 Authority for LEAP

- A.** Title 5 U.S.C. § 5545a, Law Enforcement Availability Pay Act of 1994, provides that:
- (c) Each criminal investigator shall be paid availability pay as provided under this section. Availability pay shall be paid to ensure the availability of the investigator for unscheduled duty. The investigator is generally responsible for recognizing, without supervision, circumstances that require the investigator to be on duty or be available for unscheduled duty based on the needs of the agency.

- B. LEAP replaced discretionary premium pay, commonly called “Administratively Uncontrollable Overtime (AUO),” with guaranteed compensation at the rate of 25 percent. The compensation is provided in anticipation of unscheduled work that criminal investigators are expected to perform due to the nature of their work.

002.100 Eligibility for LEAP

- A. LEAP will be paid at a rate of 25 percent of basic pay to OIG criminal investigators who certify that they expect to be “available” as defined in Section 002.080B (form OI-49) ([see Exhibit 2-2](#))
- B. All OIG criminal investigators (through GS-15) are eligible to receive LEAP and are exempt from the Fair Labor Standards Act of 1938.
- C. In the event of agency ordered or approved training, relocation, travel, and annual or sick leave, the agent will continue to receive LEAP.
- D. Because criminal investigators who take Leave without Pay (LWOP) do not work a standard 40-hour workweek that week, they might become ineligible for LEAP. In order to qualify for LEAP, a criminal investigator would be required to make up the time absent on LWOP in addition to being available the excess hours. Statutory exceptions to the 40-hour workweek include only leave or absences in a paid status.
- E. Absent specific entitlement to LWOP, (see [APPM Chapter 6 Section 14](#)) criminal investigators are not entitled to take LWOP as a matter of right and such use of LWOP by criminal investigators who exceed the federal pay cap may defeat their eligibility for LEAP.
- F. Involuntary reduction in pay resulting from a denial of certification and removal from LEAP is considered an adverse personnel action. All such actions must be coordinated through the AIGI.

002.110 Rules for LEAP

- A. A criminal investigator shall continue to be paid LEAP if the annual daily average of LEAP hours is equal to or greater than 2 hours. The hours referred to are:
 - 1. The unscheduled duty hours worked by a criminal investigator in excess of each regular workday.
 - 2. The unscheduled duty hours a criminal investigator remained available to work on each regular workday at the request of OIG management. (**NOTE:** Time spent during unscheduled work hours when the criminal investigator is merely available to work, but not specifically directed to remain available by OIG management, shall not be counted to fulfill LEAP requirements.)
- B. Compensation, either by pay or compensatory time off, for unscheduled duty hours worked over the annual daily average is not authorized.

- C. An agent who is requested by management to be available for duty during unscheduled duty hours is not required to remain in the office or at home, but must be reachable either by telephone, email, or blackberry.
- D. If the unscheduled duty hours worked by an agent on a semiannual average do not appear to allow the agent to meet the annual daily average requirement, the supervisor will examine the workload requirements of the SA and adjust the distribution of work within the particular office.
- E. Criminal investigators are generally responsible for recognizing, without supervision, circumstances that require the criminal investigator to work beyond the regular workday. Managers are responsible for determining when criminal investigators are to be available for unscheduled duty due to specific needs.
- F. OIG agents normally will not be assigned regularly scheduled overtime; however, they will be assigned tasks (investigations, surveys, administrative assignments) that will likely require unscheduled duty.
- G. The recording of unscheduled duty hours for annual LEAP purposes will be accomplished by the completion of the SA's National Investigative Case Management System (NICMS) time module ([Exhibit 2-3](#)). OIG supervisory personnel are responsible for ensuring that agents' reports of hours of unscheduled duty hours worked or available are accurate.

002.120 LEAP Reporting Requirements

- A. Completion of the NICMS time module is the only reporting requirement for SA personnel regarding hours worked for LEAP.
- B. The SAC will certify to the DAIGI each year within 30 days after the end of Pay Period 26 that all criminal investigators met the requirements for LEAP. Form OI-50 is used to authorize the continued payment of LEAP to the agent. A sample certification is shown as [Exhibit 2-4](#).
- C. Review:
 1. To ensure that each SA maintains qualification for LEAP, an annual audit will be done by a DAIGI or other individual designated by the AIGI.
 2. Because the annual audit of an individual's qualification for LEAP is "after the fact," it may show that the employee did not meet the required daily 2-hour average minimum of unscheduled duty per week for that period. The individual should be advised that they are in danger of not meeting the annual qualification for LEAP. The first-line supervisor and the employee are responsible for establishing a course of action to ensure that the individual will meet the annual qualification.

002.130 Tracking Work Hours

- A. The NICMS time module ([Exhibit 2-3](#)) is designed to capture work hours for all personnel, and must be submitted no later than ten days after the close of the pay period.
- B. Supervisors will review and approve the reports submitted by subordinate employees.

C. Preparation of individual reports:

1. Entries on the NICMS time module are made electronically. The reporting period corresponds to official pay periods.
2. Time reported under the various categories is rounded up or down, as appropriate, to the nearest one-half hour.
3. Time actually spent traveling outside the regular workday or basic workweek may be claimed as unscheduled duty hours. The time actually spent traveling is charged to the activity to which the travel is associated. Time spent traveling to and from work during a regular day commute may not be counted as unscheduled duty hours.
4. A base workday reduction is any day on which an agent took four hours or more of leave, received four hours or more of training, spent four hours or more traveling for official business, or any legal public holiday designated by the Federal Government. If no reduction is taken under the above description, LEAP may be earned for that day, even if the SA took leave and/or participated in training.

002.140 **Opting Out of Law Enforcement Availability Pay and the Part-Time Agent Program**

- A. If, for personal hardship reasons, an agent finds it necessary to work fewer hours, the agent may request to opt out of the LEAP program. In order to do so, the agent must submit a written request to his/her SAC explaining the existing circumstances that make it necessary to work a reduced work schedule. The request must state a specific period of time for which relief of LEAP requirements is being sought. The maximum length of time for which relief may be sought is 6 months. If additional time is needed, the agent must apply for the *Special Agent Part-Time Employment Program* ([Exhibit 2-5](#)). The SAC will forward the request, along with recommendations, to the appropriate DAIGI.
- B. Requests to opt out of LEAP are reviewed by the appropriate DAIGI. The DAIGI makes a recommendation as to what action should be taken. The AIGI has the final authority to either approve or disapprove the request.
- C. If approved, the request is forwarded to the OIG Office of Communications and Resource Management (OCRM). OCRM will process a Notification of Personnel Action, Form SF-50, for discontinuance of availability pay. If not approved, the DAIGI will notify the employee's SAC of the decision. In either event, the DAIGI will provide written notification to the employee through the employee's SAC.

002.150 **Media Relations**

- A. Contact with Local Media
 1. The AIGI or his/her designee, in consultation with the Assistant Inspector General for Communications and Resource Management (CRM), is responsible for all matters

involving OI's contact with the media, such as newspapers, television and radio stations, and online entities, to share or explain investigation outcomes, audit findings and recommendations, and other OIG initiatives and/or accomplishments.

2. Only SACs are authorized to speak on behalf of the OIG in their respective regions. At the SAC's discretion, this authority may be delegated to ASACs/RACs.
3. SACs or their designee(s) should coordinate with their Deputy AIGI and the OIG Communications Director, Division of Communications, on all media matters. This includes:
 - a. immediately notifying their Deputy AIGI and the OIG Communications Director of media contacts and requests—if the OIG Communications Director is not available, the AIGCRM should be notified;
 - b. consulting with their Deputy AIGI and the OIG Communications Director before releasing information to the media that may generate significant media coverage or draw significant attention to the agency;
 - c. consulting with their Deputy AIGI and the OIG Communications Director before taking proactive measures to publicize the results of their FD's work, or before coordinating local media activities with SSA's Regional Public Affairs Officer (RPAO); and
 - d. consulting with their Deputy AIGI and the OIG Communications Director to determine whether OIG information may be released to the media under applicable statutes, regulations, and policies pertaining to the disclosure of information.
4. After consulting with their Deputy AIGI and the OIG Communications Director, SACs or their designee(s) should only speak to the local media about the OIG in general terms, and should refrain from discussing OIG policy and procedures. SACs must not disclose or release any information regarding any open/active OIG investigation without prior approval of the AIGI and the OIG Communications Director.
5. Following any interaction with local media, SACs must provide a summary of the interaction to their Deputy AIGI and the OIG Communications Director, via email.
6. SACs or their designee(s) must coordinate with their Deputy AIGI and the OIG Communications Director when preparing **written** responses to media inquiries.
7. SACs or their designee(s) must **immediately** report significant arrests or incidents in their respective FDs, which could lead to nationwide publicity or media inquiries, to their Deputy AIGI, the OIG Communications Director, and the RPAO.
8. SACs or their designee(s) should provide to the RPAO all fact sheets that are of local or regional interest.

B. Formal Interview Requests

1. Requests by local or national media for formal interviews to discuss OIG work results must be coordinated in advance through their respective Deputy AIGI, who will coordinate with

the OIG Communications Director. The Inspector General and Deputy Inspector General, in coordination with the AIGI, the OIG Communications Director, and the AIGCRM will decide whether the OIG will accept requests for formal interviews.

2. The OIG Communications Director will coordinate all formal interviews, after consultation with the AIGI/Deputy AIGI, to prepare the interviewee, identify any subject-matter restrictions, and to determine ground rules for the interviews.
3. Only SACs and, if delegated by the SAC, ASACs/RACs are authorized to participate in on-camera interviews.
4. Unscheduled, spontaneous interviews, such as those outside a hearing or at a public meeting, should be avoided. Instead, media representatives should be referred to the OIG Communications Director, and/or the appropriate United States Attorney's Office (USAO). If this is not feasible, alert your Deputy AIGI and the OIG Communications Director, immediately following the interview.

C. Media Coverage Affecting the OIG

1. SACs should ensure that relevant news articles, photographs and/or radio/television stories involving significant matters are promptly forwarded to the OIG Communications Director, and/or to the Division of Communications by email at oig.oer@ssa.gov, fax at (410) 597-0821, or via postal mail at the following address:

OIG Division of Communications
Room 3-ME-4
6401 Security Boulevard
Baltimore, MD 21235

D. Coordination with U.S. Attorney's Offices

2. To the extent possible, SACs should coordinate with the USAO on any USAO press release involving an OIG case. The OIG Communications Director is available to assist with SAC quotes for inclusion in press releases, at the FD's request.
3. When a USAO issues such a press release, SACs or their designee will immediately provide a copy to OI's Criminal Investigations Division and the OIG Communications Director via oig.oer@ssa.gov or fax at (410) 597-0821.

E. General Guidelines for Releasing Information

In general, information about OIG investigations may be released externally **only** after an arrest has been made or an indictment returned. Premature release of information could interfere with the success of an investigation and any subsequent judicial action, and may violate the *Privacy Act*.

Before releasing any information, SACs should consult with the AIGI or his/her designee and the OIG Communications Director.

Under no circumstances should **any** OI employee make public statements concerning:

1. Personal opinion about any subject or investigation.
2. Speculation about sources of information.
3. Exaggerated facts or statistics.
4. Any undercover agent or the office to which the agent is assigned.
5. An informant's identity.
6. Advance notice of contemplated arrests or other law enforcement actions.
7. Pending investigations or the names of persons involved in pending investigations.
8. Ongoing or potential investigative methodology.
9. A defendant's character or prior criminal history.
10. A defendant's statements, admissions, confessions, alibis, or the refusal or failure to make a statement.
11. Investigative procedures such as handwritten examinations, fingerprints, polygraph examinations, laboratory tests, or a refusal by a defendant to submit to such tests or examinations.
12. Witnesses' identity, testimony, or credibility.
13. Evidence or arguments in any judicial proceeding, whether or not it is anticipated that such evidence or arguments will be used.
14. Speculation as to a defendant's guilt, the possibility of a guilty plea, or the possibility of a plea to a lesser offense.
15. Any attempt to influence the outcome of a judicial proceeding.

NOTE: The preceding list may not be comprehensive. If an OI employee wishes to release information that is not specified above, he or she **must** receive prior approval from the AIGI or his/her designee and the OIG Communications Director.

In addition, under no circumstances should any OI employee:

1. Assist news media in photographing or televising a defendant or accused person being transported or held in Federal custody.
2. Make available photographs of a defendant unless releasing the photograph serves a law enforcement function.

3. Permit a media representative to accompany OIG employees on official investigations.
4. Furnish media representatives with material from official files without prior approval of the AIGI or his/her designee and the OIG Communications Director.

002.160 Disclosure of Information

- A. Information in the possession of OI will be disclosed only as authorized by law and regulation.
- B. OI personnel in possession of confidential information are responsible for protecting such information from unauthorized disclosure.
- C. Additional instructions regarding the disclosure of information are located in Chapter 6 (006.020–SSA Record Access and Disclosure), Chapter 11 (011.040 – Release to PAO), and Chapter 19 (019.000 – Freedom of Information Act – General) of this *Handbook*, and in Chapter 5-15 of the *OIG Administrative Policies and Procedures Manual* (Use and Disclosure of SSA Data).

002.170 Congressional Inquiries

- A. All congressional letters addressed to OIG, or forwarded to OIG by SSA or other agencies, will be referred to the Office of External Relations (OER). OER is responsible for maintaining logs of congressional correspondence, and for all necessary coordination to ensure that a timely response is made on behalf of OIG. If a congressional inquiry is received at the Allegation Management and Fugitive Enforcement Division or in an FD, it should be electronically forwarded to OER, with a copy to OI HQ before any action is taken. You will be notified if the original documentation is needed.
- B. Congressional Inquiry Procedures
 1. OER is responsible for preparing all responses to congressional inquiries.
 2. If the inquiry contains an allegation of fraud, OER will consult with OI HQ with regard to the appropriate action. Once a response letter has been sent, OER will send the entire congressional package to OI HQ for disposition. OI HQ will forward the package to the appropriate FD SAC.
 3. FD will:
 - log the information into NICMS as an allegation, noting the entry as a congressional inquiry;
 - take appropriate action in accordance with the IG’s letter to the Congressperson; and
 - notify OI HQ within two weeks of the disposition of the congressional inquiry, including the NICMS allegation number and case number, if applicable.
 4. If a congressional office sends a follow-up letter requesting a status, OER will request information from OI HQ for the purpose of drafting an appropriate response.

Chapter 2 — **EXHIBITS**

[2-1 — Certification for Home-to-Work Use of Official Government Vehicles \(OI-46\)](#)

[2-2 — Availability Pay Certification \(OI-49\)](#)

[2-3 — NICMS Time Module](#)

[2-4 — Annual Certification of Availability Hours \(OI-50\)](#)

[2-5 — Special Agent Part-time Employment Program](#)

Office of the Inspector General
Office of Investigations
Social Security Administration

**CERTIFICATION FOR HOME-TO-WORK
USE OF OFFICIAL GOVERNMENT VEHICLES**

EMPLOYEE INFORMATION:

Name: _____ Position/Title: _____

Home Address: _____

FOR THE PERIOD: _____ **TO** _____
(Starting Date) (Ending Date)

I am familiar with the SSA OIG Official Government Vehicle Home-to-Work policy and will follow the procedures and requirements as listed in Chapter 2, section 002.060 of the *Special Agent Handbook*, Use of Official Vehicles.

I understand that I must be re-certified if there is a change in my duty assignment or residence. I understand this certification may be withdrawn at the discretion of the Special Agent-in-Charge, the Assistant Inspector General for Investigations, or a Deputy Assistant Inspector General for Investigations.

(Signature of Employee)

(Date)

CERTIFICATION:

I certify that this home-to-work use is necessary for the safe and efficient performance of criminal law enforcement duties in accordance with Chapter 2, Section 002.060, Use of Official Vehicles, as outlined in the SSA OIG OI *Special Agent Handbook*.

(Signature of Special Agent-in-Charge,
Assistant Inspector General for Investigations, or
Deputy Assistant Inspector General for Investigations)

(Date)



Memorandum

To: Assistant Inspector General for Investigations

From:

Subject: Availability Pay

I, Special Agent _____, certify that I expect to be able to perform official duties during unscheduled duty hours and agree to be available for unscheduled duty based on the needs of the Office of the Inspector General, Social Security Administration.

Special Agent _____
(Print Name)

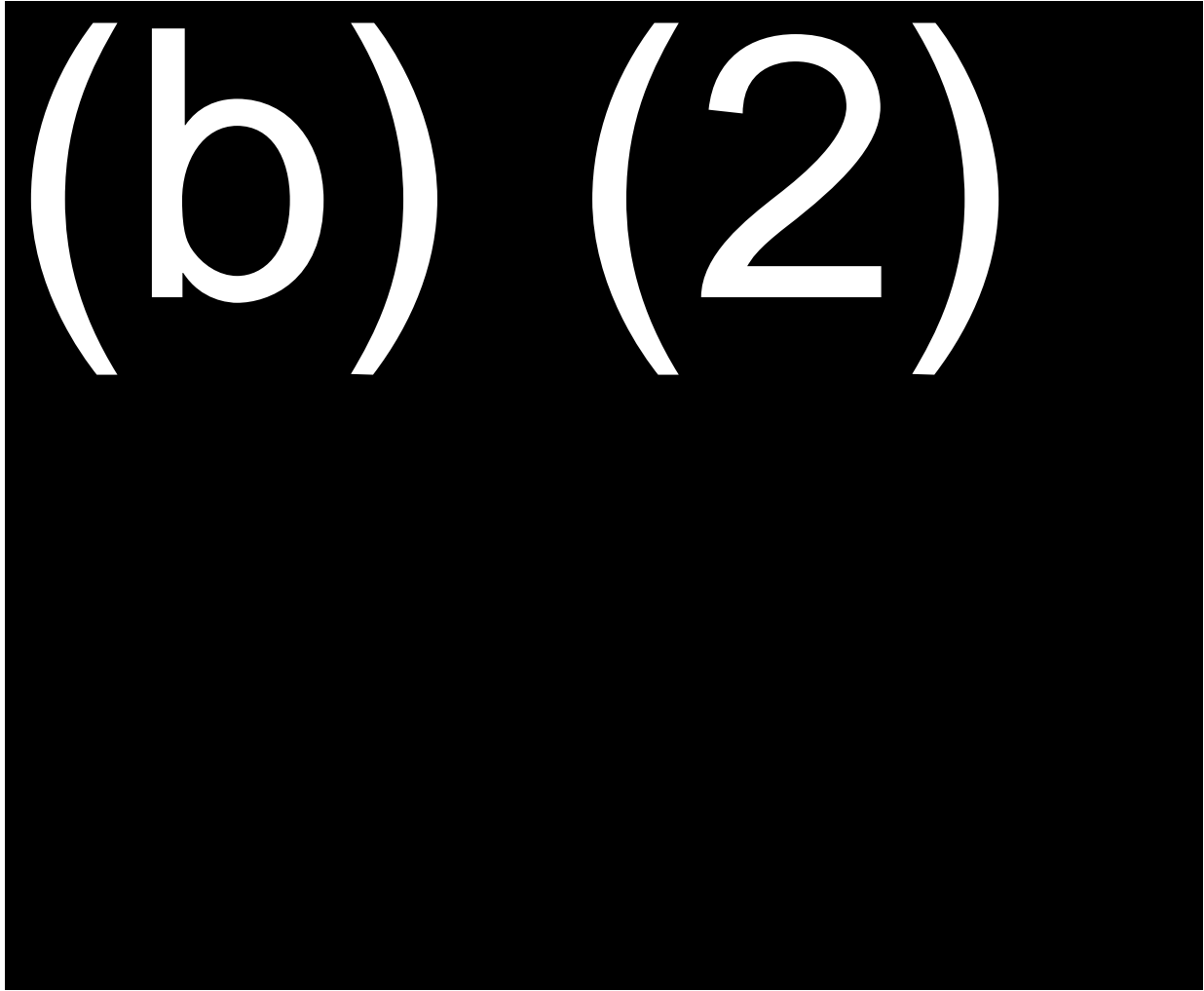
(Signature)

(Date)

Concur: _____
Special Agent-in-Charge

Date: _____

Exhibit 2-3





MEMORANDUM

Date: ENTER INFO

Refer To: SAH 002.120

To: Deputy Assistant Inspector General
for Investigations

From: Special Agent-in-Charge

Subject: Annual Certification of Availability Hours

The personnel listed below performed official duties during this past year during unscheduled hours of duty or were available to perform work during unscheduled hours of duty and are qualified for availability pay in accordance with the Law Enforcement Availability Pay Act of 1994 (Section 633 of Public Law 103-329, 5 U.S.C. § 5545a).

By this report, I certify the agents listed were under my supervision during this reporting period, and in accordance with requirements of their official duties, performed work during unscheduled hours of duty, and qualify for availability pay. I also certify that the Special Agents listed below are expected to continue to meet these requirements:



Special Agent Part-time Employment Program

Purpose

In response to the needs of Special Agents for additional workplace options, the Office of Investigations (OI) has established a Special Agent Part-time Employment Program (SAPTEP). This program is designed to assist in the accommodation of Special Agents who are experiencing a temporary personal situation or hardship that is severely impacting their ability to fulfill the obligations of full-time employment and may require them to resign to manage the situation. The program enables agents to continue their employment with OI part-time, while empowering them to deal with personal situations such as child care, elder care, death, or illness.

Eligibility Requirements

To qualify for SAPTEP, a Special Agent must:

1. Have demonstrated a personal situation or hardship such as child care, elder care, death, or illness that is severely impacting their ability to fulfill the obligations of full-time employment and may require them to resign to manage the situation.
2. Have completed at least 3 years and 120 days as a Special Agent with OI and have career status.
3. Be at the GS-13 grade level or below.
4. Have received an "Acceptable" performance rating for the past year.
5. Be assigned to an office or division that qualifies for this program, as determined by the needs of the OIG at the time of the request.
6. Sign a part-time employment work agreement stipulating the conditions of SAPTEP (see attached).

Procedures for Application

Participation in the SAPTEP program is voluntary. Requests to participate in the program should be stated in a memorandum and forwarded through the Special Agent's SAC to the appropriate DAIGI.

The memorandum must state the reason for seeking entry into the program, the proposed schedule, and the number of hours per week the agent intends to work. The applicant's SAC will consider the request in light of the agent's personal circumstances, career phase, and the operational needs of the office. Modifications to the agent's proposed schedule shall be agreed upon by the agent and the SAC. The SAC will forward his/her recommendation and the memorandum to the DAIGI overseeing his or her division. The DAIGI will then forward his/her decision to the Assistant Inspector General for Investigations (AIGI). If a request is denied, the AIGI will respond in writing detailing the specific reasons for the

Exhibit 2-5

denial, and, if applicable, will attempt to provide alternative solutions. Special Agents may challenge denials through established OIG grievance/EEO procedures. Questions regarding these procedures should be directed to the Office of Communications and Resource Management (OCRM).

It is important to note that the SAPTEP is designed to incorporate the needs of Special Agents while meeting the demands of the OIG's investigative and protective responsibilities. All requests may be influenced by the availability of funds and resources, or by changes in our protective and/or investigative responsibilities and the needs of the OIG.

Legal Authority

Office of Personnel Management (OPM) regulations governing law enforcement availability pay generally provide that “an employing agency may, at its discretion, approve a criminal investigator's voluntary request that the investigator generally be assigned no overtime work (including unscheduled duty) for a designated period of time because of a personal or family hardship situation.” 5 C.F.R. § 550.182(f). The parameters of SAPTEP may be set at the discretion of the employing agency; the regulation only requires that “[t]he investigator must sign a written statement documenting this request and his or her understanding that availability pay will not be payable during the designated period.” Id.

While employing agencies are given broad discretion in designing a SAPTEP program, the OPM has advised:

This voluntary opt-out provision is intended to apply to situations where the expected duration of the designated period is long enough that the investigator would likely be unable to satisfy the annual average hours requirement. Agencies are expected to monitor closely the use of this authority to ensure that investigators are not allowed to opt out of availability pay for long periods of time, only to opt back in at the end of a career as a way of inappropriately inflating the average salary used in the retirement annuity computation. 59 FR 66149 (Dec. 23, 1994).

Administration of SAPTEP

Length of Participation

Special Agents will initially be approved to participate in this program for up to a one-year period, renewable up to one-year increments, for a maximum career total of five years. For example, a Special Agent may enter the program for two years, return to full-time employment, and then reenter the program later. Each one-year renewal requires certification/approval by the agent's SAC and a DAIGI.

When an employee returns to full-time status, his/her office must submit an SF 52 documenting that action. The immediate supervisor must also certify the employee's availability for unscheduled duty to allow payment of Law Enforcement Availability Pay (LEAP).

Part-time Schedule

Part-time Special Agents must work not less than 16 hours or more than 32 hours a week.

The part-time agent and his/her supervisor must establish a set schedule for the number of hours and days to be worked each week.

Exhibit 2-5

An SF 52 will be completed and forwarded to OCRM along with a copy of the part-time employment agreement that states the employee acknowledges he/she is not eligible to participate in LEAP. The SF 52 will reflect the change in status of the Special Agent from full-time to part-time and the number of hours per day and days of the week to be worked. Additionally, any requests for changes to the number of hours to be worked in a pay period must be submitted in advance to the supervisor to ensure that the part-time agent is afforded the proper pay, leave accruals, and other benefits associated with work hours. A new SF 52 must be prepared to reflect any change in the number of hours to be worked.

It is important for supervisors to note when establishing schedules that many Federal holidays fall on Mondays.

Complete instructions for posting time and attendance hours for a part-time employee can be found in the SSA Time and Attendance Manual.

Transfer Policy

Participation in the SAPTEP does not exempt the agent from the OIG transfer policy. Additionally, agents seeking accommodation through the SAPTEP may be offered the opportunity to transfer if it would be difficult for their current office to accommodate a part-time agent position. Refusal to accept an offer of transfer may result in an agent being unable to enter the SAPTEP.

Promotions

Part-time agents may participate in the Merit Promotion Plan for GS/GM-1811. Agents must discontinue part-time schedule to advance beyond the GS-13 level.

Assignments

Due to the nature of part-time employment, certain work assignment limitations may be placed on the part-time Special Agent. Sound management practice dictates that part-time agents receive case and administrative work that does not require the agent to work full-time to achieve successful completion.

Supervisors must exercise sound judgment, creativity, and resourcefulness in assigning work to part-time agents.

Part-time agents will be required to meet the same firearms qualification and physical fitness assessment standards that full-time agents are required to fulfill.

Part-time agents will not be assigned a government vehicle for home-to-work driving.

Travel

Part-time agents generally will not travel. Staffing situations may, however, warrant that a part-time agent travel to fulfill mission requirements. Further, a part-time agent's schedule may include scheduled travel that meets the needs of the OIG and the Special Agent's part-time requirements.

Performance Appraisals

Part-time Special Agents will be issued a performance plan consistent with their assigned duties and will be evaluated according to the current performance appraisal process.

Exhibit 2-5

Outside Employment

If a part-time agent wants to engage in certain permitted outside activities as outlined in the OIG Administrative Procedures Manual, he/she must obtain written permission from the AIGI and the AIG OCRM.

Compensation and Benefits

Pay

Part-time Special Agents will be paid on an hourly basis computed at the hourly rate for their grade and step. Part-time Special Agents will continue to receive any applicable geographic pay rate and special pay adjustment for law enforcement officers.

Part-time Special Agents will be required to sign a part-time employment agreement. By signing this agreement, the part-time agent is also confirming that he/she understands that LEAP will not be payable during the time he/she works part-time. When the part-time agent returns to full-time status, the agent's supervisor must ensure that the agent is again certified to receive LEAP.

Part-time agents are eligible for night differential pay for any portion of their scheduled tour of duty that occurs between 6:00 p.m. and 6:00 a.m. 5 CFR 550.121. Part-time agents are also eligible for holiday pay if the holiday falls on a regularly scheduled workday. 5 CFR 550.131. Part-time agents are not eligible for Sunday premium pay due to Federal employment regulations. 5 CFR 550.171(a).

Within Grades

Part-time agents are eligible to receive a within grade increase if they meet all requirements. Because within-grade waiting periods are based on calendar weeks, not hours worked, the waiting period is not affected. See 5 C.F.R. 531.405.

Overtime

Part-time agents should not be scheduled to work more than 32 hours per week or 64 hours per pay period. If on an occasional and irregular basis, a particular assignment (e.g., court appearance, trial preparation, etc.) requires the part-time agent to work more hours than he/she is normally scheduled for, appropriate compensation will be allowed. Part-time agents may be entitled to receive overtime pay under the Fair Labor Standard Acts (FLSA) and Title 5, U.S. Code for hours worked in excess of eight hours a day, or 40 hours per week.

Hours worked in addition to the part-time agents regular schedule must be mutually agreed upon between the agent and his/her supervisor. Increases in weekly work hours may not continue for longer than two consecutive pay periods.

Retirement

Part-time Special Agents will accrue prorated retirement credit under the Civil Service Retirement System (CSRS) and the Federal Employees Retirement System (FERS). Part-time employment will not affect an agents retirement eligibility, only the computation of his/her annuity. See 5 USCS §§ 8339(p), 8415(e).

Thrift Savings Plan

Exhibit 2-5

Part-time Special Agents may contribute to the Thrift Savings Plan under the same rules as full-time agents. There is no difference in ability to contribute to TSP between full-time and part-time employees. Contributions are based on actual earnings.

Health Insurance

SAPTEP agents are eligible to continue participation in the Federal Employees Health Benefits Program (FEHBP); however, the government's contribution to the employee's premium is reduced in direct proportion to the number of hours worked. Part-time agents will be required to pay the regular full-time employee premium plus that part of the government's share remaining after the reduction.

Life Insurance

Part-time Special Agents are eligible to continue their enrollment in the Federal Employees' Group Life Insurance (FEGLI) Program. The government's contribution to the life insurance premium is the same for part-time agents as for full-time agents. The amount of the life insurance coverage is based on the part-time salary.

Leave Accrual

Part-time Special Agents accrue annual leave according to their length of Federal service. Annual Leave (A/L) is earned as follows: 1 to 3 years of service earns one 1 hour A/L for every 20 hours in a pay status, 3 to 15 years of service earns 1 hour A/L for every 13 hours in a pay status, and 15 or more years of service earns 1 hour A/L for every 10 hours in a pay status. 5 CFR 630.303 A part-time employee may accumulate not more than 240 or 360 hours' annual leave on the same basis that a full-time employee may accumulate not more than 30 or 45 days' annual leave. 5 CFR 630.304.

A part-time employee earns 1 hour of sick leave for every 20 hours in a pay status. 5 CFR 630.406

For specific information regarding an employee's benefits, he/she should contact OCRM.

Exhibit 2-5

Sample Special Agent Part-time Employment Program Work Agreement

UNITED STATES GOVERNMENT

memorandum

DATE:

TO: DAIGI

FROM: (Name of Agent)

SUBJECT: Request for Part-time Employment

The following constitutes an agreement between:

**the Office of the Inspector General of the Social Security Administration and _____
of the terms and conditions of the Special Agent Part-time Employment Program (SAPTEP).**

Employee volunteers to participate in the SAPTEP and agrees to adhere to the applicable guidelines and policies.

Employee agrees to participate in the SAPTEP for a period not to exceed one year beginning _____ and ending _____.

Employee's official days of duty will routinely be _____.

Employee's official hours of duty will routinely be _____.

Employee understands that his/her work schedule may be adjusted to meet the needs of the OIG.

Employee understands that an SF-52, Request for Personnel Action, will be submitted to initiate participation in the SAPTEP, to change the part-time work schedule or hours, and/or to terminate participation in the SAPTEP.

Employee understands that to be eligible to participate and remain in the SAPTEP, his/her most recent performance rating of record must be "Acceptable."

Sample Special Agent Part-time Employment Program Work Agreement

Employee understands that his/her part-time salary will be computed based on his/her work schedule and the hourly rate for his/her grade and step.

Employee understands by signing this agreement, he/she also confirms that he/she understands the Law Enforcement Availability Pay (LEAP) will not be payable while in a part-time status.

Employee understands that he/she will not be assigned a government vehicle for home-to-work driving.

Exhibit 2-5

Employee must discontinue part-time schedule to advance beyond the GS-13 level.

Employee understands that he/she will be required to meet the same firearms qualification and physical fitness assessment standards that full-time special agents are required to fulfill.

Employee understands that he/she will not be eligible for Sunday premium pay.

Employee understands that he/she will accrue prorated retirement credit under the Civil Service Retirement System (CSRS) or the Federal Employees Retirement System (FERS).

Employee understands that the government's contribution to the health benefits premium is reduced and is based on the actual number of hours worked and that the employee must pay the difference.

Employee understands that the amount of his/her life insurance coverage is based on his/her part-time salary.

Employee understands that his/her annual and sick leave accrual rate are reduced due to his/her part-time status.

Employee Signature

Date

The OIG concurs with the employee's participation and agrees to adhere to the applicable guidelines and policies.

Special Agent-in-Charge

Date

Deputy Assistant Inspector General for Investigations

Date

CASE MANAGEMENT

003.000 General

- A.** The ability to manage information is essential to the success of any organization. Within the Office of Investigations (OI), two types of information are collected and stored: administrative and investigative. Standardized management of information assures that the information is available to anyone within OI who has a legitimate need for the material. All employees share in the responsibility of handling information that comes into their possession as part of their official duties. For the purposes of this chapter, information is classified as either part of the case management process or as administrative files.
- B.** The case management process tracks the workload of field divisions (FD) and individual Special Agents (SA). It assists in the making of informed judgments on resource allocation, program vulnerabilities, and general management oversight. The system is also designed to provide statistical information for reports to the Inspector General, the Commissioner of the Social Security Administration (SSA), and the Congress, and for other reports as necessary.
- C.** Administrative files are established to store information of a general nature relating to policies, procedures, and correspondence to or from SSA Office of the Inspector General (OIG). Administrative file management is discussed further in [Chapter 23](#) of this handbook.

003.010 Policy

- 1.** Referrals and complaint information shall be analyzed and processed, sources acknowledged, and case opening determinations made in a thorough and expeditious manner.
- 2.** Management information shall be accurately and regularly reported, and entered into National Investigative Case Management System (NICMS).
- 3.** Actions shall occur as necessary to ensure proper and timely disposition of the case.
- 4.** Cases are not to be closed until all legal action, other than CMP, has been taken and properly documented in the case file. Cases involving potential administrative action against SSA employees shall be closed after the information is reported to SSA, and SSA reports back to OIG with a description of the administrative action taken against the employee.
- 5.** Allegations containing an element of child abuse shall be reported to an agency specifically designated by the Attorney General as authorized to conduct these types of investigations in accordance with the provisions of the *Victims of Child Abuse Act of 1990*. Failure to comply

with the law's provisions can result in criminal charges. Questions about this Act or the names of specifically designated agencies should be directed to the Office of Counsel to the Inspector General (OCIG).

003.020 Receipt of Allegations from SSA

All information concerning potential wrongdoing involving SSA programs, employees, or operations that is received by an SSA OIG component will be accounted for in the SSA OIG NICMS.

- A.** OIG and SSA Operations developed a system for reporting allegations electronically. That system is referred to as the electronic 8551 (e-8551) form and referral process. The process is as follows:
- 1.** The e-8551 is available on the SSA Intranet. This form is filled out online and electronically submitted to the OIG's Office of Communication and Resource Management (OCRM), Division of Systems Support, Software Development and Support Staff, where it is uploaded into NICMS. An allegation number is assigned to the allegation.
 - 2.** The allegations are then routed to the appropriate OIG OI office based on the subject's zip code or state code (where the zip code is absent). The allegation will appear on the OI office's ASAC or RAC's NICMS "To Do" list.
 - 3.** Weekly, updated agreed upon allegation information is sent to the SSA Fraud Information Tracking System (FITS). In addition, if the allegation is closed or if a case is opened, an automated email is sent to the email address listed on the E8551 referral (provided that the address is a valid SSA email address) advising the submitter of the action.
 - 4.** If a case is opened, at the case closing, agreed upon case information is provided to SSA FITS.
- B.** Reports of potential violations are made to the servicing OI FD with jurisdiction over the investigation. A list of OI FD offices and areas of responsibility can be found in the SSA Program Operations Manual System (POMS), GN 04124.010. Reports are made as soon as possible after SSA obtains sufficient evidence to support an allegation or suspicion, but not longer than 30 days after the situation is discovered.
- C.** All reports of potential violations from SSA offices to OI FDs are made using the electronic version of Form SSA-8551. If an electronic version of the form is not available, the paper form SSA-8551 may be used as a temporary substitute. All allegations, however, *must* be in electronic e-8551 form in the least amount of time practical. SSA will refer to GN 04111.065 for instructions on completing paper form SSA-8551. Instructions for the electronic versions will be documented with the form.
- NOTE:** The e-8551 should never be used to forward an allegation that was originally received by SSA from the OIG Fraud Hotline. SSA should forward such allegations to the OI FD by fax, e-mail, inter-office mail, or regular mail.
- D.** Procedures followed by SSA Field Offices
- 1.** After developing enough evidence to substantiate the allegation or suspicion, the FO reports the potential violation to an OI FD using the Form SSA-8551 template if electronic version is

available, or the paper SSA-8551. If using the electronic version, any attachments may be separately forwarded to OI FD (see GN 04111.060 for instructions on how to establish an integrity file).

2. The SSA FO holds all evidence and other allegation material for 30 days pending OI FD's response. If no response has been made within 30 days, a follow-up request may be made to the OI FD to which it was referred.

3. (b) (7)(E) [REDACTED]
[REDACTED] A field office employee's name and telephone number should be given.

4. The SSA FO is instructed not to delay payment adjustment (suspension or termination) pending OI FD's response.
5. SSA National 1-800# Teleservice Center (TSC) representatives are instructed to document fraud allegations on the electronic 8551 (e-8551) form for any caller who refuses to contact the SSA OIG Fraud Hotline.
6. TSC personnel can not perform development of allegations they receive via the 1-800#, and there is no mechanism for them to forward the e-8551 directly to another SSA office. Furthermore, TSC personnel do not establish temporary "program integrity files."

NOTE: SSA National 1-800# operators are instructed, in TSC Operating Guide (OG) Section TC 31001.110 – Problems with the Use of SSN, Subsection B. Reports of Fraud and/or Misuse Involving SSNs, to refer the following to the Federal Trade Commission (FTC):

- concerns about protecting his/her personal information; and
 - allegations of identity theft, such as using another person's SSN to obtain false credit, credit cards, or other goods or services.
7. Allegations referred by 1-800# personnel can be identified by the notation in "Section I C. Position Title" of the e-8551 referral. TSC representatives are required to complete this section in the following manner: **"800# Operator."**
 8. Callers are advised that the information will be forwarded to the SSA Office of the Inspector General for evaluation and any necessary action deemed appropriate.
 9. TSCOG instructions further state that the OIG will contact the appropriate SSA Field Office/Program Service Center (FO/PSC) for necessary action.

E. OI FD accepts the allegation and opens a criminal investigation:

1. OI FD will send a notice of case opening to SSA within 45 days of referral. Upon receipt of OI FD's notice, SSA will:
 - a. remove the violations material from the holding file and forward to OIG annotated with the case number; and

- b. complete any pending adjudicative and post-adjudicative actions in consultation with the OIG Special Agent.
 - c. If further development is needed, the OI FD may contact the FO. Otherwise, the OI FD will notify the FO of the disposition of the referral when the case is closed.
- F. How SSA Handles Non-Routine Requests for Assistance from the Office of Investigations Field Division (OI FD)

SSA Field Offices - If the OI FD requests assistance or information in connection with a fraud investigation that may endanger SSA employees, cause a public relations problem, or is otherwise unusual, SSA will immediately telephone the CSI in their region for guidance in handling the request.

G. How Employees Report SSA Employee Criminal Violations

1. Non-management employees of SSA are instructed to report allegations of fraud involving SSA employees directly to the OIG by telephoning the nearest OI field division (OI FD) office or the SSA OIG Fraud Hotline at 1-800-269-0271. SSA employees may remain anonymous. See POMS GN 04112.015 for details.
2. Management employees of SSA are instructed to report allegations of fraud involving SSA employees by using the manager's only electronic fraud reporting form e8551 available from SSA's Fraud Information Tracking System (FITS). After an employee fraud allegation e8551 is submitted, the manager will receive online confirmation of the referral. Additionally, FITS will send an email to the submitting manager's personal mailbox within 24-48 hours.
3. It is permissible for SSA to gather additional information, (b) (7)(E)

- H.** The OI FD will evaluate reports of potential violations received from SSA offices to determine if criminal, civil, and/or administrative remedies are appropriate. The OI FD will either accept the allegation and open a criminal investigation or decline to open a criminal investigation. In either case, the SSA reporting office will be notified, via an automated email, of the FD's decision provided that a valid email address was provided by the SSA on the e8551 at the time of submission.

003.030 Divisional Responsibilities

- A.** Upon receipt, all allegations will be examined by the OI FD to determine suitability for investigation.
- B.** If the allegation was received via e-8551 or from the Hotline, an allegation number will have already been established in NICMS. The OI FD should access the existing allegation number in NICMS and either close the allegation or convert the allegation into an open case.
- C.** To open a case from an allegation in NICMS:

1. On the NICMS menu screen, do a General Search, then an Allegation Search, under Advanced Search options. View Allegation.
 2. After viewing the allegation in NICMS, use the Case Creation Screen to create a case from an allegation.
 3. NICMS will generate a case number.
- D.** To close an allegation in NICMS: On the NICMS menu screen, enter the closing date and close the allegation.
- E.** See chapters 4 and 8 of the NICMS Reference Manual for more detailed NICMS instructions.
- F.** If an allegation becomes an investigation, the information will be reflected on a NICMS Case Opening Report, Form OI-1, and Additional Subjects/Victims/Alias Data, Form OI-1A. The case opening system procedures are discussed beginning in Section 003.050. The FD enters that information into NICMS.
- G.** If the allegation was received directly from the complainant, the FD shall enter information into NICMS if the allegation is not to become an investigation.

003.040 Hotline and Field Division Responsibilities

- A.** Allegations received by Headquarters (HQ).
1. Allegations received by correspondence and telephone, including all allegations received directly by the OIG, will be entered into NICMS if the allegation involves SSA programs. The Office of Communications and Resource Management's (OCRM) Allegation Management and Fugitive Enforcement Division (AMFED) staff, under the guidance of the AMFED Director, will review the allegations. Allegations received by AMFED that require disposition will be handled as outlined below:
 - a. Referred directly to the OI FD or other OIG component. AMFED will electronically forward all allegations to the OI FD or other component via NICMS.
 - b. Referred directly to the suitable SSA field component, Regional Commissioner's Office, CSI, or the Office of Disability Adjudication and Review (ODAR) for further development or appropriate action. AMFED will electronically forward all allegations to SSA components via NICMS.
 - c. Referred to another governmental agency.
 - d. Administratively closed.
- B.** Original documents will be retained in the AMFED files until such time as requested by the OI FDs or until the records retention policy of the AMFED has been met. At that time, any original documents will be destroyed. Exceptions to this process are allegations referred to other government agencies and specific requirements of OI components (copies of the forwarded correspondence are maintained in the AMFED files). For example, original documentation will

be submitted on allegations forwarded to the Office of Counsel to the Inspector General (OCIG) pertaining to misleading advertisements.

- C. Allegations received by AMFED that contain an element of child abuse will be forwarded to the relevant OI field division, requesting that the field division refer the matter to the appropriate agency, and also to document the referral in NICMS in the Developmental Comments Section.
- D. Allegations received by the FDs.
 - 1. Allegations received by the FDs must be entered into NICMS by FD personnel.
 - 2. The information and supporting documentation for allegations requiring investigation in another FD will be forwarded to the appropriate division via memorandum.
 - 3. Allegations that contain an element of child abuse will be referred to the appropriate local agency, and the referral memorialized in the allegation's Developmental Comments Section in NICMS.
- E. For information on allegations received at AMFED or in a FD via congressional inquiries, see [section 002.170](#).

003.045 SSA's Fraud Information Tracking System (FITS)

- A. (b) (7)(E) [Redacted]
- B. (b) (7)(E) [Redacted]
- C. (b) (7)(E) [Redacted]
- D. (b) (7)(E) [Redacted]
- E. (b) (7)(E) [Redacted]

003.050 Case Opening Procedures

In accordance with OIG Performance Measure 2.2, 90% of allegations received by an OI FD are to be either opened or closed in the NICMS database within 60 calendar days of receipt. The responsibility for case opening decisions will not be delegated below the Assistant Special Agent-in-Charge (ASAC), Resident Agent-in-Charge (RAC), acting ASAC/RAC, or CDI Unit Team

Leader level. Allegations opened and pending for more than 10 working days should be assigned for required development.

003.060 Case Opening Priorities

OIG/OI policy is to concentrate its resources on conducting criminal investigations relating to the programs and operations of SSA. The priorities are subject to change based on Congressional or public interest. Generally, the order in which cases are to be investigated is as follows:

- 1. (b) (7)(E)
- 2. [Redacted]
- 3. [Redacted]
- 4. [Redacted]

003.070 Case Opening Guidelines

The following factors should be considered when deciding whether to open cases. They are provided as a guide, are not intended to replace sound judgment, and do not preclude the exercise of discretion by the SAC.

1. Specificity of the allegation.
2. Current SA caseload.
3. Primary and/or shared OI jurisdiction.
4. (b) (7)(E)
5. (b) (7)(E)
6. Local prosecutorial guidelines. Can the allegation be “packaged” with other allegations for presentation?
7. (b) (7)(E)
8. (b) (7)(E)

003.080 Case Numbering System

SSA OIG has used an alphanumeric system to designate cases since October 1, 1996. This enhances OIG's ability to track cases, identify program areas, and retrieve accurate statistics. The case number consists of the following elements:

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

3. A sequential number designation is be assigned as each new investigation is opened in the office/HQ component. Each FD/office will generate its own sequentially numbered cases.
4. A program category designation will identify the most appropriate category from the list below. It is recognized that many cases involve multiple allegations. However, the most significant category should be designated based on OI's investigative priorities.

(b) (7)(E) [Redacted]

Office designations are provided below:

<p>(b) (7)(E)</p>		<p>(b) (7)(E)</p>	
<p>(b) (7)(E)</p>		<p>(b) (7)(E)</p>	
<p>(b) (7)(E)</p>		<p>(b) (7)(E)</p>	
		<p>(b) (7)(E)</p>	

003.090

Guidelines for Administratively Closing Referrals of Potential Violations

The following factors should be used in evaluating whether to close referrals rather than formally convert them into open investigations:

1. current case opening guidelines;
2. prosecutorial guidelines;
3. (b) (7)(E) [REDACTED]
4. (b) (7)(E) [REDACTED]
5. (b) (7)(E) [REDACTED]
6. (b) (7)(E) [REDACTED]

003.100

Case Reviews

- A. A case review is a regularly scheduled evaluation and discussion of the investigative status/progress of all pending cases between a first-line supervisor and the SA to whom such cases are assigned. For non-CDI cases, case reviews shall be conducted at least three times a year in three different quarters, or more frequently at the discretion of the first-line supervisor, with SAC concurrence. CDI case reviews shall be conducted at least three times a year in three different quarters on cases 90 days old or older.
- B. Case reviews will be documented on a Supervisory File Review Sheet ([Form OI-20](#), [Exhibit 3-1](#)). Form OI-20 is a computerized form generated from information maintained in NICMS. Form OI-20 also serves as a device for validating NICMS data.
- C. While the review of documents and evidence in the case file is important, the case review process should not be viewed as merely a review of documents. Rather, it is an evaluation of the investigative progress and potential of the SA's cases. Therefore, using the OI-20 screen in NICMS, supervisors and agents shall document their discussions, to include supervisory instructions or directions. Supervisors shall ensure that any updates, instructions, directions or events related to the investigation that occur following the submission of an OI-6 (Prosecution Report) or OI-6A (Prosecution Report- ROI Cover Letter) and prior to the closing of an investigation, are reported on the OI-20.
- D. As part of the Quality Assurance Review process, OI will request the OIG's Office of Quality Assurance and Professional Responsibility to review/audit OI-20s for all cases that remain open 120 days following the OI-6/OI-6A submission date, in order to confirm that supervisory case file reviews were conducted and accurately reported, as outlined above.

003.110 Case File Organization

- A.** OI investigative case files are maintained in two forms – electronic and paper. Electronic files/documents are stored in NICMS under the case file number. Electronic documents that require a signature must contain an electronic signature. Paper documents are stored in a file folder using the same case file number. Paper documents that require a signature must contain either an electronic or wet signature, prior to filing. Documents contained in investigative case file folders will be filed according to a standardized system using a two-part file with numbered tabs to separate groups of documents ([Exhibit 3-2: OI-31](#)) as follows:
1. Left side of folder
 - a. Investigative Techniques (Tab One)
 - b. Waiver and Consent Forms/Statements (Tab Two)
 - c. Commercial Database Items - Lexis/Nexis, etc. (Tab Three)
 2. Right side of folder
 - a. Judicial/Administrative/Monetary Support Documentation (Tab Four)
 - b. Reports ([OI-2](#), [OI-6](#), and Investigative Notes, etc.) (Tab Five)
- B.** Case files are maintained at the case agent’s assigned office (FD or office).

003.120 Case File Arrangement and Closing Checklist

All documents placed in the case file will be noted on the Case File Arrangement and Closing Checklist ([Form OI-31](#), [Exhibit 3-2](#)). The OI-31 will be kept as the top document on the left side of the file. The Case File Arrangement and Closing Checklist permits SAs and supervisors to see what documents have been placed in the file and provides the supervisor with the information needed to justify statistical claims made by the agent. The Case File Arrangement and Closing Checklist should be filed/utilized based on case closing date and all documents should be filed accordingly. The Case File Arrangement and Closing Checklist will remain a permanent part of the official file.

003.130 Documenting Monetary Achievements

To show the results of OI’s efforts to counter fraud, waste, and abuse in SSA programs and operations, OI compiles and issues statistical reports to Congress, SSA, and the public. This section explains OI’s policy and procedures with regard to reporting monetary outcomes resulting from criminal or civil prosecutions and administrative actions. This section establishes procedures by which all OI FDs will report and document these achievements.

A. Monetary Achievements

Monetary achievements may result from criminal, civil, and/or administrative actions, and may be claimed on both SSA program and non-SSA program-related cases. These statistical achievements are based on the following types of investigative actions or activities:

1. court-ordered restitution arising from criminal conviction, pretrial diversion, or similar action;
2. pre-trial agreements;
3. civil judgment;
4. administrative action to prevent loss, achieve savings, or recover fraud loss;
5. fines, assessments, or other penalties imposed in criminal, civil, or administrative cases;
6. Civil Monetary Penalties (CMP); or
7. identification of fraud loss.

B. Claims for Statistical Monetary Achievements

1. **POLICY STATEMENT:** ALL MONETARY ACHIEVEMENT CLAIMS WILL BE APPROVED BY A SUPERVISOR, AND SUPPORTED BY DOCUMENTATION (e.g. court order, SSA documents or reports, etc.) IN THE CASE FILE.
2. Decisions regarding monetary achievement claims should rightfully be made to withstand both public and Congressional scrutiny. In that regard, OI will **only** claim credit in those cases in which OI played some **significant** role in effecting the action that led to the savings, recovery, or restitution.
3. OI may **only** take credit for monetary achievements in cases where:
 - a. OI had the lead role in the investigation. For example: OI completed the investigation and presented its findings to the appropriate party for disposition, regardless of whether another agency was involved to a lesser degree.
 - b. OI did not have the lead role, but was a **significant participant** in the investigation. Significant participation or playing a significant role in an investigation are defined as actively participating in actions that require a sustained commitment of time and effort, and have more than a peripheral effect on the outcome of an investigation. These actions include: conducting surveillances and/or stakeouts; conducting personal interviews; preparing affidavits; personally participating in searches and/or arrests; and testifying before a grand jury and/or trial about criminal activity pertaining directly to SSA programs and operations (not merely as a custodian of records). It must be noted that extracting data from SSA's system of records and sharing that information with other law enforcement partners does not constitute "significant involvement."
4. No credit should be taken in any case in which OI's role could reasonably be construed as that of a mere conduit through which information was passed. For example, if OI's only role in a joint investigation was to verify SSNs or provide certified SS-5s, then it **would not** be appropriate to claim a resultant monetary achievement.
5. For all claims to monetary achievements an explanation must be provided in Form OI-4, Report of Investigation, addressing OI's significant role in the investigation, and how the amount was determined. Monetary achievements should be added to NICMS by the agent's

supervisor, CDI Team Leader, or designated CDI staff, once the case has been reviewed and approved prior to closure.

6. Documenting accurate amounts in the correct categories at the proper time is critical to the OIG's ability to provide appropriate information when required.

C. Types of Monetary Achievements (see also NICMS Reference Manual 8.7)

This section defines the various types of SSA and non-SSA monetary achievements resulting from criminal, civil, and administrative actions, and establishes uniform procedures by which OI FDs will document those outcomes. Definitions of the available NICMS fields relating to monetary achievements, and guidelines for their use, are detailed in the following sections. For the purpose of those definitions, CMP cases shall be considered civil cases, with the exception that CMP claims shall be posted on the NICMS CMP screen instead of the NICMS civil screen.

1. Restitution ordered (NICMS field *MONETARY INFORMATION, MONEY TYPE, RESTITUTION*) (Criminal cases only)

- a. **Definition:** A **court-ordered** repayment resulting from Pre-Trial Diversions, guilty pleas, plea agreements, and convictions, which can be categorized as SSA or non-SSA program amounts. The amount of the restitution claimed by OI should match the amount of restitution documented on the Judgment and Commitment Order (J&C) or Pre-Trial Diversion agreement.
- b. Restitution can be claimed only in criminal cases, and should not be posted in NICMS until after sentencing or Pre-Trial Diversion.
- c. [Form OI-68](#), Report of Court-Ordered Restitution/Judgment (*see Exhibit 3-4*), must be prepared for each case resulting in an SSA program restitution. Execution and proper distribution of this form is essential (*see 003.160*).

2. Fine and/or Penalty (NICMS field *MONETARY INFORMATION, MONEY TYPE, FINE*) (Criminal and Civil cases)

- a. **Definition:** A **court-ordered** penalty, including any special assessment fees, imposed upon conviction in a criminal case or judgment in a civil case and requiring that a specified sum of money be paid to the court. In those cases in which fines are ordered to the court, the fines should be claimed as **non-SSA** fines. In cases in which the fines are ordered to SSA, the fines should be claimed as SSA fines. In order to comply with Congressional reporting requirements, it is imperative that fines be posted accurately.
- b. Fines can be claimed in both civil and criminal cases, and should not be posted in NICMS until after sentencing or judgment.

3. Recovery (NICMS field *MONEY TYPE, RECOVERY*) (Criminal, Civil, and Administrative cases)

- a. **Definition:** A *non-court ordered repayment* of funds to which an individual was not entitled, and/or a seizure and return of funds to which an individual was not entitled, which can be categorized as SSA or non-SSA program-related.

- b. SSA and non-SSA program-related recovery can be claimed as a result of criminal, civil, and administrative actions.
 - c. NICMS allows for multiple SSA and non-SSA recovery entries per case. That field is used for recording the total recovery identified at the time of case closing.
 - d. Repayment agreements entered into by subjects of an investigation are treated as recoveries. Any subject who states a desire to repay money to SSA must be referred to an SSA office to execute the repayment agreement. Although OI agents shall not accept repayment agreements on the behalf of SSA, agents should provide information to subjects in order to facilitate the execution of repayment agreements with SSA.
 - e. An overpayment posted to a MBR or SSID based on information developed during an investigation by OI and provided to SSA is considered a recovery for statistical purposes. Documentation of the overpayment and the information reported to SSA must be included in the OI case file.
- 4. Fraud Loss** (NICMS field *MONEY TYPE, FRAUD LOSS*) (Criminal, Civil, and Administrative cases)
- a. **Definition:** The total financial loss sustained by all defrauded parties as a result of the illegal activities of the subject. Fraud loss can be categorized as SSA and non-SSA program-related.
 - b. For SSA program cases, the value of the fraud loss should equal the total value of the administrative overpayment calculated by SSA. The fraud loss is *independent* of any restitution, judgments, fines, and/or recovery associated with the case.
 - c. For non-SSA cases, the value of the fraud loss should equal the total value of the financial loss sustained as a result of the subject's actions.
 - d. Fraud loss can be claimed in criminal, civil, and administrative actions. Fraud loss should not be posted to NICMS until the case is concluded by a criminal, civil, or administrative action, and a legitimate calculated amount is provided by the component, agency, or companies defrauded.
- 5. Judgment** (NICMS field *MONEY TYPE, JUDGMENT*) (Civil cases only)
- a. **Definition:** A judicially ordered payment resulting from a civil action, either through a Department of Justice (DOJ) civil proceedings or the CMP Program, which can be characterized as either SSA or non-SSA related. The distinguishing characteristic of a judgment is its nexus to a civil action, as opposed to a criminal restitution.
 - b. *A judgment is claimed only in civil cases.* It should not be posted in NICMS until the court or other civil authority has ruled on the civil action. The amount of the judgment claimed by OI should match the amount of the judgment documented on the Civil Judgment Decree, less any fines included in the judgment.

- c. Form OI-68, Report of Court-Ordered Restitution/Judgment ([Exhibit 3-4](#)), must be prepared for each case resulting in an SSA program judgment. Execution and proper distribution of this form is essential (See 003.160).

6. Program Savings (NICMS field *MONEY TYPE, SAVINGS*) (Criminal, Civil, and Administrative cases)

- a. **Definition:** A calculation of the avoidance of actual dollar loss by actions that result in the termination of improper payments or improper expenditures of program funds. Program savings relate *only* to SSA cases.
- b. Program savings may be claimed as a result of criminal, civil, and administrative actions, and should be posted only after SSA has taken administrative action to suspend or terminate improper payments.
- c. Savings, or cost avoidance amounts, will be determined by methods that represent the best available estimate, and will remain subject to change as new information becomes available. Each program and each eligibility factor violated could warrant different considerations when estimating their impact. As these factors are analyzed, OIG's methods and formulas for calculating savings will reflect the most realistic and defensible means possible.

1. SSA Program Cases (except Disability Cases, i.e. cases opened under program categories F – Program Fraud/Title II Disability and H – Program Fraud/Title XVI SSI Disability, see [003.080](#)) – Projected savings may be calculated by the following methods.

a. (b) (7)(E)

- b. Program savings will not be claimed in cases that result in the suspension or termination of SSA employees.

2. Fugitive Felon Cases

- a. With the implementation of the Fugitive Felon Automation Program, SSA no longer reports back to OIG with overpayment and monthly payment at the time of suspension information. In FY 2003, OI senior management ceased claiming monetary statistics for the electronic Fugitive Felon Program (FFP) cases processed solely at HQ. Case agents, however, will be allowed to claim monetary statistics for field-generated FFP cases under the following circumstances:

- 1) If the case agent actively participates in the apprehension of a fugitive, then monetary statistics should be claimed.

- 2) If the case agent simply shares information with the law enforcement agency that issued the warrant, then monetary statistics should not be claimed. Agents must actively participate in the apprehension of a fugitive in some substantial investigatory capacity in order to justify the claiming of monetary statistics.
- b. Program savings attendant to field investigations related primarily to fugitive felons will be calculated as follows: the difference of 24 months **minus** (-) the number of months that the warrant remains outstanding, **multiplied by** (x) the monthly benefit amount. No savings will be claimed when the warrant is in existence over 24 months.

The 24-month projected savings is based on a Department of Justice study that found that, on average, a warrant remains outstanding for two years.

3. Title II and Title XVI Disability Cases, Program Categories F – Program Fraud/Title II Disability and H – Program Fraud/Title XVI SSI Disability, see 003.080, (to include Cooperative Disability Investigations-CDI) – Projected savings may be calculated by one of two methods which are summarized in the chart below:

	FY 2015 Savings Estimates	
	Initial Claim	In-Pay Claim
(b) (7)(E)		(b) (7)(E)
(b) (7)(E)		
(b) (7)(E)		

- a. When the investigation resulted in the denial of an initial claim, a set rate must be claimed for SSA savings. *(Note: If the case is a CDI program investigation, be sure the nation operation code “RK ”and local project code is entered on the allegation and case number. If the case was not a CDI program investigation, be sure that the national operation code and local project code fields are left blank/not entered for the allegation and case number.)*

1. (b) (7)(E)
2. (b) (7)(E)
3. (b) (7)(E)

- b. (b) (7)(E)
- The result is the amount to claim for SSA program savings.

(b) (7)(E)

(b) (7)(E)

- c. When the investigation resulted in the suspension, cessation or termination of a current claim as well as the denial of an initial claim, (for example, a Title XVI beneficiary who recently became eligible for Title II benefits and has a pending TII application) use the set rate for initial concurrent claims, \$47,814.

003.140 Documenting Arrests

- A. OI may **only** take credit for an arrest in cases when OI personnel physically participate in the arrest. **“Physically participates in an arrest”** is defined as personally taking a subject into custody as part of a primary arrest team. As an example, three agents who effect the arrest of a subject within a residence, two going through the front door and one covering the back door, act as a primary arrest team. As a second example, two agents who arrest a subject during a worksite enforcement operation, one handcuffing the subject while the second agent covers, act as a primary arrest team.

On the other hand, performing perimeter security duties during a worksite enforcement operation does not constitute physical participation in an arrest, unless the agent meets the parameters outlined in the first part of this definition. Finally, actions related to the issuance of a summons do not constitute physical participation in an arrest.

- B. In order to claim any of the arrests identified in section 003.140, the case file must contain the following:

1. Arrests in Program, Employee, Enumeration or SSN Misuse Cases

- a. [OI-19](#) personal history form ([Exhibit 3-5](#)).
- b. Charging documents (e.g., warrant, complaint, information, indictment).
- c. [OI-4](#), “Report of Investigation ([Exhibit 3-6](#)),” which reflects the OIG SA’s specific role in the investigation.
- d. Arrest Fact Sheet, reference SAH 011.040 C.
- e. Fingerprints of the subject arrested (or specific location where the fingerprints can be located, including the name of the law enforcement agency, case number, case agent, telephone number, and address). Document this information in the OI-4.
- f. Title 28 CFR Part 28 requires the collection of DNA samples from individuals who are arrested, facing charges, or convicted, and from non-United States persons who are

detained under the authority of the United States pursuant to 42 U.S.C. 141a(a)(1)(A). An agency that arrests and fingerprints an individual, then transfers the individual to another agency (such as the U.S. Marshals Service) for detention cannot transfer responsibility for DNA-sample collection to the detention agency unless that agency agrees to assume responsibility for that function. DNA collection kits are available free of charge from the FBI's Federal Convicted Offender Program. The kit order form is found as Exhibit 3-11. Ordering instructions are on the form. Instructions, which must be followed exactly, are included in each DNA kit.

2. **Arrests in Task Force Operations or Joint Investigative Operations** - These arrests include [Homeland Security Projects](#) (usually in conjunction with DHS-Homeland Security Investigations), Joint Terrorism Task Force Operations, Fugitive Felon Operations (U.S. Marshals Fugitive Operations), and other large scale multiple defendant operations, in which agents physically participate.
 - a. OI-19.
 - b. Charging documents.
 - c. OI-4 Report of Investigation explaining the OIG SA's specific role in the investigation.
 - d. Photographs of the subject arrested (or specific location where the photographs can be located, including the name of the law enforcement agency, case number, case agent, telephone number, and address). This information will be documented in the OI-4. The reverse of the subject's photograph will contain the following: name, date of birth, OIG case number, FBI number (if available), and the name of the SA assigned to the case.
 - e. Fingerprints of the subject arrested (or specific location where the fingerprints can be located, including the name of the law enforcement agency, case number, case agent, telephone number, and address). Document this information in the OI-4.
 - f. DNA samples must be collected from the subject. This is for Qualifying Federal offenses only, misdemeanors do not apply. Qualifying Federal offenses include: any felony, any offense under chapter 109A of Title 18 (i.e. sexual abuse), any crime of violence (i.e. violent crime, as defined in section 16 of Title 18), and any attempt or conspiracy to commit a felony, any offenses under chapter 109A of Title 18, or a violent crime. See section 003.140 B.1F for information.

The collection of DNA must be reported in a Report of Investigation or a copy of a DNA collection form must be obtained and placed in the investigative file. The form must be filed under the "Arrest Warrant/Photographs/Prints/R-84/DNA Collection form" section of the Form OI-31, located under Tab 4.

- g. Request for Special Project Approval to the Intelligence and Analysis Division (IAD).
- h. Approval documentation from IAD for the project (e-mail or memorandum).

If, during the course of an operation solely for immigration violations, undocumented aliens are apprehended they should be turned over to DHS-Homeland Security Investigations and no arrest claimed. The total number of these apprehensions and any

unusual incidents that occurred during the operation will be recorded in the OI-4 for this operation.

Any arrest claimed must have a charge that specifically pertains to SSA violations and the case file must contain the information listed above.

3. Arrest of a Fugitive Felon

1. OI-19 personal history form.
2. Photograph of the subject or a copy of a document bearing the subject's photograph.
3. A copy of the arrest warrant or warrant number and the name of the law enforcement agency or department from which these items may be obtained.
4. Fingerprints and DNA samples will be taken if OI is the only agency participating in the arrest. If OI is assisting another agency and that agency accepts responsibility for processing the arrestee, the agent must include the name of the agency, and the names of the agents or officers who participated in the arrest, in the report of investigation. In all instances, documentation of fingerprints and DNA samples will be recorded on the arrest report of investigation.

003.150 Requests for Investigative Activities by Another Division (Collateral Investigations)

- A.** Requests for investigative leads to be addressed in one FD as part of a continuing investigation in another FD are referred to as **collateral investigations**.
- B.** The following guidelines should be used when requesting investigative assistance from another FD:
 1. The SAC/ASAC/RAC of the requesting FD (controlling office) shall notify the SAC/ASAC/RAC of the assisting FD of the nature of the assistance to be requested, via e-mail or memorandum.
 2. The case agent, to include CDI Unit team leaders, shall prepare a [form OI-4](#), Report of Investigation (see [Exhibit 3-6](#)), detailing the nature of the case and the assistance required. The collateral Report of Investigation should also include:
 - a.** a brief summary of the allegation;
 - b.** the issues upon which the collateral request is based;
 - c.** the specific collateral investigation required;
 - d.** all available background information on individuals relevant to the request; and
 - e.** time sensitivity or restrictions, if any.

3. The Report of Investigation (ROI) must be approved by an OI supervisor at the controlling office. Following the approval of the report, the controlling office supervisor will notify the assisting office supervisor via e-mail that a collateral investigation is requested. The assisting office supervisor should check the report to see what action(s) his/her office is asked to perform.
- C. The following guidelines should be used when completing and reporting investigative activity to the requesting FD:
1. The SAC/ASAC/RAC of the assisting FD will assign an agent(s) to complete the requested activity.
 2. **The assisting FD will complete all investigative activity using the requesting FD case number. A new case number will not be generated.**
 3. After the assisting FD completes the required activity, a collateral ROI will be prepared in NICMS under the requesting FD case number. Notification that the approved ROI is available in NICMS will be sent via e-mail by the SAC/ASAC/RAC of the assisting FD to the supervisor of the office requesting the information. The ROI should contain the following information, as applicable.
 - a. Date and location of completed action
 - b. Results of the investigative activity
 - c. Names of participating SSA/OIG agents or other law enforcement officers involved
 - d. Other agencies participating
 - e. Judicial activity
 - f. Name and phone number of prosecuting attorney
 - g. Any other pertinent information that would be necessary for the case agent's completion of applicable NICMS entries into fact sheets, criminal/civil disposition screens, etc.
- D. All statistical achievements will be credited to the requesting FD. The requesting FD is responsible for entering all data into NICMS, including the following:
1. Date of arrest
 2. Agents participating in arrest
 3. Any monetary achievements
 4. Conviction information
 5. Completion of Fact Sheets

- E. The assisting FD should make every effort to complete the collateral request in an expeditious manner. The results of the collateral investigation will be reported to the requesting FD within 30 days unless extenuating circumstances cause a justifiable delay.

003.160 Reporting of Judgments and Court-Ordered Restitution

- A. Congress has mandated that SSA OIG track the actual receipts derived from court-ordered restitution and judgments, and report this information to Congress semiannually. OI thus has a responsibility to inform SSA of all civil judgments and court-ordered restitution that will ultimately be ordered to SSA by the courts. SSA then has a responsibility to track receipts and apply credits to the proper account when funds are received. SSA's Debt Management Section will credit the beneficiary's record and deposit the payment in SSA's Treasury account.
- B. In order to ensure accurate OI reporting in this regard, OI agents will complete [Form OI-68](#), "Report of Court-Ordered Restitution/Judgment" (see [Exhibit 3-4](#)), for every case in which a court orders a defendant to return or pay funds to SSA. Restitution and judgments ordered to non-SSA entities (i.e., financial institutions, credit corporations, etc.) shall not be reported on form OI-68.
 - 1. Form OI-68 was developed in conjunction with the Administrative Office of the United States Courts and SSA, and provides the information necessary for both agencies to collect and properly post payments intended for SSA.
 - 2. In most cases, DOJ is responsible for collecting restitution payments ordered by Federal courts and forwarding payments to SSA, as required. However, in some districts, the defendant is ordered to make payments directly to SSA. In most state courts, the defendant is similarly ordered to make payments directly to SSA.
 - 3. The SSA Payment and Recovery Policy staff monitors the defendants' compliance with the court orders. Both DOJ and SSA will use form OI-68 to fulfill their respective requirements in forwarding and processing judgment and/or restitution payments intended for SSA.
- C. Form OI-68 shall be prepared in its entirety by the SA in accordance with the instructions below:
 - 1. Section 1, "Defendant Information": Enter the court case number, the full name of the defendant, and the SSN of the defendant.
 - 2. Section 2, "Claimant Information": Enter the name of the claimant involved in the fraud (may be the same as the defendant), the SSA claim number involved in the fraud, and check either "Title II" or "Title XVI," as appropriate.
 - 3. Section 3, "Judicial District": Enter the name of the Federal or state judicial district, the identity of the Clerk of the Court or Financial Administrator (whichever is responsible for tracking restitution for the particular court), the address of the court, and the telephone number of the Clerk of the Court or Financial Administrator.
 - 4. Section 4, "Restitution/Judgment": Enter the total amount ordered by the court, the date of the order, the value of any interest or penalties assessed by the court, the monthly payment ordered to SSA, and the date that the first payment is due (all of which is included in the J&C).

5. On the bottom of the form, the case agent shall enter his/her name, address, telephone number, and date that the Form OI-68 was prepared.

D. Distribution of Form OI-68 – *Completed* copies of form OI-68 should be distributed as follows:

1. At the conclusion of the investigation, the case agent is responsible for electronically forwarding form OI-68 with copies of the Judgment and Commitment (J&C) and the Sentencing Fact Sheet to the SSA and judicial components listed below via the “OI-68 Referral Information” tab in NICMS. Instructions for doing this are located in [Exhibit 3-4A - How to Use NICMS to Submit OI-68](#).
 - a. Social Security Administration, P.O. Box 2861, Attn: Court Refund, Philadelphia, PA, 19122 (Debt Management).
 - b. Social Security Administration Regional Contact in the area responsible for servicing the region where the violation occurred.
 - c. The Clerk of the Court or Financial Administrator of the Court. (NOTE: If the case was prosecuted on the *state* level and you do not have the email address for the Clerk of Court, you must mail a hard copy to them.)
2. If the Case Agent requested the subject's claim folder during the investigation, *a copy of the Form OI-68, a copy of the J& C Order from the court of record, and a copy of the Sentencing Fact Sheet must be placed in the claim folder prior to returning it to SSA.*

003.170 Closing/Disposition of Investigative Files

- A.** Following receipt of information indicating completion of all civil, criminal, and/or administrative actions in a case, the case agent and the approving supervisor must ensure that the following documents are contained in the case file (and that copies of these documents have been distributed, as required by policy, prior to closing the investigation):
1. final judicial document(s) that specify the allegations, findings, and judicial orders (i.e., the J&C, Pre-Trial Diversion Agreement, Civil Judgment);
 2. Sentencing Fact Sheet, detailing a synopsis of the investigation and the results of the judicial/administrative action;
 3. a case-closing Report of Investigation (OI-4 or OI-4 CDI as appropriate); and
 4. in cases in which an individual was booked (arrest or summons) on any OI-related charge(s), or in which OI was the lead investigative agency and fingerprints were forwarded to the FBI, a copy of FBI Form R-84 to report the disposition of the case should be maintained in the case file for submission to the FBI at the conclusion of the case. The FBI defines a disposition as an action regarded by the criminal justice system to be final. A disposition states that the arrest charge(s) have been modified, dropped, or reports the findings of the court. If someone from another agency (e.g., the U.S. Marshals Service) submitted the fingerprints on OI's behalf, the OI SA shall obtain the agency's Originating Agency Identifier (ORI) and include that ORI on the R-84 submitted to CJIS. (*Note: If another agency makes*

the arrest and submits an R-84, there is no need for OI to complete and submit a second R-84. This should be documented in the closing ROI.) R-84s submitted without an ORI number will be rejected by CJIS

5. for federal cases, the collection of DNA must be reported in a Report of Investigation (ROI) or a copy a DNA collection form must be obtained and placed in the investigative file under the “Arrest Warrant/Photographs/Prints/R-84/DNA Collection form” section of the Form OI-31, located under Tab 4.
 6. for non-federal cases, the agent should ensure that the charges are entered into the appropriate state criminal history repository at the time of arrest or summons. The agent should ensure that the final disposition is entered into the state criminal history repository at case conclusion. The various states report criminal history information regularly to the FBI CJIS via magnetic tape and CD-ROM. (See the Department of Justice, Federal Bureau of Investigation, Criminal Justice Information Services – CJIS, Arrest Disposition Submission, Section II. Arrest Disposition Submission Formats website – <http://www.fbi.gov/hq/cjisd/arrestdispositions.htm> - for details on the R-84 form.)
- B.** Any attachments or documents that are not to be returned to a custodian will be retained in the case file for a minimum of three years after the case has been closed.
- C.** All original documents or other items obtained as evidence must be properly disposed of (i.e., returned to the owner, returned to the Agency, released to another agency, or destroyed). Disposition of evidence should be recorded on the final Report of Investigation. See [*Special Agent Handbook Chapter 14*](#), “Acquisition, Preservation, and Management of Evidence,” for a complete explanation of evidence handling procedures.
- D.** Refer to [Chapter 5](#) of the Administrative Policies and Procedures Manual for instructions pertaining to the maintenance and disposal of closed case files.

003.180 Reporting State & Local Informations, Indictments, Fugitives from Justice, and Judgment and Commitment Orders to FBI’s National Instant Criminal Background Check System

- A. The National Instant Criminal Background Check System (NICS) was established in 1998 so that Federal firearms dealers could effectively determine, prior to issuing a firearm, whether a potential buyer is prohibited from receiving that firearm based on the Federal Gun Control Act of 1968 ([Federal Prohibitors](#)), as amended by the Brady Handgun Violence Prevention Act of 1993 (codified at 18 U.S.C. Chapter 44). The ability of NICS to quickly and effectively determine whether an individual is prohibited from possessing or receiving a firearm or explosive is dependent upon the completeness and accuracy of information provided by Federal, State, Local, and Tribal authorities.
- B. In January 2013, the President issued a Memorandum to strengthen the accuracy and efficiency of the Federal background check system for firearms purchases. The Memorandum created a Working Group, chaired by the Department of Justice, to provide guidance to agencies regarding the identification and sharing of relevant Federal records. Heads of all executive departments and agencies were directed to prioritize the submission of relevant records to the NICS on a regular and ongoing basis. In addition, agencies were

directed to submit a report and implementation plan concerning relevant records in their possession and to submit annual reports on their progress thereafter. SSA is submitting a report to which SSA OIG will contribute.

- C. In March 2013, the Working Group issued its *Guidance to Agencies Regarding Submission of Relevant Federal Records to the NICS* ([Guidance](#)), in which Section I of the Guidance addresses which records are “relevant” for purposes of the President’s Memorandum. Section II clarifies when an agency “possesses” a record that must be submitted to NICS. Section III explains the process for providing the information in its possession and explains the requirements for updating, correcting, modifying, and/or removing records from the NICS. Section IV discusses the contents of the (1) Report and Implementation Plan that must be submitted by agencies and (2) the annual report agencies with records in their possession must submit.
- D. Section I - Identification of Relevant Records – Relevant records include information relevant for the NICS that identifies an individual as being prohibited from shipping, transporting, possessing, or receiving firearms under Federal firearms law. The Guidance sets out 10 categories:
1. Felons;
 2. Fugitives from justice;
 3. Persons unlawfully using or addicted to any controlled substance;
 4. Persons adjudicated “mentally defective” or committed to a mental institution;
 5. Illegal/unlawful aliens, and aliens admitted on a non-immigrant visa;
 6. Persons dishonorably discharged from the military;
 7. Citizen renunciates;
 8. Persons subject to a domestic violence restraining order;
 9. Persons convicted of a misdemeanor crime of domestic violence; and
 10. Persons under indictment.
- E. OI is responsible for providing information from our investigative files on 3 of these 10 categories of individuals, **and then only if the individuals are being prosecuted in a State or local court**: (1) Felons; (2) Fugitives from Justice; and (3) Persons under Indictment/Information. This information will be provided to the FBI’s NICS effective March 1, 2015. The FBI has access to the records for those individuals that we investigate who are prosecuted in the Federal court system. The Department of Justice will address all reporting requirements for Federal cases (i.e. Federal warrants, indictments, informations, and convictions).
- F. Section II – Records in an agency’s possession that must be submitted to the NICS. In determining whether SSA OIG houses relevant records, a distinction is made between records SSA OIG creates and records it possesses. To “create” a record, SSA OIG must have

generated the record or caused it to be generated by a third party at our request. To “possess” a record that is contained in SSA OIG files means the record was obtained from sources or processes independent of the SSA. Since these records were not created by SSA OIG, but obtained from a State or Local jurisdiction, they are considered to be in the “possession” of the SSA OIG and not “created” by the SSA OIG. SSA OIG is responsible for providing the relevant records to the NICS.

G. The relevant records for these categories that are to be provided include:

1. Felons – Judgment and Conviction Orders (also known as Judgment and Commitment Orders) from the Court.
2. Fugitives from Justice – Misdemeanor and Felony Warrants and Charging Documents.
3. Persons under Indictments – Indictments and Informations.

H. There are four circumstances that could justify not submitting the records to the NICS. If any of these four is present in your case, the Special Agent-in-Charge (SAC), Assistant Special Agent-in-Charge (ASAC), and/or Resident Agent-in-Charge (RAC) should take the appropriate action and the case agent must document the reasons for non-submission of records via Form OI-4. The four circumstances are:

1. Where submission of the records would substantially undermine another program or policy interest;
2. Where submission would be inconsistent with confidentiality or limited use assurances made when the record was obtained;
3. Where previous record-keeping practices prevent the agency today from determining which records are relevant; or
4. Where the logistical hurdles associated with producing the records would be prohibitive.

I. To comply with the President’s Memorandum, the case agent must obtain a filed copy of the indictment (if such document is not sealed), or information or misdemeanor and felony warrants and charging documents for fugitives from justice and forward, via email to the FBI’s NICS Index Submission at NICS_Index_Submissions-External@ic.fbi.gov. Upon sentencing, the judgment and conviction order/judgment and commitment order must also be forwarded via email to the NICS Index Submission (see above email address). If the relevant information is under seal, the case agent should take the appropriate action under the sealed order and ensure this information is documented via Form OI-4. The NICS Index Submission email cover sheet must be attached to all documents submitted ([Exhibit 3-13](#)). The email must include the following:

1. Case Number;
2. Subjects Name, DOB, Sex, Race and any other identifying information/descriptors available;

3. Type of document (Information, Indictment, misdemeanor/felony warrants and charging documents for fugitives from justice, or Judgment and Commitment Order) and copy of document;
 4. State or Local Jurisdiction where the document originated; and
 5. Contact information for the state or local jurisdiction where the document was generated.
- J. Section III – Procedure for Submitting Relevant Records to the NICS and Ongoing Requirement to Updates, Correct, Modify and/or Remove Records – OI case agents will submit the criminal history information upon receipt of the document(s), not to exceed one month, to the FBI’s NICS Index Submission. Before submitting the information to the NICS, the case agent must check with the Interstate Identification Index (III) and NCIC to see if the State or local jurisdiction has already submitted the information. If the information has been submitted, OI does not need to provide the records to the NICS; however, a list of records not submitted should be maintained by the OI office. If the State or local jurisdiction has not submitted the information to the III or NCIC, the case agent must submit the records, via email to the NICS Index Submission at NICS_Index_Submissions-External@ic.fbi.gov. The OI office will maintain a list of records submitted to the NICS for inclusion in SSA’s annual report submitted pursuant to Section IV of the Guidance.
- K. Section IV – Submission of Report and Implementation Plan and Annual Report. In May 2013, SSA submitted an Implementation Plan to DOJ that includes SSA OIG providing records to the NICS. SSA OIG will provide to SSA the number of submissions provided by OI to the NICS for inclusion in SSA’s annual report.
- L. Field Division Responsibilities - OI case agents will submit the criminal history information upon receipt of the document(s) to the FBI’s NICS Index Submission (*see letter I and J. Section III for additional submission requirements*). If the case agent is unable to submit the information upon receipt, the information must be submitted no less than monthly to the FBI. The submission of criminal history information must also be documented in a Form OI-4, Report of Investigation, advising of the date the criminal history information was reported to the FBI’s NICS Index Submission. The NICS Index Submission email cover sheet ([Exhibit 3-13](#)) must be filed under the “Judgment and Commitment Order or Indictment/Information/Complaint” section of the Case File Arrangement and Closing Checklist-Form OI-31, located under Tab 4. It is recommended that each OI Office maintain copies of all criminal history information emails submitted to the FBI’s NICS Index Submission to respond to OI Headquarters, via a quarterly control, regarding the number and type of NICS Index Submissions.
- M. OI Headquarters Responsibilities - Information will be obtained by OI Headquarters, via a quarterly control, to the OI Field Divisions regarding the type of category reported and number of submissions made, during that quarter, to the NICS Index Submission. Each fiscal year, OI, via the Policy and Administration Division, will provide these numbers to SSA for inclusion in their annual report to the President of the United States through the Attorney General. OI will report this information annually to SSA on or about September 1st.
- N. OI Headquarters will request information pertaining to the number and type of NICS Index Submissions on a quarterly basis. To ensure OI reports the correct information to SSA, OI case agents must document the following:

- The number of submissions for the type of document submitted (Information, Indictment, Fugitives from Justice, Judgment and Commitment/Conviction Order) and corresponding OI case number and subject type (Beneficiary/Recipient, Representative Payee, Illegal alien, SSA Employee, or N/A).
- For cases involving multiple subjects, each charging document and/or judgment and commitment/conviction order submitted via one facsimile should be counted as a separate submission for reporting purposes.
- If the case agent reports a Judgment and Commitment/Conviction Order based on a previously reported indictment or information or fugitive from justice, the case agent must also reflect the previous submission when reporting the number and type of NICS Index Submissions each year, providing the case number as a reference and subject type [(beneficiary/recipient or other subject type) (see table below)].

Category	# of Submissions	Category previously reported (information, indictment, or fugitive from justice)	OI Case Number	Subject Type Indicate whether subject type is: Recipient (T16/SSI) Beneficiary (TII/RSI) Representative Payee Illegal Alien SSA Employee N/A
Information	2		(b) (7)(E)	Beneficiary
			(b) (7)(E)	Recipient
Indictment	1		(b) (7)(E)	N/A
Fugitives from Justice	0		N/A	N/A
Judgment and Commitment/Conviction Order (J&C)	0		N/A	N/A
# of J&Cs submitted this quarter resulting from previously reported NICS submissions	1	Information	(b) (7)(E)	Recipient

003.190 Notification to SSA at the Conclusion of an Investigation

- A. Upon reaching judicial finality in a case referred by SSA to OI, the referring SSA entity and the Public Affairs office, along with all other SSA entities playing a significant role in assisting OI with the case and shall be notified of the final disposition of the case via the official OI Fact Sheet. After review of the final Fact Sheet by respective SAC or their designee within each Field Division, the Fact Sheet may be disseminated to a variety of offices and/or persons in addition to the current required distribution list. Additional distribution may include the respective Regional Commissioner's Office, Area Director's Office, and the District Office Manager of the referring office. It is recommended that Fact Sheets be distributed electronically.
- B. OI offices wishing to forward to referring SSA entities some form of additional notification on the disposition of a case (e.g., letters of appreciation, copies of court-generated J&Cs, emails, etc.) may do so at their discretion.

003.200 Monthly Verification of Statistics

Each FD must run the regional Investigative Productivity Reports (IPR) from NICMS to verify the accuracy of the statistics entered into NICMS for the month. Using the OIG's Control system, each SAC (or in his/her absence the ASAC) must certify that the required monthly verification was completed and accurate. This process is to be completed by the seventh working day of the month, with the exceptions of April and October, when the certification should be conducted by the fourth day, due to the Semiannual reporting requirements.

003.210 Reopening of Previously Closed Cases

Cases that have been closed can be reopened if additional information is received that would help substantiate one or more violations of misconduct, or that a suspect in an investigation has been identified. Only a supervisory Special Agent (SAC, ASAC, or RAC) can reopen a previously closed case.

003.220 Quarterly Case Reviews by the Policy and Administration Division

- A. On a quarterly basis, PAD will conduct reviews of randomly selected cases closed during the previous quarter. Cases will be selected in order to best capture a variety of OI's caseload.
- B. The case reviews are conducted to identify areas for corrective measures; ensure compliance with OI policies and procedures; and to identify anomalies, trends, and/or issues which may warrant further OI review. The results of the quarterly case reviews are provided via the Quarterly Case Review report to the AIGI and DAIGIs through the SAC of PAD.
- C. After receipt of the respective OI Field Division's case report, SACs must provide a memorandum within 45 days to the AIGI advising of their field division's corrective actions to

resolve issues indicated during the review of case files. Those responses are maintained and stored by PAD.

003.230 *For Future Use*

003.240 **Organizational Representative Payee Cases**

- A.** In addition to “special interest” cases, CID also tracks cases regarding potential Organizational Representative Payee (ORP) misuse. Cases designated as "Organizational Representative Payee" investigations include those cases involving organizations serving as a representative payee, regardless as to: 1) whether the subject of the investigation is the organization itself, or a single employee of the organization; or, 2) the number of beneficiaries whose benefits were misused.
- B.** On a semi-annual basis, CID will report the status of all open ORP cases based on information provided by the OI Field Divisions in NICMS. This information is provided, via the ORP Report, to the AIGI and DAIGIs through the SAC of CID. The purpose of the ORP Report is to provide management information in a timely manner regarding all open ORP investigations. Cases designated as ORP investigations are required to be updated in NICMS until the case is closed, or at the discretion of OI senior management.
- C.** OI Field Division Responsibilities
1. ORP investigations must be updated in NICMS, via the Case Status tab, no later than the last day of the fiscal year’s semi-annual reporting period (i.e. July and December), unless otherwise advised by CID.
 2. Supervisors are responsible for ensuring the timely completion and accuracy of quarterly updates by the Special Agents to whom the cases are assigned. In addition, before finalizing and submitting to CID, supervisors are encouraged to review the last ORP Report to ensure that the current update is accurate, specific, and addresses the outcome(s) of any investigative activities indicated in the prior report. Supervisors should also ensure that all investigative activities and outcomes are captured as well as all instructions advised of during case reviews were completed.
 3. OI Special Agents must update three status fields, under the Case Status tab, when updating the cases listed as an ORP investigation. The three status fields are:
 - a. Case Description: An initial description is entered during the first Quarterly ORP Report, after the case has been opened. This field is only updated if the case description has substantially changed during the course of the investigation.
 - b. Status: Information must state “Status as of (last day of reporting month):...” If the investigation is ongoing, start with “Investigation is ongoing.” All investigative activities conducted during the reporting period, to include the outcome of those activities, must then be specified. If an investigative activity was advised of during the last reporting period but no outcome was indicated, be sure to advise of the outcome. If the investigation is complete, the status should state, “The investigation is complete.”
 - c. Judicial Status: All judicial information must be provided (i.e. presentation date, acceptance/declination, name of AUSA/prosecutor, judicial district, complaint/

indictment/information date, criminal violation(s), sentencing date, final disposition, etc.).

Chapter 3 — **EXHIBITS**

[3-1 — Supervisory File Review Sheet \(OI-20\)](#)

[3-2 — Case File Arrangement and Closing Checklist \(OI-31\)](#)

[3-3 — NICMS Disposition Form \(OI-9\)](#)

[3-4 — Report of Court-Ordered Restitution/Judgment \(OI-68\)](#)

[3-4A — How to Use NICMS to Submit OI-68s](#)

[3-5 — Personal History Information Form \(OI-19\)](#)

[3-6 — Report of Investigation \(OI-4\)](#)

- [3-7 — Reserved for Future Use](#)
- [3-8 — Report of Investigation— \(OI-4 CDI\) Cooperative Disability Investigations Unit](#)
- [3-9 — FBI Laboratory Buccal Collection Kit Re-Order Form](#)
- [3-10 — Methodology for Calculating Disability Program Savings](#)
- [3-11 — CJIS Fingerprinting Supply Requisition Form](#)
- [3-12 — Request for Audit and Financial Forensic Assistance](#)
- [3-13 — NICS Cover Sheet Facsimile](#)

Exhibit 3-1

SUPERVISORY FILE REVIEW SHEET PAGE: 1
 DATE CONDUCTED _____ NEXT SCHEDULED _____ SUPERVISOR _____ INITIALS: _____
 AGENT NAME: _____ FLD. DIV.: _____ OFFICE: _____

CASE NUMBER AND IDENTIFIERS	DATES	AGENT'S COMMENTS A. BRIEF DESCRIPTION OF CASE B. WORK TO BE DONE	SUPERVISOR'S COMMENTS (INCLUDING INSTRUCTION)
CASE NUMBER: ALLEGATION NUMBER: PRIMARY SUBJECT NAME: TYPE: SRCE: PROG: ALLEG: LEMUS:	OPENED: ASSIGNED: MRIM: PRESENT: ACCEPTED: DECLINED: INDICTED: ARRESTED: FINL ACT: FINL TYP:	A. B.	
CASE NUMBER: ALLEGATION NUMBER: PRIMARY SUBJECT NAME: TYPE: SRCE: PROG: ALLEG: LEMUS:	OPENED: ASSIGNED: MRIM: PRESENT: ACCEPTED: DECLINED: INDICTED: ARRESTED: FINL ACT: FINL TYP:	A. B.	
CASE NUMBER: ALLEGATION NUMBER: PRIMARY SUBJECT NAME: TYPE: SRCE: PROG: ALLEG: LEMUS:	OPENED: ASSIGNED: MRIM: PRESENT: ACCEPTED: DECLINED: INDICTED: ARRESTED: FINL ACT: FINL TYP:	A. B.	
CASE NUMBER: ALLEGATION NUMBER: PRIMARY SUBJECT NAME: TYPE: SRCE: PROG: ALLEG: LEMUS:	OPENED: ASSIGNED: MRIM: PRESENT: ACCEPTED: DECLINED: INDICTED: ARRESTED: FINL ACT: FINL TYP:	A. B.	

Exhibit 3-2

Social Security Administration-Office of the Inspector General

Office of Investigations

Case File Arrangement and Closing Checklist

(b) (7) (E)

SOCIAL SECURITY
Office of the Inspector General

NICMS DISPOSITION FORM

(b) (7) (E)

Exhibit 3-4

Office of the Inspector General
Office of Investigations
Social Security Administration

REPORT OF COURT ORDERED RESTITUTION/JUDGMENT

OI Case Number: _____

To the Financial Administrator/Clerk of the Court : When the Social Security Administration (SSA) is the victim, note the **SSA OI Case Number** on the check, or *attach a copy of this form and forward to:*

**Social Security Administration
Debt Management Section
ATTN: Court Refund
PO Box 2861
Philadelphia, PA 19122**

1. Defendant Information

Court Case Number: _____

Defendant's Name: _____ **Defendant's SSN:** _____

To the SSA Mid-Atlantic Payment Center: The following information should be used to properly post this payment.

2. Claimant Information (refers to the number on which the improper benefits were paid)

SSA CLAIM NUMBER: _____ Title II Title XVI **(Check One)**

Name: _____

3. Federal/State Judicial District _____

Financial Administrator (Name): _____

Address: _____

Telephone #: _____

4. Restitution/Judgment

AMOUNT ORDERED: _____ **Date of order:** _____

Monthly Payment Amount: _____ **Interest and Penalties:** _____

Date First Payment Due: _____

Special Agent: _____

Address: _____

Telephone #: _____ **Date:** _____

APPROVED BY: (Signature of SAC/ASAC/RAC) _____ **Date:** _____

Distribution: 1. Financial Administrator 2. OI CID 3. OI Case File

How to Use NICMS to Submit OI-68s

Preparing the OI-68 to be Emailed

1. The agent must complete the “Victim & Claimant List” tab in NICMS. Go to “Update Victims & Claimants” tab.

- No longer list SSA as the victim
- Input the claimant’s name
- Put the SSN of the SSA record to be credited with the restitution.

(b) (7) (E)

2. The information entered in the “Victim & Claimant List” tab will be propagated to the Claimant Information Section on the OI-68 tab.

Exhibit 3-4A

3. Go the “Edit OI-68” tab and input the following information:
 - Address of the clerk of court (in the Federal/State Judicial Section)
 - Restitution amount
 - Address and phone number of the agent

4. Click on the Green Arrow to save your changes.

(b) (7) (E)

Sending the OI-68 Referral Email

(b) (7) (E)



(b) (7) (E)



SOCIAL SECURITY
Office of the Inspector General

PERSONAL HISTORY INFORMATION

(b) (7) (E)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)

(b) (7) (E)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

Exhibit 3-6

Office of the Inspector General
Office of Investigations
Social Security Administration

REPORT OF INVESTIGATION

TITLE OF CASE:

CASE NUMBER:

PROGRAM CATEGORY:

PERIOD COVERED:

From: To:

RELATED CASE NUMBERS:

REPORT BY:

FIELD DIVISION / OFFICE:

FD: Office:

STATUS OF CASE:

() INVESTIGATION CONTINUED

- INITIAL REPORT
- STATUS REPORT
- JUDICIAL STATUS REPORT

() COLLATERAL INVESTIGATION

() INVESTIGATION CLOSED

SYNOPSIS

ALLEGATION or REFERENCE TO MOST RECENT REPORT

INVESTIGATIVE ACTIVITY

SUBJECT(S) AND/OR DEFENDANT(S)

JUDICIAL ACTION

DISPOSITION OF EVIDENCE, GRAND JURY MATERIAL, AND/OR PERSONAL PROPERTY

MONETARY ACHIEVEMENT

SUBMITTED BY:

Signature of Reporting Agent

Date

APPROVED BY:

Signature of Approving Supervisor

Date

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). This report is FOR OFFICIAL USE ONLY, including, but not limited to, its use in the claims adjudication process. It may not be copied or reproduced without written permission from the SSA OIG; however, for purposes of claims adjudication by SSA, including the DDS and the ODAR, it may be copied and incorporated into official claims files. Disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552 and 552a.

Exhibit 3-7

Reserved for Future Use



**COOPERATIVE DISABILITY INVESTIGATIONS UNIT
[CITY, STATE]**

**SUMMARY REPORT OF INVESTIGATION
TRANSMITTAL AND RECEIPT FORM**

PLEASE DETACH THIS FORM FROM THE REPORT, COMPLETE THE BOTTOM SECTION, AND RETURN THE FORM TO THE CDI UNIT IN: [CITY, STATE]

Transmittal Date:	CDI Reference Number:
Destination:	SSA Office:
Referral Received:	DDS Branch:
Referral Source:	Name..... Address..... Telephone.....
Allegation(s):	

SUBJECT:

Name.....
SSN.....
Address.....

Telephone.....

CHECK ONE: Claimant Representative Interpreter Doctor Lawyer Other

TO BE COMPLETED BY SSA, DDS, OR ODAR EMPLOYEE: CHECK ONE

SSA DDS ODAR

____ The CDI Summary ROI was considered during the disability determination. Reg Basis/Reason Code: ____

____ The CDI Summary ROI was not considered during the disability determination. Reg Basis/Reason Code: ____

____ The disability claim was adjudicated prior to receipt of the CDI Summary ROI. Reg Basis/Reason Code: ____

____ The disability claim (initial) was allowed or disability benefits were continued. Reg Basis/Reason Code: ____

____ Other/Comments:

STAFF SIGNATURE	PRINTED NAME	TITLE	DATE



SUMMARY REPORT OF INVESTIGATION

COOPERATIVE DISABILITY INVESTIGATIONS UNIT
[CITY, STATE]

Subject:
SSN:
DOB:
CDI Reference Number:
Date of Report:

OIG Point of Contact:	Name, Title
	Telephone Number
DDS Point of Contact:	Name, Title
	Telephone Number

I. SUBJECT DATA

CDI Reference Number:

Name:

SSN:

DOB:

Related Reference Number(s):

II. SYNOPSIS

Highlight any inconsistencies in the claimant's record and synopsise investigative results that directly influence the adjudication process.

III. NATURE OF REFERRAL

Identify date and source of referral.

Summarize the complaint.

IV. TYPE OF CLAIM

Specify Title II, Title XVI, or concurrent pay.

Indicate whether initial claim or in-pay.

V. ALLEGED DISABILITY / FUNCTIONAL LIMITATIONS

List the claimant's alleged impairments.

Summarize the subject's responses to the daily activities questionnaire, and any third-party information.

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). This report is FOR OFFICIAL USE ONLY, including, but not limited to, its use in the claims adjudication process. It may not be copied or reproduced without written permission from the SSA OIG; however, for purposes of claims adjudication by SSA, including the DDS and the ODAR, it may be copied and incorporated into official claims files. Disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552 and 552a.

VI. DETAILS OF INVESTIGATION

Provide appropriate background data obtained from (b) (7)(E)

Provide a detailed account of all investigative activities conducted in the field.

VII. LIST OF EXHIBITS

Include as attachments to the report all appropriate witness statements, automated printouts, photographs, etc. and list them by description and exhibit number in this section. Local preferences, as agreed to by OIG, SSA, DDS, and ODAR officials, may dictate how much supporting documentation to provide.

VIII. SIGNATURES

Submitted By:

Special Agent / CDI Team Leader

Date

Approved By:

Assistant Special Agent in Charge or
Resident Agent in Charge

Date

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). This report is FOR OFFICIAL USE ONLY, including, but not limited to, its use in the claims adjudication process. It may not be copied or reproduced without written permission from the SSA OIG; however, for purposes of claims adjudication by SSA, including the DDS and the ODAR, it may be copied and incorporated into official claims files. Disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552 and 552a.

**FBI Laboratory
Buccal Collection Kit Re-Order Form**

Please allow 2 weeks for delivery of collection kits.

Date Requested: _____
Agency Requesting Kits: _____
Person Requesting Kits: _____
Number Of Kits Needed: 50____ 100____ 150____ 200____ Other____ (multiples of 50)

Number Of Additional Forms Needed: _____

Note: An additional supply of forms equivalent to 10% of your total kit order will be included automatically

Shipping Address:
Facility: _____
Address: _____
Address: _____
City: _____
State, Zip Code: _____
Phone Number: _____
Fax: _____
Point of Contact: _____

**PLEASE FAX YOUR REQUEST DIRECTLY TO
The FBI Laboratory
AT (703) 632-7620**

IF YOU HAVE ANY QUESTIONS, PLEASE CALL (703) 632-7529

Official Use Only

Date Request Received: _____
Request Approved By: _____
FBI Release Number: _____
Date Request Sent To Contractor: _____

Methodology for Calculating Title II and Title XVI Disability Program Savings

Savings Attributable to Initial Claims	
Title II Initial Claim	\$74, 364
Title XVI Initial Claim	\$40, 484
Concurrent Initial Claim	\$47, 814

Savings Attributable to In-Pay cases	
Monthly Benefit Amount	\$1,062
Monthly Benefit Amount times 61.6	\$12,744
SSA Program Savings Amount	\$65, 419

*These percentages will be updated each fiscal year based on information provided by SSA.

Exhibit 3-11

CJIS Fingerprinting Supply Requisition Form

Click on Icon to obtain form.



1-178

1_requisition_form.p



MEMORANDUM

Date: ENTER INFO

Refer To:

To: Click here for SAC's Name

From: (b) (6)
Assistant Inspector General for Investigations

Thru: Special Agent-in-Charge or Director, Intelligence and Analysis Division

Subject: Request for Audit and Financial Forensic Assistance

Case Number: (Input OI Case Number)

Brief description of case:

1. Reason for Assistance Needed:
2. Description and Location of Evidence: (to include number of beneficiaries, claims, or entities involved)
3. Offense(s):
4. Duration and Dates for Assistance:
5. Name of OI Supervisor Overseeing the Investigation
6. Additional Items for Consideration and/or Unusual Expenses:

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.**

U.S. Department of Justice
Federal Bureau of Investigation
Criminal Justice Information Services Division
National Instant Criminal Background Check System (NICS)



FEDERAL LIAISON ATTENTION: NICS INDEX SUBMISSION

EMAIL: (b) (6) TOLL FREE FAX: (b) (6)

FEDERAL LIAISON: (b) (6) PHONE: (b) (6)

FROM: _____ DATE: _____

NAME OF OFFICE: _____ PHONE: _____

FAX: _____ EMAIL : _____

Subjects of a NICS Index submission are required to contain the subject's Name, DOB, Sex, and Race. Any additional descriptors are highly recommended. Please ensure the attached documentation contains those items.

9999991216

INVESTIGATIVE GUIDELINES AND PROCEDURES

004.000 Types of Investigations

- A. Investigations conducted by special agents (SA) of the Office of Investigations (OI) are classified as:
1. **External** – Investigations of individuals and organizations, who commit, or attempt to commit fraud against the programs administered by the Social Security Administration (SSA), commonly referred to as “program fraud.”
 2. **Internal** – Investigations of employees of SSA who are involved in, or suspected of being involved in, criminal activities in the workplace. These activities may relate to theft, disclosure of information, accepting of bribes, or violations of other Federal statutes.
 3. **SSN Misuse** – Investigations involving the misuse of a Social Security number (SSN) or a number purported to be an SSN, for any purpose, with the intent to deceive, and not otherwise associated with program fraud and/or internal misconduct.
 4. **Background** – Investigations relating to pre-employment screening of applicants under consideration for positions with any component of the Office of the Inspector General (OIG).
- B. The primary focus of OI’s investigative activities is on allegations of felonious violations of law and otherwise substantive civil and/or administrative misconduct. Allegations of malfeasance such as time and attendance issues should be referred directly to SSA management.
- C. Substantiated violations of Federal law must be referred to the Office of the United States Attorney in the district in which the violation occurred. That office is responsible for deciding if the violator will be prosecuted in Federal court or if prosecution will be declined. Agents may consider referring a case to State or local prosecutors after prosecution has been declined federally.
- D. Especially Sensitive Targets - Investigations involving certain classes of persons may result may result in serious security concerns, especially regarding the (b) (7)(E) [REDACTED]. Therefore, investigations must be coordinated with the Office of Enforcement Operations, Criminal Division, Department of Justice, when the investigation:

(b) (7)(E) [REDACTED]

[REDACTED]

[REDACTED]

(b) (7)(E)

- E. Investigations that require coordination with the Office of Enforcement Operations and are not conducted with the participation of the Federal Bureau of Investigation may not be disclosed to any other agency without the explicit approval of the Office of Enforcement Operations.

004.010 Program Fraud Investigations

- A. The two sections of the Social Security Act, as amended, for which the OIG has primary investigative authority are:

1. Title II (Federal Old-Age, Survivors, and Disability Insurance)

- a. Retirement benefits are monthly benefits paid to individuals who have reached retirement age, and who have worked and attained fully insured status. Auxiliary benefits are also paid to eligible family members and spouses.
- b. Survivors benefits are paid to certain members of a deceased insured individual's family including widow, divorced widow, widower, divorced widower, and/or minor children.
- c. Disability benefits are paid to individuals who have been found to be disabled within the scope of Social Security law, and have insured status. Auxiliary benefits are also paid to eligible family members.
- d. SSA benefits are paid from the SSA Trust Fund.

2. Title XVI (Supplemental Security Income)

- a. Title XVI benefits are paid from general revenue funds, not from the Social Security Trust Fund.
- b. A needs-based benefit program for the aged (65 or over), blind, and disabled who have limited income and resources, and who do not have fully insured status.
- c. The amount of the Supplemental Security Income (SSI) monthly benefit is determined by the applicant's other income, living arrangements, and other circumstances that affect his/her financial needs.

- B. The definition of *disability* under SSA law, whether Title II or Title XVI, is that a person must be *totally disabled*. This includes a medical condition(s) that prevents the individual from working. The disability or combination of disabilities must also be expected to last for at least 12 continuous months, or result in death. There is no partial payment for a percentage of disability under SSA law as there is under other programs, such as those of the Department of Veterans Affairs (VA), which has its own definition of disability. Thus, a person may be receiving benefits from VA, but not be eligible for benefits for SSA or SSI purposes.

004.020

Investigation of Representative Payees

- A. A Representative Payee (RP) is a person or organization that receives benefits on behalf of the beneficiary. A person who acts as a RP is usually a relative or friend of the beneficiary. An organizational RP can be a for-profit or non-profit organization. Some of these organizations can be approved by SSA to charge a fee for their services.
- B. RP investigations primarily involve the misuse of benefits by the RP, but they also include the concealment of information affecting the beneficiary's eligibility. Examples include, but are not limited to:
 - 1. RP of minor child/children who fails to report that the child/children are no longer in his/her care or custody, *and* the RP fails to provide for the child's care.
 - 2. RP converts the funds to his/her own personal use.
 - 3. RP fails to report that the beneficiary is incarcerated.
 - 4. RP fails to report that the beneficiary is deceased.
- C. Investigative steps for allegations of RP misconduct include, but are not limited to:

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

004.030

Disability Investigations

- A.** The issue of disability within SSA is extremely complex. Under both Title II and Title XVI disability, an individual meets the definition of disability if he/she is unable to perform past relevant work, but also cannot perform any other type of work (significant gainful activity or SGA) because of a physical or mental impairment which has lasted, or is expected to last, for at least 12 months, or which can be expected to result in death. The amount an individual can earn in order to meet the SGA standard changes each year. Consult the SSA Intranet for the current amount (<http://mwww.ba.ssa.gov/cola/>). If an individual is found to have engaged in a number of successive months of SGA, SSA may suspend disability payments. Spouses and minor children of disabled wage earners may also be entitled to Title II auxiliary payments, Disabled Widow(er) payments, and Disabled Child payments.
- B.** Disability investigations must pursue two distinct goals. The first goal, criminal prosecution, is most significant. The second goal, however, involves an administrative determination from SSA that will facilitate in suspension of payments and collection of overpayments. OI disability investigations must address both the regulatory requirements for payment suspension as well as the amount of fraud loss that results from the subject's illegal activities. Fraud loss in SSA program cases, including disability cases, is determined by SSA upon application of current Social Security regulations. Not only will the amount of fraud loss usually impact sentencing in any criminal prosecution, but it also represents the sum of money that SSA will attempt to collect as an "overpayment." Issues of eligibility, trial work period (see Section 004.030 C), SGA, medical determinations, etc., will impact SSA's administrative payment suspensions and the eventual calculation of fraud loss. It is, therefore, imperative that OI's disability investigations address SSA's administrative requirements.
- It should be noted that in some cases, an OI disability investigation has resulted in a criminal conviction for false statements and an associated court ordered restitution. However, the SSA administrative process was not addressed during the investigation. When SSA applied disability regulations to the facts after the conviction was obtained, it was determined that no overpayment had occurred. When received by SSA, the restitution payments ordered by the court were returned to the subject. This type of situation can be avoided through early coordination with SSA.
- C.** Under Title II disability, there is a five-month waiting period from the month SSA establishes the date of onset of the disability until SSA benefits begin. There is also a provision in the SSA law that allows disabled beneficiaries to a nine-month (not necessarily consecutive months) Trial Work Period (TWP). The beneficiary can still receive disability benefits while attempting to become gainfully employed or self-employed. If the work attempt is successful, the disability will be found to cease in the 10th month, and benefits terminate in the 12th month. The *Social Security Protection Act of 2004*, Public Law 108-203, provides that an individual who is convicted by a Federal court of fraudulently concealing work activity during the trial work period (TWP) is not entitled to receive a disability benefit for TWP months that occur prior to the conviction but within the same period of disability. If payment has already been made, he or she is liable for repayment plus restitution, fines, penalties and assessments.
- D.** Under Title XVI, the eligibility of an individual who is blind or disabled is determined on the basis of a monthly assessment of the individual's income and resources. The amount of the SSI benefit depends on how much other income an individual receives, the living arrangements, and other circumstances that affect an individual's financial needs. False statements on initial

applications for Title XVI disability benefits are prosecuted under Title 42, United States Code, Section 1383a(a)(1).

E. Other widespread types of disability investigations involve:

1. Concealment of work and earnings (Title II: 42 USC 408(a)(4); Title XVI: 42 USC 1383a(3)).
2. Concealment of assets, living arrangements, or other income (Title II: 42 USC 408(a)(4); Title XVI: 42 USC 1383a(a)(3)).
3. Falsifying the condition or severity of the disability (Title II: 42 USC 408(a)(3); Title XVI: 42 USC 1383a(a)(2)).
4. Impersonation to include the use of another individual's identity and SSN to receive benefits (Titles II and XVI: 42 USC 408(a)(7)(B)).
5. Individuals/Institutional entities that have received benefits as a representative payee on behalf of a beneficiary and then used the benefits for something other than for the use and benefit of the beneficiary (Title II: 42 USC 408(a)(5); Title XVI: 42 USC 1383a(a)(4)).

F. Investigative steps for allegations of disability fraud include, but are not limited to:

1. (b) (7)(E) [Redacted]
2. (b) (7)(E) [Redacted]
 - a. (b) (7)(E) [Redacted]
 - b. (b) (7)(E) [Redacted]
 - c. (b) (7)(E) [Redacted]
 - d. (b) (7)(E) [Redacted]

(b) (7)(E)

3. (b) (7)(E)

4. (b) (7)(E)

a. (b) (7)(E)

b. (b) (7)(E)

1. (b) (7)(E)

2. (b) (7)(E)

5. (b) (7)(E)

a. (b) (7)(E)

b. (b) (7)(E)

004.040 Deceased Payee Investigations

A. SSA beneficiaries are not entitled to benefits after death. Deceased payee investigations involve the improper payment of SSA benefits to beneficiaries, after their death. SSA is usually notified of a beneficiary's death by the funeral home, relatives and/or as the result of a computer death match conducted between SSA and various states, after which SSA terminates the beneficiary's benefits. Whether by error, omission or fraud, if SSA is not notified of a beneficiary's death, or if the provided information is incorrect, the monthly benefits may continue and an overpayment will occur. After confirmation of death and computation of the overpayment, SSA makes a referral of potential fraud to the OIG.

B. Investigative steps for deceased payee investigations include, but are not limited to:

1. (b) (7)(E) [REDACTED]
2. (b) (7)(E) [REDACTED]
 - a. (b) (7)(E) [REDACTED]
 - b. (b) (7)(E) [REDACTED]
 - c. (b) (7)(E) [REDACTED]
3. (b) (7)(E) [REDACTED]

C. Subjects of Deceased Payee investigations are usually:

1. the beneficiary's RP;
2. the child or relative of the beneficiary who assisted with their care prior to death (and who may also be the Informant on the death certificate); or
3. the parent/guardian of a child or severely disabled adult.

004.050 Case Opening Guidelines for Allegations of SSA Employee Misconduct

- A. (b) (7)(E) [REDACTED]
- B. An investigation will be opened if the complaint information involves the following:
1. A violation of a felony statute of Federal law within the jurisdiction of the SSA OIG which potentially falls within prosecutorial guidelines for accepting the case for prosecution.
 2. Any employee's alleged misconduct that is considered an official matter (i.e., conduct which reflects adversely on the employee's suitability for continued employment or adversely affects the performance of his/her duties) and that, if proven, could lead to the removal of, or other serious disciplinary action against the employee. (b) (7)(E) [REDACTED]

3. (b) (7)(E)

- C. Regardless of whether or not they are SSA employees, all individuals retain their Fifth Amendment right against providing self-incriminating testimony in a criminal investigation. **Any** SSA employee who is a suspect in a criminal or an administrative misconduct investigation, but who is not in custody, **must** be given either a Federal Employee Advice of Rights (*Form OI-15, Exhibit 4-1* [*Spanish, 4-2*]), or Kalkines (*Form OI-14, Exhibit 4-3, [Spanish, 4-4]*).
- D. An [Employee Investigation Checklist \(Form OI-89\)](#) is provided as a tool to assist the SA with the significant steps of an employee investigation.

004.055 Employee Misconduct Notifications

- A. OI FDs will notify the appropriate regional Desk Officer in the Criminal Investigations Division (CID) at OI Headquarters upon receipt of substantive allegations of criminal misconduct or egregious non-criminal misconduct by SSA employees. The OI FD will complete the “Report of Alleged SSA Employee Misconduct” memo, Form OI-84, (*described in section D*) which documents possible SSA employee misconduct. The Desk Officer will forward a copy of this document to the Deputy Assistant Inspector General for Investigations-Field Operations (DAIGI-FO) through the Special Agent-in-Charge (SAC) of CID. You must have an open allegation to conduct any investigation.
- B. Upon receipt of allegations involving SSA employees at the GS-15 level or above, including Senior Executive Service (SES), the OI FD should notify the regional Desk Officer by telephone **within 24 hours** and confirm in writing, through their Desk Officer, within 3 working days. The FD will conduct the investigation.
- C. Upon receipt of allegations involving SSA employees below the GS-15 level, the FD will notify the SAC CID, through their regional Desk Officer, **within three (3) working days**.
- D. The “Report of Alleged SSA Employee Misconduct” memo, Form OI-84, ([Exhibit 4-5](#)) should contain:
1. The employee’s name, position title, grade, and organizational component.
 2. The date the complaint was received or the incident was otherwise discovered.
 3. The OI allegation or case number and case agent’s name.
 4. A brief description of the suspected violation.
 5. The action the FD has taken or plans to take (include dates).
 6. Information as to other significant factors such as:
 - a. media interest

- b. relation to other investigations
 - c. monetary impact
7. An indication whether the FD has any objections to OIG HQ notifying the employee's senior management of the existence of the complaint.
- E.** Once OI substantiates allegations as criminal violations, the appropriate division of the United States Department of Justice, Office of the United States Attorney, must be notified. This notification must be made within 30 days after the allegation is substantiated. The referral may either be verbal or in writing, as preferred by the United States Attorney.
- F.** OI will notify the Director, (OGE), 1201 New York Avenue NW, Suite 500, Washington, DC, 20005 (telephone 202-482-9300 or fax 202-482-9237) of all conflict of interest cases (violations of 18 U.S.C §§ 203, 205, and 207-209) referred to a United States Attorney for prosecutive consideration on OGE Form 202, and will inform the OGE of subsequent developments relative to the referral.

004.060 Notifications for OIG Employee Allegations of Misconduct

- A.** If an OIG employee is implicated, notifications shall be made to the DAIGI – Field Operations and the Office of Quality Assurance and Professional Responsibility (OQAPR) (see Chapter 11, Section 011.050).
- B.** OQAPR will investigate allegations against OI employees. The results of their investigation will be reported to the SA's SAC in a report format. OQAPR shall maintain all records relating to these investigations.

004.065 Employee Case Notifications at Conclusion of the Investigation

- A.** Upon completion of SSA employee investigations, the OI Field Division (FD) Special Agent-in-Charge (SAC) will prepare a SAC Summary Memorandum (*Exhibit 4-6A*) and provide supporting documents or forms (i.e. Warnings and Assurances to Employee Required to Provide Information-Kalkines/Form OI-14, Warnings and Assurances to Employee Required to Provide Information on a Voluntary Basis-Garrity/Form OI-15, and Witness Statements-Form OI-16) to the appropriate SSA official, outlining the results of the investigation with certain information redacted.
- B.** Address all confidentiality and privacy concerns within the summary memorandum before releasing such information to the agency. This requires the removal of the following information:

1. (b) (7)(E) [REDACTED]
2. (b) (7)(E) [REDACTED]
3. (b) (7)(E) [REDACTED]
4. (b) (7)(E) [REDACTED]

- C.** Consult with the Office of Counsel to the Inspector General (OCIG) if it is determined that privacy concerns may be compromised by the release of such information to the agency.
- D.** The SAC Summary Memorandum ([Exhibit 4-6A](#)) should include the following:
1. A narrative overview of the OIG investigation which substantiates or does not substantiate the allegation (s);
 2. A statement that copies of Reports of Investigation may be made available upon request by the appropriate SSA official;
 3. A request for written feedback of any administrative action within 60 days (if applicable);
 4. Include a reminder that such information should be protected by the agency under relevant Privacy Act standards;
 5. A statement encouraging the agency maintain a list of all SSA employees with access to the memorandum and any supporting documentation.
- E.** OCRM never recommends disciplinary action in the SAC Summary Memorandum, or any other communication. Do not attend meetings where potential disciplinary action will be discussed. Disciplinary action lies solely within the discretion of the agency.
- F.** Prior to disclosure to the agency, the OI FD SAC will send a signed copy of the summary memorandum and any supporting documents to Headquarters through CID's Desk Officer for review and final approval by the SAC of CID, Deputy Assistant Inspector General for Investigations (DAIGI)-Field Operations (FO), and Assistant Inspector General for Investigations (AIGI).
- G.** Once the OI FD SAC has received approval from Headquarters, the OI FD SAC will transmit the SAC Summary Memorandum and all supporting documents for presentation as follows:
1. Regional SSA employees – to the relevant SSA Regional Commissioner.
 2. Regional or non-headquarters Office of Disability Adjudication and Review (ODAR) employees GS-14 and below – to the Regional Chief Administrative Law Judge (ALJ) in the appropriate region.
 3. Headquarters (HQs) SSA employees (to include ODAR HQs employees) or ODAR employees GS-15 and above – to the DAIGI-FO.
 4. Office of Central Operations (OCO) employees located in the field but whose management is located at HQs – to the DAIGI-FO.
- H.** AIGI Summary Memorandum ([Exhibit 4-6B](#)) is used when the AIGI transmits employee case information and all supporting documents for presentation as follows:
1. Regional SSA employees – to the Deputy Commissioner, Office of Operations.
 2. Regional or non-headquarters ODAR employees GS-14 and below – to the Deputy Commissioner, Office of Disability Adjudication and Review.

3. HQ SSA employees (to include ODAR HQs employees) or ODAR employees GS-15 and above – to the appropriate Deputy Commissioner, Chief Actuary, or General Counsel.
 4. Office of Central Operations (OCO) employees located in the field but whose management is located at HQs – to the appropriate Deputy Commissioner.
- I.** If the agency does not respond within 60 days, a subsequent summary memorandum should be sent by the field division SAC, utilizing the same form ([Exhibit 4-6A](#)). Field divisions that do not receive a response from the agency within 60 days after sending a second summary memorandum, should notify CID and provide Headquarters a copy of the second summary memorandum. CID will draft a memorandum for the AIGI to send to the appropriate SSA Deputy Commissioner to request a report regarding SSA's disposition of the matter. If no response is received in 60 days, the AIGI will then ask the IG to send a letter to the appropriate SSA Deputy Commissioner to request a status report.
- J.** Once the SAC and AIGI Summary Memorandums ([Exhibits 4-6A and 4-6B](#)) and supporting documents are released to the agency, the OIG no longer has control over the information. The agency has authorization to copy and reproduce such documents or any provided reports, although they must still comply with all Privacy Act requirements regarding disclosure outside the agency. The agency may ultimately use the memoranda and/or exhibits in administrative proceedings, such as Merit Systems Protection Board hearings, which may result in the subject of the investigation being provided access to the documents and any provided reports. Therefore, it is imperative that all confidentiality and privacy issues are addressed prior to the release of such documents and any provided reports to the agency.

004.070 Types of Employee Misconduct

The following is a description of fraudulent activities that may be committed by SSA employees and investigated by the SSA OIG. This list is not all-inclusive; other types of fraud activities may be uncovered:

- A.** Misuse of SSA Data Bank Information/ System Security Violation – These cases involve accessing SSA computerized records. System Security Violations where the employee accesses the SSA databases, i.e. MBR, SSR, DEQY, and NUMI are the most common. The violations range from simple browsing based on curiosity, to accessing records for personal gain, to assisting family members, or for malicious intent. A common scheme is the sale of Numident information to outside parties who use the personal information relating to the account holder (e.g. mother's maiden name) to activate stolen credit cards. SSA employees have been known to misuse the SSA records for revenge, such as inputting a death termination on someone that they did not like. (An explanation of MBR, SSR, DEQY and NUMI can be found in Chapter 6).
- B.** Sale of Social Security Account Number Cards – SSA employees open legitimate SSN accounts in the names of individuals not entitled to receive them. Purchasers of the SSNs include illegal aliens seeking employment, drug dealers laundering money, fugitives hiding under another identity, and others seeking to create new identities for financial fraud.

- C. Conspiring to Fraudulently Secure Benefits – This includes cases where the SSA employee falsifies records to enable others to obtain benefits to which they are not entitled. Examples of this include falsifying evidence (e.g. recording a date of birth earlier than the true date to enable payment of benefits), changing medical denials to approvals, inputting an Administrative Law Judge (ALJ) decision other than the one actually rendered, and waiving an overpayment when the case does not meet the requirements for a waiver.
- D. Diversion of Government Funds – This area encompasses a wide range of fraudulent activities. Some of the types of fraud perpetrated by SSA employees include; diverting monthly payment checks to their own accounts when receiving information that the payee has died; creating fictitious underpayments that are routed to their own accounts or to a co-conspirator’s account; and stealing refund remittances, office cash, and SSA blank checks.
- E. Soliciting Bribes – In most instances, the SSA employee is approached to perform an act in return for a monetary or other reward. There are cases where the SSA employee solicits a bribe directly from an applicant. Examples of this include requests for “fees” to process an SSN application, or to expedite the processing of a claim for benefits.
- F. Voucher Fraud – The main area of voucher fraud committed by SSA employees involves per diem reimbursement. Employees have submitted fraudulent hotel bills when, in fact, they rented cheaper accommodations or stayed with friends or at a relative’s home for free. Other areas include submission of fraudulent invoices to falsely justify business expenses, and false bills for taxi expenses when cheaper forms of public transportation were utilized (e.g. busses and subways).

004.075 Computer Assistance in Employee Investigations

A. Intelligence and Analysis Division

- 1. The IAD’s Information Technology (IT) Specialist will be assigned to extract specific information from SSA records which may be beneficial in employee investigations.
- 2. Proper procedures for requesting assistance from IAD can be found in Chapter 5, Section 005.090 (Data Mining and Analysis Team).

B. Digital Forensics Team

- 1. The Digital Forensics Team (DFT), which is part of OI’s Criminal Investigations Division (CID), can provide specialized support for employee investigations. DFT can assist in analyzing (b) (7)(E)

The acquisition of this information is sensitive and should only be requested if there is reason to believe that access to this information is likely to produce evidence. DFT should always be notified in cases that involve criminal misuse of a government computer.

- a. To determine if computer forensic assistance is an appropriate measure, contact the Assistant of the Special Agent-in-Charge (ATSAC) of DFT by either phone

or email. If, after consulting with the ATSAC of DFT, it is determined that assistance is necessary, an official request must be submitted.

- b.** For an official request, the SA should send an electronic request through the National Investigative Case Management System (NICMS), “Request DFT” tab on the “Case Data” screen. The request should include the following:

 - 1.** Identify the employee’s status (current/former);
 - 2.** Employee’s title and duty station;
 - 3.** Brief synopsis of alleged activity and nexus of misconduct relevant to the employee’s employment/position (i.e. utilizing SSA equipment for personal use while on duty);
 - 4.** Indicate any preliminary work conducted by SSA;
 - 5.** Advise if employee misconduct is criminal or administrative in nature;
 - 6.** Indicate the criminal statutes violated;
 - 7.** Advise if an Assistant United State’s Attorney or local prosecutor is assigned to the employee investigation; and
 - 8.** Indicate the type of assistance required and why (e.g. (b) (7)(E) [REDACTED])
- c.** Once the request is received and approved by the agent’s Assistant Special Agent-in-Charge (ASAC)/Resident Agent-in-Charge (RAC), the request will be forwarded directly to the ATSAC of DFT for initial review.
- d.** The DFT will review the request for appropriate information. If the request does not have the required information, the ATSAC will contact the SA to ensure the required information is included within the request. When the request is approved, it will be sent to the DAIGI for final approval, in consultation with the AIGI and Deputy IG. When the DAIGI approves the request, it will be routed back to the DFT for assignment.
- e.** Once the request is received by the DFT, from the DAIGI, it will be assigned to a Computer Forensic Examiner (CFE) who will contact the SA within two business days to discuss the details of the request. Once the requested material is received, the data will be analyzed in accordance with the policies and procedures of the DFT. An examination report detailing the results of the analysis will be completed and provided to the case agent.
- f.** Contact the DFT’s ATSAC with any questions or for guidance regarding your request. For a listing of the DFT ATSAC and CFEs, go to [OIG’s SharePoint>Directories>Office Directory>Digital Forensics Team](#).

004.080

Duty of Employee to Cooperate

- A.** SSA employees are obligated to give information to SSA OIG when called upon, if the interview relates to official matters and/or if the information was obtained in the course of employment, or as a result of relationships incident to employment. This obligation includes furnishing a signed statement. Failure to respond by not submitting to an interview, not providing required information, or not appearing as a witness in an official proceeding could result in disciplinary action up to and including dismissal from government service.

- B.** SSA employees are generally required to assist OIG investigators in the performance of their official duties. Section 1.2 of SSA's Annual Personnel Reminders, "Support of SSA Programs," states that all employees "are required to assist the Inspector General and other investigative officials in the performance of their duties or functions. This requirement includes the giving of statements or evidence to investigators of the Inspector General's office or to other SSA investigators authorized to conduct investigations into potential violations."

The effect of this policy is that an SSA employee who has no foreseeable criminal exposure can be compelled to cooperate with OIG. This policy can be found on the Intranet at <http://personnel.ba.ssa.gov/ope/cpps/APR-Part1-2.html>.

- C.** (b) (7)(E) 

- D.** If an SSA employee with no foreseeable criminal exposure refuses to cooperate in an official investigation, the SA will advise the employee of the standards of conduct requirement as noted above, and will give the employee a Request for Information or Assistance (Form OI-56, [Exhibit 4-7](#)).
 - 1.** If the employee still refuses to cooperate, the immediate supervisor of the employee may be asked to order the employee to cooperate.
 - 2.** If the employee still refuses to cooperate, the matter should be directed through supervisory channels to the AIGI for referral to SSA.

- E.** Generally, an SSA employee who has foreseeable criminal exposure will not be compelled under the Standards of Conduct to cooperate with an OIG investigation. Any compelled statement obtained would not be admissible in a criminal proceeding against that employee.

004.085

Employee Misconduct with Prosecution Potential

- A. The fact that a subject is an employee of the Federal Government in no way diminishes the constitutional right not to be compelled to give information that could be used against the employee in criminal proceedings.
- B. However, the Government may require its employees to account fully for their actions in the course of their official duties. This requirement sometimes conflicts with the employee's right against self-incrimination. The United States Supreme Court and other Federal courts have established the following legal principles to accommodate the legitimate interests of both the Government and the employee:
 - 1. Any statement given by a public employee based upon a threat of dismissal from his/her job if the employee fails to provide such statement will be inadmissible against the employee in subsequent criminal proceedings.
 - 2. A public employee who is being questioned in any proceeding about a matter that could result in a criminal prosecution of him or her may not be dismissed solely for invoking the Fifth Amendment privilege and refusing to answer or to sign a waiver of immunity.
 - 3. A public employee does have an obligation to answer the employer's (Government's) work-related inquiries. Therefore, an employee may properly be disciplined or dismissed from his/her job for failure to answer if the employee:
 - a. is assured that the answers and information obtained as a result of those answers cannot be used against the employee in a criminal proceeding; and
 - b. is advised that he/she may be disciplined or dismissed from his/her job for failure to answer.

Note: It is SSA, not OIG, which takes administrative action against SSA employees. SAs must not suggest that OIG will discipline or recommend discipline of an SSA employee. OIG merely reports investigative findings, including failure to cooperate.

004.090

Federal Employee Rights in Criminal Investigations

- A. If an SSA employee has foreseeable criminal exposure in a case and is asked to make a statement, then the SA must give the warnings specified on the Federal Employee Advice of Rights (Form OI-15, [Exhibit 4 -1](#)).
- B. If the subject is in custody, the employee must also be advised of their full Miranda rights.
- C. If the subject exercises his/her right against self-incrimination, the interview must be terminated.

- D. If the subject agrees to make a statement, the Federal Employee Advice of Rights form must be completed in order to protect the admissibility of the subject's statement in future criminal proceedings.
- E. If the subject refuses to sign the Federal Employee Advice of Rights (Form OI-15), the SA should annotate this refusal on the form, have the form signed by the secondary SA, and articulate the subject's refusal in the ROI reporting the interview.

004.095 Federal Employee Rights in Non-Criminal Investigations

- A. If an SSA employee is the subject of investigation and does not have foreseeable criminal exposure in the case, no special warnings need to be given.
- B. The employee can be compelled under the SSA Standards of Conduct to cooperate or face disciplinary action for failure to cooperate.
- C. If the interview develops into a situation where the subject appears to have foreseeable criminal exposure, the SA shall immediately stop the interview and advise the subject of his/her rights.

004.100 Waiver of Prosecution to Obtain Cooperation of Employee

- A. Situations may arise where OIG is willing to forego the possibility of pursuing criminal action against an employee in order to compel the employee's cooperation.
- B. The Department of Justice (DOJ) has established guidelines on how to proceed in these situations:
 - 1. The matter must first be discussed with the Federal prosecutor having jurisdiction over the criminal aspects of the case.
 - 2. If DOJ approval is obtained, the SA will give the following notice, commonly referred to as Kalkines, (see *Exhibit 4-3*, *[4-4*: Spanish]) to the employee prior to questioning:
 - a. "You are going to be asked a number of specific questions concerning the performance of your official duties."
 - b. "You have a duty to reply to these questions, and agency disciplinary proceedings resulting in your discharge may be initiated as a result of your answers. However, neither your answers nor any information or evidence which is gained by reason of such statements can be used against you in any criminal proceedings."
 - c. "You are subject to dismissal if you refuse to answer or fail to respond truthfully and fully to any questions. This does not preclude criminal charges stemming from false statements or false answers made by you in this interview."
- C. The above warning is intended primarily as a means of requiring an employee with no foreseeable criminal exposure to make a statement concerning his/her work-related

actions. By removing the possibility that the statement or the fruits of the statement will be used against the employee in a criminal proceeding, SSA asserts its right to require the employee to explain his/her work-related actions or face disciplinary action (including termination) for failure to do so.

004.105 Waiver of Disciplinary Action Against an Employee

- A. A situation could arise where SSA would be willing to waive disciplinary action against an employee in exchange for a statement from that employee.
- B. In such situations, the Regional Labor Relations Officer (RLRO) may obtain, from the appropriate agency official, an agreement to waive administrative discipline in exchange for cooperation.
- C. If the employee has foreseeable criminal exposure and the Government is not also willing to forego prosecution, the terms of any such agreement between the employee and the Agency should be reduced to writing and should contain the following written disclaimer:

“Nothing contained herein shall be deemed or construed to affect criminal liability or to limit the responsibility of the Department of Justice to prosecute violation of Federal criminal laws. This agreement does not constitute a grant of immunity from criminal prosecution, and its acceptance by (employee’s name) shall constitute a knowing and personal waiver of rights under the Fifth Amendment to the United States Constitution.”
- D. The agreement containing the disclaimer must be signed by the employee being interviewed.
- E. In the event that the employee’s statement contains evidence reflecting that a criminal violation of Federal law has been committed, or in the event that other evidence is developed reflecting such a criminal violation, the signed statement containing the disclaimer shall be forwarded to DOJ when the matter is referred for prosecution.

004.110 Employee’s Right to Representation (Weingarten Rights)

A. Union Representation Permitted

POLICY STATEMENT: It is the policy of the SSA OIG that SSA employees who are members of bargaining units and are to be interviewed by OI SAs shall be permitted to have a union representative present during the interview, if the employee so requests. This is the case regardless of whether the employee is the investigative subject or a witness, regardless of whether the investigation may result in criminal prosecution, and regardless of whether the interview may result in disciplinary action.

1. Affirmative Advisement of Right to Union Representation

In addition to the above, if the SSA employee to be interviewed is the subject of the investigation, and is a member of a bargaining unit, the interviewing SA shall advise the employee at the outset of the interview that he or she is entitled to have a union representative present during the interview. Advising an employee of their entitlement to a union representative is in addition to, not in lieu of, the appropriate

advice of rights (Kalkines, Federal Employee Advice of Rights, Miranda) to be given based on the nature of the investigation.

2. Requests for a Specific Union Representative

If an employee requests a particular union representative, an interview should be delayed for a reasonable period to permit that representative to be present, but need not be delayed indefinitely to accommodate such a request.

A particular union representative may be precluded from attending the interview if “special circumstances” exist (i.e., if the requested union representative is a subject or a witness in the case, and his/her attendance would jeopardize the integrity of the investigation).

3. The Role of the Union Representative

The union representative may actively participate in the interview by posing questions and clarifying issues and by conferring with and advising the employee, but may not interfere with the interview.

If a union representative is interfering with the interview, the SA should:

- a. attempt to resolve the issues in conflict by discussing them with the union representative outside the presence of the employee. If this is unsuccessful, the SA may:
 1. proceeding without the union representative; or
 2. discontinuing the interview.
- b. either terminate the interview or give the employee the option of:

In this case, the SA should include in the record the actions taken and the reasons for taking such action. A Union Representative Advisory To SSA Employee (Form OI-80, [Exhibit 4-8](#)) should be presented to the employee and included in the Report of Investigation.

Any questions concerning union representation in interviews of SSA employees may be brought to the attention of OCIG at (410) 965-6211.

B. Attorney Representation

POLICY STATEMENT: It is the policy of the SSA/OIG/OI that any SSA employee being interviewed by OI SAs (regardless of whether the employee is the subject of the investigation or a witness) may have an attorney present during the interview. It is not, however, necessary to advise an employee of any right to legal representation, unless the interview meets the requirements of *Miranda* (see [010.050](#), “Advice of Rights”).

004.120 Exculpatory and False Exculpatory Statements

- A. When a subject denies his/her involvement or culpability in an offense, agents will make every attempt to obtain a written statement from the subject. That statement should be written in the first person and include the specific denials.
- B. The purpose of obtaining that statement is to restrict the subject from altering the account of facts of the violation to a set of facts that would be more beneficial to his/her eventual defense. (b) (7)(E)

004.130 Written Statements

In an employee misconduct case where the allegations could result in disciplinary action, obtain a sworn statement from any material witness. The reasons for this requirement include:

- 1. The attendance of a non-Government witness at a hearing on appeal from an adverse action cannot be compelled.
- 2. It may be impossible or impractical to require a Government witness to attend the hearing.
- 3. Testimony at such hearings is under oath or affirmation.
- 4. Hearing officers tend to give greater weight to sworn statements than to non-sworn statements and non-sworn oral testimony.

004.140 Allegations of Misuse of Official Time by Union Officials

- A. All incoming allegations of misuse of official time by a union official or union representative will be referred to OCIG.
- B. Allegations of misuse of official time received by the AMFED, OI FDs, and OIG HQ will be controlled with a NICMS allegation number and referred to OCIG.
- C. If possible, all initial referrals to OCIG should include all of the information set forth in Section 004.055, of this Handbook, including:
 - 1. The employee's name, position title, grade, and organizational component.
 - 2. The date the complaint was received or the incident was otherwise discovered.
 - 3. The OI allegation/case number.
 - 4. A brief description of the suspected violation.
 - 5. If a direct referral from an OI FD, the action the OI FD plans to take (include dates). The OI FD should consult with OCIG before taking any action to ensure there is legal basis and adequate support for intended actions.

6. Information as to other significant factors such as:
 - a. media interest
 - b. relation to other investigations
 - c. monetary impact
7. An indication of whether the OI FD has any objection to OIG HQ notifying the employee's senior management of the existence of the complaint.

D. Initial Determination by OCIG

1. Upon receipt of the initial referral, OCIG will either concur or disagree with the OI component's (OI FD or OI HQ) or AMFED's intended action(s). If there is a disagreement between the OI component and OCIG, OCIG's decision will be controlling.
2. In rendering its decision, OCIG will make one of the following legal findings:
 - a. OCIG has determined that the allegation does not involve misuse of official time and will refer the matter back to the originating OI component for disposition. The disposition action is decided by the OI component and can include referral to SSA management, development by an OI FD, or closure of the allegation.
 - b. OCIG has determined that the allegation involves internal union misconduct (rather than mere employee fraud) and will refer the allegation to the Department of Labor for its review.
 - c. OCIG has determined that the allegation merits an investigation (either at the incoming level or after further development by OI) and the misuse of official time is within the purview of OI, as opposed to the Department of Labor or SSA management. OCIG will refer the case to the originating OI component and recommend that OI conduct a full investigation under normal employee crime procedures as set forth in this Handbook.
 - d. OCIG is unable to provide a legal determination due to insufficient information and will refer the allegation to the originating OI component for a decision on whether to pursue further development (the understanding is that OCIG will revisit the case at a later date, if warranted).
3. If OCIG determines that the facts warrant an investigation by OI and that OI has sole jurisdiction, the appropriate OI FD will conduct the investigation.

E. Final Disposition of the Case after Full OI Investigation

1. After the appropriate investigative unit within OI has conducted a full investigation, a final ROI shall be submitted to OCIG for final disposition. Depending on the findings in the ROI, final disposition may involve referral to:

- a. DOJ for potential prosecution;
 - b. SSA management (as a party to the collective bargaining agreement with the union) for potential disciplinary personnel action, as deemed appropriate by SSA management; or
 - c. The Department of Labor, if the investigation has uncovered “internal union misconduct.”
2. If the ROI recommends closure because of a lack of evidence, OCIG will review the ROI and underlying supporting documentation, as appropriate, and either concur, or disagree and request further development by OI.

004.150 Updating the Status of Employee Cases in NICMS

- A. Employee cases should be updated no later than the last day of the quarter, i.e. March, June, September and December, unless otherwise notified by CID’s Investigative Support and Compliance Team (ISCT).
- B. When applicable, the supervisor responsible for ensuring the completion of the quarterly updates should review the last quarter’s Employee Case Report before updating the current quarter, so that the status will be logical and flow from quarter to quarter. In addition, the update should advise if the investigative steps delineated in the previous report were completed, as well as their outcome. (Example: If in the 1st quarter it states the victim will be interviewed, the update for the 2nd quarter should state when the victim was interviewed, as well as the result of the interview.)
- C. Employee cases are updated under the Case Status tab in NICMS. The NICMS Case Status tab contains the following four status fields, which should be reviewed and updated each quarter, as appropriate:
 - 1. **Case Description:** An initial description is entered during the first quarterly update after the case is opened. Thereafter, this field is updated only if the case description has substantially changed during the course of the investigation.
 - 2. **SSA Employee Status (should include one of the following):**
 - a. “Employee is/is not aware of the investigation”
 - b. “Employee is/is not still in same position”
 - c. “Employee is suspended with/without pay”
 - d. “Employee is terminated”
 - 3. **Current Status (should include):**
 - a. Investigative activities

- b. Interviews and results
- c. Arrests, etc.

4. Judicial Status (should include):

- a. Complaints
- b. Indictments
- c. Initial appearances, etc.
- d. Judicial districts and name of prosecuting agency.

D. Further detailed instructions on formatting and how to update employee cases can be found in the PowerPoint training presentation - [Quarterly Employee Case Report](#).

004.160 Social Security Number (SSN) Misuse Investigations

A. The Social Security number (SSN) has become a widespread means of identification in the United States. As its use as an identifier has grown, so has the opportunity for its misuse. Title 42, United States Code, Section 408(a)(7)(B) is the most commonly used statute in the prosecution of SSN misuse. SSN misuse occurs when an individual, for any purpose, with intent to deceive, falsely represents a number to be the SSN assigned to him/her, when, in fact such number is not the SSN assigned to him/her by the Commissioner of the Social Security Administration.

B. OI's policy is to investigate cases that involve palpable threats to the security of the SSN. Appropriate cases for OI development are based on a variety of sources, including reports and requests from SSA field offices, requests for help from other agencies at every level of government, and hotline allegations. Specifically, OI will conduct investigations when allegations involve:

1. (b) (7)(E) [REDACTED]
2. (b) (7)(E) [REDACTED]
3. (b) (7)(E) [REDACTED]
4. (b) (7)(E) [REDACTED]
5. (b) (7)(E) [REDACTED]
6. (b) (7)(E) [REDACTED]
7. (b) (7)(E) [REDACTED]

8. (b) (7)(E) [REDACTED]

9. (b) (7)(E) [REDACTED].

D. As the SSN migrated to its unintended role as the de facto national identifier, SSN misuse has become an aspect of many identity crimes in the United States. One example is the use of another person's name and SSN in an identity theft scheme to obtain driver's licenses, credit cards, loans, bank accounts, etc. In 1998, with the passage of Public Law 104-318, the *Identity Theft and Assumption Deterrence Act of 1998* (Identity Theft Act), the United States Criminal Code was amended to state that the SSN is a "means of identification" and that the unlawful transfer or use of another person's means of identification constitutes a felony. Pursuant to this Act, the Federal Trade Commission (FTC) established a centralized database to receive allegations of identity theft, which can include SSN misuse complaints. Although much of the Federal government response to identity theft issues belongs to the FTC, by law and by mission the SSA OIG has a narrow but important role in this overall effort.

E. SSN misuse cases require the application of standard investigative techniques combined with whatever intuitive approaches are suggested by experience and the facts and circumstances of the particular case under investigation. Some of the steps to take while investigating SSN misuse include, but are not limited to:

1. (b) (7)(E) [REDACTED]

2. (b) (7)(E) [REDACTED]

3. (b) (7)(E) [REDACTED]


4. (b) (7)(E) [REDACTED]

5. Obtaining statements of witnesses/subjects.

004.170 Background Investigations

A. OI is responsible for conducting limited background investigations (LBIs) on applicants recommended for employment with OIG. These background investigations are limited to inquiries concerning education, employment, and neighborhood contacts. The background investigations will cover a period of ten years for those applicants applying for Top Secret and/or Criminal Investigator positions and seven years for Secret and/or non-Criminal Investigator positions.

B. The Policy and Administration Division (PAD) will initiate a LBI upon receipt of a request from the Office of Communications and Resource Management (OCRM). PAD coordinates with the OI Field Division(s) (FDs) responsible for conducting all or part of the inquiry.

- C. PAD will create a case within the National Investigative Case Management System (NICMS) using the Program Category 818 – OI Background Investigation. All LBIs will be tracked in NICMS. PAD will provide the case number, Non-Criminal Background Investigations Forms, a copy of the applicant’s Electronic Questionnaire for Investigations Processing (eQIP), and any supporting documents regarding the applicant to the appropriate OI FD to conduct the LBI in a timely manner, usually within ten days from the date referred.
- D. The OI FD assigned the background investigation will be responsible for completing the Non-Criminal Background Investigation forms (see *Exhibits 4-9*, “Education”; *4-10*, “Employment”; and *4-11*, “Neighborhood”) documenting the investigation conducted. Once completed, all forms (education, employment, and neighborhood, to include agent notes and any additional forms obtained during the investigation) must be uploaded as an attachment in NICMS. Note: DO NOT alter the forms provided and ensure that all applicable fields on each form are completed.
- E. In the event the applicant’s employment and education background information is in the local Headquarters commuting area (State of Maryland), PAD will conduct the employment and education verification sections of the background investigation as well as contact the individual listed under the “Person Who Knew You” heading on the eQIP for places where the applicant has resided (only within the State of Maryland).
- F. (b) (7)(E) 
- G. All completed information will be directed to the ATSAC and/or SAC of PAD for review and forwarding to the appropriate DAIGI for final review and approval prior to forwarding to OCRM.
- H. OCRM will forward to OIGHR who will consider the information included on the forms (to include consultation with OCIG based on negative results of the LBI) before selecting the applicant for employment with the OIG.
- I. The Office of Personnel Management (OPM) handles the background investigation required for a security clearance. OCRM is responsible for the coordination of requests to OPM for security clearances.

004.180 Reprisals Against SSA Employees

- A. Any employee who believes that he/she has been threatened with a personnel action or any other action, or who has been harassed or harmed by any action as a reprisal for having made a complaint or provided information to the OIG, may request the OIG to review his/her complaint about such reprisal. The OIG has the authority to investigate such complaints.
- B. If OIG/OI has reason to believe that the reprisal complaint may have merit, it may, depending on the circumstances, decide to conduct an investigation or refer the matter to another entity for investigation. If the OIG refers the matter to another entity for investigation, the referral will be to:

1. the SSA Deputy Commissioner for Human Resources, or
2. the Office of Special Counsel (OSC).
 - a. An employee may also file a complaint directly with the OSC.
 - b. The OSC has the ability to seek a stay of any agency personnel action from the Merit Systems Protection Board.

004.190 Investigation of Threats and Assaults Against SSA Employees

- A. The safety of all SSA personnel and facilities is of paramount concern to the Office of the Inspector General (OIG). Section 206 of the *Social Security Protection Act of 2004*, inserted section 1129B into the Social Security Act. Codified at 42 U.S.C.1320a-8b, this section expands the role of the OIG in matters relating to the safety of SSA personnel and facilities. This law imposes criminal penalties for attempting to interfere, either by force or by threat of force, with the administration of the Social Security Act. The statute makes it a crime to attempt to intimidate or impede (corruptly or by force or threats of force) any officer, employee, or contractor of the Social Security Administration acting in an official capacity to carry out a duty under the Social Security Act, or to otherwise obstruct or impede, or attempt to obstruct or impede, the administration of the Social Security Act. This may include threats against their family.

The maximum penalty for a conviction of use of force is a fine of \$5,000 and/or three years' imprisonment. The maximum penalty for a conviction of a threat of force, but not the use of force, is a \$3,000 fine and/or one year's imprisonment.

In subsection B., below, procedures for the receipt of allegations of threats and assaults against all covered employees, contractors, and facilities, as well as for the actions that OI agents and SSA managers are expected to take when threats or assaults are reported are set forth. These instructions are intended to create a uniform OIG policy pertaining to these time-sensitive allegations and investigations. The procedures enhance OIG's ability to analyze and respond to these types of allegations/investigations.

B. Procedures

1. OI shares the responsibility for investigating reports of threats of force or use of force against SSA employees with the Department of Homeland Security Federal Protective Service (FPS), which has jurisdiction over physical property owned or leased by the Federal government (to include jurisdiction over threats of force and use of force that take place on Federal property), and with local law enforcement if the activity occurred off of federally owned or leased property.
2. OI field divisions receive allegations of threats from various sources. Generally, threats of force or use of force should be handled by the first law enforcement agency to respond to the threat, whether that is OI, Federal Protective Service (FPS), local law enforcement, or another law enforcement agency having jurisdiction. The primary objective is to stop the threat of force or use of force.
3. As soon as possible, all incidents of threats must be entered as an allegation into NICMS, and

the appropriate threat incident category level must be selected (i.e., Category 1, Category 2, or Category 3). In addition, all “Category 1” incidents must be reported to OI Headquarters through the assigned Criminal Investigations Division (CID) desk officer, via email or telephone, within one hour of being notified of the situation.

4. Upon receipt of a threat allegation, the decision to conduct an investigation and procedures to follow will be based on the seriousness and sensitivity of the incident, as defined by the following threat categories:

- a. **“Category 1” Incidents**

Definition: Incidents designated as “Category 1” (CAT 1) involve direct and imminent threats or occurrences of physical assault or endangerment against specific SSA employees and their families, contractors, and/or facilities. Examples include: an assault or threat to do bodily harm to an employee, “white powder” mailings, bomb threats (where a specific target is mentioned e.g. the Dallas Regional Commissioner’s office), or other incidents which may impede or disrupt SSA operations, or cause SSA to deviate from normal operating procedures.

In addition, any other incidents designated “sensitive” by the Assistant Inspector General for Investigations (AIGI), e.g. threats against the Inspector General, Special Agents or the Commissioner of Social Security, will be treated as a CAT 1 threat.

All reported “Category 1” incidents require OI to open an investigation under an OI case number, regardless whether or not another law enforcement agency, e.g. FPS, is also involved.

Additionally, **within 24 hours**, the Special Agent-in-Charge (SAC), or his/her designee (ASAC/RAC), will submit a “Category 1 Threat Notification Report” (CAT 1-TNR), Form OI-95, to OI Headquarters via their assigned CID desk officer, with a “cc” to the SAC and ASAC of CID (see [*Exhibit 4-21*](#)). This report will serve as a formal notification and a follow-up to the initial 1- hour required notification. The report should contain as much pertinent information as is possible, based upon what is known to OI at that particular time.

- b. **“Category 2” Incidents**

Definition: Incidents designated as “Category 2” (CAT 2) involve non-imminent or less specific threats against SSA employees, contractors, and/or facilities. This category covers instances of conditional written or verbal statements directed against an SSA employee(s), contractor(s) and/or facility about a potential, future action or event (e.g. bomb threats that are vague in nature, such as an anonymous caller states there is a bomb at SSA, yet no additional information is provided). Threats made by individuals who lack the apparent physical ability to carry out the stated threat are also included in this category.

All reported “Category 2” incidents require an OI allegation number. When an OI office receives an allegation involving this type of incident, the matter must be recorded in NICMS and developed for investigative merit. OI supervisors (SAC/ASAC/RAC) will assess the nature and circumstances surrounding the incident in order to determine whether the allegation warrants an investigation.

- c. **“Category 3” Incidents**

Definition: Incidents designated as “Category 3” (CAT 3) involve situations that may be “harassing” in nature toward an SSA employee, contractor or official; however, they do not cause any impact or direct effect on the normal operations of SSA.

All reported “Category 3” incidents must be recorded in NICMS as an allegation. Similar to CAT 2 allegations, OI supervisors (SAC/ASAC/RAC) will assess the nature and circumstances surrounding the incident in order to determine whether the allegation warrants further OI action.

***NOTE:** For any incidents (e.g. contract guards using force) that do not clearly fall within one of the three categories above, a determination will be made in conjunction with OI Headquarters as to the appropriate category and/or course of action, at the time of the notification.*

C. In responding to allegations of threats or assaults, OI Field Division personnel will:

1. Respond to the scene. Responding to the scene of a CAT 1 incident is mandatory unless otherwise directed by the AIGI or a DAIGI after discussion with the SAC. SACs, or their designee, will determine if response is required for CAT 2 and CAT 3 incidents.
2. Coordinate with any initial responders (FPS, local law enforcement, etc.), as well as the appropriate SSA officials, regarding an investigative action plan, to include the preservation of any evidence, follow-up interviews, etc.
3. Notify OI Headquarters (CID), as outlined in paragraph B of this section.
4. Query appropriate databases for additional background information on the subject (NCIC, NICMS, SSA, LexisNexis, DMV, etc.).
5. Obtain all readily available information from SSA, to include:
 - i. (b) (7)(E) [REDACTED]
 - ii. (b) (7)(E) [REDACTED]
6. Obtain copies of all reports issued by other investigating agencies and upload into NICMS, upon receipt.

A Threat/Assault Interview Worksheet ([Exhibit 4-16](#)) is available with optional items for consideration when conducting these types of investigations.
7. When conducting threat investigations, OI will not promise protection to any SSA employee or their family members, unless specifically instructed to do so by the AIGI or his/her designee.

D. Security Automated Features and Enhancements (SAFE)

1. SSA's SAFE web portal provides a centralized repository of physical security reports, information, and tools to assist and manage SSA's physical and protective security program. SAFE houses both the Automated Incident Reporting Systems (AIRS) and a library, containing various SSA security policies and memorandums.
2. All OI supervisors (SACs/ASACs/RACs) have access to SAFE via the SSA Intranet. This access allows supervisors the ability to:
 - a. monitor threats in their respective field divisions and respond to threats in a timely manner;
 - b. access AIRS reports; and,
 - c. be proactive in searching for incident patterns within their respective field divisions.
3. OI field divisions can search SAFE for AIRS incidents by SSA office codes, dates, types of incidents, etc.

E. SSA Automated Incident Reporting System (AIRS)

1. The Automated Incident Reporting System (AIRS) is an online incident-based reporting system through which data is collected for incidents, occurring in SSA facilities nationwide, that affect the safety and security of SSA personnel, property or operational capabilities.
2. SSA management is responsible for documenting all incidents that adversely impact the safety and security of SSA personnel, visitors and property by completing an AIRS Alert within two working days.
3. Incidents reported in AIRS are criminal and non-criminal events, including threats or potential threats affecting the security and safety of SSA employees and their families, guards, visitors, facilities, and records. In addition, if a VIP High Risk Alert is created, an AIRS Incident Alert must also be completed.
4. Within OI Headquarters, CID monitors AIRS incidents on a routine basis, via the Outlook mailbox, ^OIG AIRS. CID reviews all AIRS notifications to ensure the threat was reported to the appropriate OI field division. In instances where the proper field division was not notified, CID disseminates the threat accordingly. If a threat or incident has the potential to impact OI offices in areas other than where the initial threat occurred, the information is also forwarded to the corresponding field division, as appropriate.

- F.** Other Federal statutes may also apply in criminal prosecutions resulting from these investigations (see [Exhibit 4-17](#)).

004.200

Protecting the Identity of Employee Allegers

- A.** OIG/OI is authorized under Title 5, United States Code, Appendix 3, Section 7, to receive and investigate allegations from SSA employees concerning possible violations of law, rules, or regulations; mismanagement, gross waste of funds and abuse of authority involving SSA programs and operations. This statute prohibits the OIG from disclosing the identity of an employee who provides a complaint or information to the OIG without his/her consent unless such disclosure is unavoidable during the course of an investigation. OI personnel will take all necessary steps to protect the identity of an SSA employee who has made allegations and/or provided information about wrongdoing.

- B.** The provision regarding confidentiality in the IG Act does not extend to an employee who is first contacted by OIG staff during the conduct of an investigation or audit, unless the information provided is not related to the subject matter and had not been solicited during the course of the interview. The confidentiality provision also does not apply to an SSA supervisor or manager who is reporting an allegation concerning a subordinate.

004.210

Disclosure of Employee Identity

With Consent

- 1.** If an SSA employee makes a complaint or provides information to the OIG in the course of an investigation and consents to disclosure of his/her identity, such consent must be documented in the appropriate file(s).

- 2.** There may be cases in which an employee has not authorized OIG to release his/her identity. However, the employee may, inadvertently or otherwise, disclose his/her identity outside the OIG with the result that there is no longer any confidentiality to be maintained by OIG. In those cases, the OIG must verify (preferably with the employee personally) that the disclosure by the employee has actually occurred before disclosure by the OIG may be made. The appropriate file(s) must then be documented to show these actions.

B. Without Consent

- 1.** The disclosure outside SSA OIG of the identity of an SSA employee who makes a complaint or provides information in an investigation without his/her consent may be made if it is determined such disclosure is unavoidable during the course of the investigation. A determination to disclose the employee's identity without his/her consent may be made only by:
 - a.** a SAC or his/her designee; or
 - b.** an OIG/OI HQ management official at the GS-15 level or above.

- 2.** Disclosure of an employee's identity must be documented in the appropriate file(s) within 24 hours of the time the disclosure is made. The documentation will:
 - a.** Set forth the facts and circumstances that made disclosure unavoidable.

- b. Identify the person to whom the disclosure was made, showing the organizational affiliation of that person and the date of the disclosure.
3. At the time of its inclusion in the appropriate file(s), a copy of the documentation regarding the disclosure will be sent through the appropriate Regional ASAC to a Deputy Assistant Inspector General for Investigations (DAIGI).
4. When presenting cases to prosecutors, disclosures of the identities of SSA employees who are complainants or who provide information are deemed unavoidable and are not subject to the requirements above.

004.220

(b) (7)(E)

- A. Under Section 552a (k)(2) of the Privacy Act, certain investigatory material (non-criminal) may be exempted from full disclosure to the subject of the record, or a third party, if its disclosure would reveal the identity of the source (or witness) who furnished the information under an expressed pledge that the source's identity would be held in confidence.
- B. (b) (7)(E) applies only to the source's identity and to information that may tend to identify the source.
- C. Agents conducting non-criminal investigations will, if asked about confidentiality by interviewees other than subject(s), inform the person:
 1. The information provided, including the source's identity, could be disclosed to the individual being investigated if that person so requests.
 2. The witness may ask that his or her identity not be disclosed to the subject of the investigation, and the report will reflect this stipulation.
 3. The witness could conceivably still be asked to testify in a subsequent legal proceeding.

If a witness, after being advised of items 1, 2, and 3 above continues to have reservations about providing information or seeks anonymity as a condition for providing information, the agent may (b) (7)(E) if it is deemed necessary to the successful completion of the investigation.

The agent, (b) (7)(E) will inform the source that the agent's report will not identify the source. The report will state that the identity of the source is not being disclosed as the information in the report was furnished (b) (7)(E). The procedure for identifying a person (b) (7)(E) in a report will be the same as for a confidential informant.

Every effort will be made to obtain information (b) (7)(E) so that it may be used openly and freely in a hearing or administrative action. An appeal should be made to the witness on the grounds of the need to maintain public respect for government operations and programs, as well as the need to obtain all the facts so as to produce a balanced, thorough investigation.

004.230 **Avoidance of Informal Agreements**

Promises and representations made informally during employee misconduct investigations can affect criminal liability. **Under no circumstances** should an agent or any other SSA OIG official enter into informal understandings or agreements with a witness concerning the cooperation of that witness without prior consultation with, and approval of a DAIGI and the appropriate DOJ official. Such agreements are likely to be interpreted by witnesses as waiving potential criminal liability or accountability to the Agency in exchange for cooperation in the SSA OIG investigation.

004.240 **Confidential Informants**

A. Policy

1. (b) (7)(E) [Redacted]

2. (b) (7)(E) [Redacted]

3. (b) (7)(E) [Redacted]

B. CF expenditures are generally authorized for securing evidence or information, making payments to or on behalf of confidential informants and sources, making payments in connection with undercover operations, or expenditures of an emergency nature when confidentiality is crucial to the outcome of the investigation.

C. Definition and Usage

1. A *Confidential Informant* (CI) is a:
 - a. cooperating individual who has a reasonable expectation of confidentiality;
 - b. provides intelligence information and/or lawful services concerning criminal and/or other misconduct on a one-time, regular, or continuing basis;

- c. **works under the direction and control** of a special agent with SSA OIG; and
 - d. who may, or may not be compensated for the provided information or service.
2. The term “Confidential Informant” shall be strictly interpreted.
- a. CI is not synonymous with “complainant.”
 - b. CI is not to be applied to a person who willingly supplies information without concern for his/her confidentiality.
 - c. CI is not to be used to refer to a person who provides information from public records.
3. **Attorney General Guidelines** – The Attorney General Guidelines and the SSA OIG recognize the problems inherent in using CIs, such as entrapment, danger to the public, and abuse of police authority, and it therefore requires that SSA OIG obtain concurrence of a Federal prosecutor in the following situations prior to using informants:
- a. When an informant is authorized to participate in criminal activities.
 - b. When an informant or cooperating witness is a person entitled to claim a federally recognized privilege of confidentiality, such as a clergyman, attorney, or doctor.
 - c. When the aggregate payments to a confidential informant who could be a witness in a legal proceeding for services and/or expenses exceed \$25,000.
 - d. When the use of any member of the news media as a source is planned (and in such situation the prior **written** approval of a Federal prosecutor must be obtained).

D. Confidential Informant Suitability Determination – Prior to utilizing a person as a CI, it is critical that the ASAC/RAC, with the assistance of the controlling agent and the concurrence of the SAC, make a suitability determination of the individual. Thereafter, annual suitability reviews will be conducted to determine the CI’s continuing value to the SSA OIG. Factors to be considered in assessing initial and continuing suitability of an individual include the following:

- 1. The person’s age.

Policy Statement: (b) (7)(E)

- 2. The person’s alien status, if applicable.
- 3. Whether the person is a public official, law enforcement officer, union official, employee of a financial institution or school, member of the military services, a representative or affiliate of the media, or a party to, or in the position to be a party to, privileged communications (e.g., a member of the clergy, a physician, or an attorney).
- 4. The extent to which the person’s information or assistance would be relevant to a present or potential investigation or prosecution, and the importance of such investigation or prosecution.

5. The extent to which the person would make use of his or her affiliations with legitimate organizations in order to provide information or assistance to SSA OIG.
6. The nature of any relationship between the CI and the subject or target of an existing or potential investigation or prosecution, including, but not limited to a current or former spousal relationship or other family tie, and any current or former employment or financial relationship.
7. The person's motivation in providing information or assistance, including any consideration sought from the government for their assistance.
8. The risk that the person might adversely affect a present or potential investigation or prosecution.
9. The extent to which the person's information or assistance can be corroborated.
10. The person's reliability and truthfulness.
11. The person's prior record as a witness in any proceeding.
12. Whether the person has a criminal history, is reasonably believed to be the subject or target of a pending criminal investigation, or is under arrest.

NOTE: Prosecutorial concurrence **must** be obtained **prior** to using an individual as a CI **if** the individual is currently awaiting trial for any charge that contains confinement in a penal facility as part of the sentencing parameters.

13. Whether the person is reasonably believed to pose a danger to the public or is likely to conduct other criminal acts.
 14. Whether the person is a substance abuser or has a history of substance abuse.
 15. Whether the person is a relative of an employee of any law enforcement agency.
 16. The risk of physical harm that may occur to the person or his/her immediate family or close associates as a result of providing information or assistance to SSA OIG.
 17. The records of SSA OIG and any other law enforcement agency regarding the person's prior or current service as a CI, cooperating defendant/witness, source of information, including, but not limited to, any information regarding whether the person was at any time terminated for cause.
- E. Polygraph --** SACs may consider the use of the polygraph in evaluating the veracity and reliability of potential and actual CIs.
- F. Registration of Confidential Informants –** Upon approval of the SAC and the ASAC/RAC, the controlling special agent shall register the CI with the OI office supervisor by completing Form OI-27, Confidential Informant Data (see [Exhibit 4-12](#)). The OI-27 should be updated as new information pertaining to the CI is acquired. If a CI has been developed in cooperation with other law enforcement agencies, that fact should be included on the OI-27.
- G. CI Registration –** SSA OIG agents shall document and/or include the following in the CI's file:

1. A photograph of the CI.
2. Efforts to establish the CI's true identity.
3. The results of a records check with NCIC, NLETS, SSA, and other databases, as appropriate.
4. Any promises or benefits, and the terms of such promises or benefits, that are given a CI by any law enforcement or prosecuting agency (if known).
5. The original "**Agreement to Provide Information**", (Form OI-27A, *Exhibit 4-13*), which contains instructions that will be read **verbatim** to the CI by the SA (b) (7)(E) [REDACTED] That agreement outlines the CI's responsibilities and relationship to SSA OIG. (b) (7)(E) [REDACTED]

6. One original fingerprint card of the

H. Official Confidential Informant Files – (b) (7)(E) [REDACTED]

I. Issuance of Confidential Informant Numbers – (b) (7)(E) [REDACTED]

- J. Concealment of Identity** – CI numbers will be used to conceal the identity of CIs in investigative case files, reports, and memoranda. Reference to names or personal identifying characteristics will not be made in any type of official communication.

K. Documenting CI Contacts – Form OI-27B, Confidential Informant Contact Record (see [Exhibit 4-14](#)), will be used to record, in detail, all contacts and transactions with a registered CI, including in-person, telephone, and written correspondence that results in the exchange of significant information, instructions, acquisition of evidence, training, disbursement of funds, or tasking. The agent will synopsise all financial transactions during the contact, which will include the purpose and the total of all funds disbursed. The primary working agent will maintain this document in the work file during the investigation.

L. Responsibilities and Guidelines Regarding Registered Confidential Informants

1. SSA OIG agents will exercise the utmost caution to avoid interfering with or impeding any criminal investigation or arrest of a CI. No agent shall reveal any information to a CI relating to an investigation of a CI nor will an agent confirm or deny the existence of any investigation of the CI, unless authorized to do so by the appropriate prosecutor’s office.
2. SSA OIG employees shall not:
 - a. Exchange gifts with a CI.
 - b. Provide the CI with anything of more than nominal value.
 - c. Receive anything of more than nominal value from a CI.
 - d. Engage in any non-case related business or financial transactions with the CI.

Aside from making authorized expense and reward payments to CIs for information and/or assistance provided to SSA OIG, any exception to this provision requires the written approval of the SAC, in advance, when possible, based on a written finding that the event or transaction in question is necessary and appropriate for operational reasons. This written finding shall be maintained in the official CI file.

- e. Socialize with a CI except to the extent necessary and appropriate for operational reasons, as approved and documented by the ASAC/RAC.
3. (b) (7)(E) [Redacted]
4. (b) (7)(E) [Redacted]
5. (b) (7)(E) [Redacted]

M. Otherwise Illegal Behavior

1. No employee of the SSA OIG shall authorize a CI to engage in any activity that otherwise would constitute a misdemeanor or felony under Federal, State, or local law if engaged in by a person acting without authorization, except as provided for in guidelines promulgated by DOJ.
2. No employee of the SSA OIG shall authorize a CI to:
 - a. participate in an act of violence;
 - b. participate in an act that constitutes obstruction of justice (e.g., perjury, witness tampering, witness intimidation, entrapment, or the fabrication, alteration, or destruction of evidence);
 - c. participate in an act designed to obtain information for SSA OIG that would be unlawful if conducted by a law enforcement agent (e.g., breaking and entering, illegal wiretapping, illegal opening of, or tampering with the mail, or trespass amounting to an illegal search); or
 - d. initiate or instigate a plan or strategy to commit a Federal, State, or local offense.

N. Authorization

1. Otherwise Illegal Activity must be authorized in advance and in writing for a specified period, not to exceed 90 days, by the SAC **and** the appropriate Chief Federal Prosecutor. DOJ Guidelines Regarding the Use of Confidential Informants, dated May 30, 2002, enumerates specific operational requirements when Otherwise Illegal Activity is authorized for an investigation (*see Department of Justice Guidance on the OIG Employee Resource Center under Investigative/Legal Tools*). SSA OIG agents and SACs must review this document and consult with the local U.S. Attorney's Office when it appears that authorization for a CI to engage in Otherwise Illegal Activity is:
 - a. necessary either to obtain information or evidence essential for the success of an investigation that is not reasonably available without such authorization;
 - b. prevent death, serious bodily injury, or significant damage to property; or
 - c. that, in either case, the benefits to be obtained from the CI's participation in the Otherwise Illegal Activity outweigh the risks.

O. Special Notification Requirements

1. Whenever SSA OIG has reasonable grounds to believe that a current or former CI is being prosecuted by, is the target of an investigation by, or is expected to become a target of an investigation by a Federal prosecutor, for engaging in alleged felonious criminal activity, the SAC must immediately notify the Chief Federal Prosecutor of that individual's status as a CI.
2. Whenever SSA OIG has reasonable grounds to believe that a CI has engaged in any unauthorized criminal activity, the SAC shall immediately notify:
 - a. the Chief Federal Prosecutor whose district is located where the criminal activity primarily occurred;

- b. the Chief Federal Prosecutor, if any, whose district is participating in the conduct of an investigation or prosecution that is utilizing that active CI; and
 - c. the Chief Federal Prosecutor, if any, who authorized the CI to engage in Otherwise Illegal Activity.
- 3. Whenever SSA OIG has reasonable grounds to believe that:
 - a. a current or former CI has been called to testify by the prosecution in any Federal grand jury or judicial proceeding;
 - b. the statements of a current or former CI have been, or will be, utilized by the prosecution in any Federal judicial proceeding; or
 - c. a Federal prosecutor intends to represent to a court or jury that a current or former CI is or was a co-conspirator or other criminally culpable participant in any criminal activity; the SAC shall immediately notify the Chief Federal Prosecutor for that proceeding of the individual's status as a current or former CI.
- 4. In situations where the Federal prosecutor is either participating in the conduct of an investigation that is utilizing a CI, or working with the CI in connection with the prosecution, SSA OIG agents shall notify the assigned attorney, in advance when possible, if there are reasonable grounds to believe that a CI will obtain or provide information that may be subject to a legal privilege of confidentiality belonging to someone other than the CI.
- 5. If SSA OIG has reasonable grounds to believe that a current or former CI has information that is exculpatory as to a person who is, or is expected to become a target of an investigation, or as to a defendant (including convicted defendant), the SAC shall immediately notify the Chief Federal prosecutor responsible for the investigation or prosecution involving the exculpatory information.
- 6. If a Chief Federal Prosecutor seeks information from SSA OIG as to whether a particular individual is a current or former CI and states the specific basis for the request, the SAC shall provide such information promptly. If the SAC objects to providing such information, the matter should be referred to OCIG for resolution in accordance with DOJ guidelines.

P. Deactivation of Confidential Informants

- 1. At anytime an SA, RAC, ASAC, or SAC determines that a CI should be deactivated for cause or for any other reason, he or she shall immediately:
 - a. deactivate the individual;
 - b. document the reason(s) for the decision to deactivate the individual as a CI in the CI files on Form OI-27;
 - c. if the CI can be located, notify the CI that he or she has been deactivated as a CI and obtain documentation that such notification was provided.
 - d. if the CI was authorized to engage in otherwise illegal activity, revoke that authorization.

2. Delayed Notification to a Confidential Informant

- a. A RAC, ASAC, or SAC may delay providing notification to the CI during the time such notification might jeopardize an ongoing investigation or prosecution, or might cause the flight from prosecution of any person.
- b. Whenever a decision is made to delay providing a notification that decision, and the reasons supporting it, must be documented in the CI's file.

3. Contacts with Former Confidential Informants Deactivated for Cause

- a. Absent exceptional circumstances that are approved by a RAC, ASAC, or SAC, in advance whenever possible, an agent shall not initiate contacts with, or respond to contacts from, a former CI who has been deactivated for cause.
- b. When granted, such approval shall be documented in the CI's file.

4. Coordination with Prosecutors

In situations where a Federal prosecuting office is either participating in the conduct of an OI investigation that is utilizing a CI, or working with CI in connection with a prosecution, the case agent or his/her supervisor, shall coordinate with the attorney assigned to the matter, in advance whenever possible, regarding any of the decisions described in sections 1, 2, or 3 of 004.240 M.

004.250 Confidential Sources

A. Definition

Confidential Sources (CS) are those individuals who **provide pertinent investigative information to SSA OIG with a reasonable expectation of confidentiality**. A conscientious private citizen reporting suspicious or criminal activity may be registered as a CS. Similarly, individuals reporting information based on their affiliation or employment with organizations such as SSA, law enforcement agencies, the military, telephone companies, utilities companies, commercial mailbox companies, etc. may also be registered as a CS.

- B.** Individuals who provide information **on a one-time basis** (such as a telephone tip, or neighborhood canvass) are eligible to receive a **one-time only payment** for expenses and/or reward which does not exceed (b) (7)(E). Confidential Sources involved to the extent that they would incur any expense or reward beyond a "one-time payment for information" should be registered as Confidential Informants.

C. Registration and Record-Keeping for Confidential Sources

CS numbers should be assigned to the various entities described above that provide information on a confidential basis. Offices shall develop and maintain an administrative file/log that sequentially catalogues CSs used by that office. This file folder should be secured in an office safe with limited access. At a minimum, this file should include the CS number, the name of the organization, source, contact person(s), and telephone number. The **Confidential Source Registration Card**, Form OI-27C, (see [Exhibit 4-15](#)), should be utilized as a CS record system.

(b) (7)(E)

CS numbers will be used to conceal the identity of confidential sources in all investigative case files, reports, and memoranda. Offices that pay a CS for information must follow the procedures set forth in Chapter 9, "Confidential Funds," for the proper utilization and documentation of confidential funds.

- D. Law enforcement officers may be registered as Confidential Sources to protect their identity in an undercover operation, and to cover expenses (vehicle rentals, hotel expenses, and airline/train tickets) in connection with the officer's undercover duties and activities. Travel expenses of other law enforcement personnel not acting in an undercover capacity should be covered under an individual travel authorization.

004.260 Searches of Government Property

- A. As an employer, the Government has the right to ensure that the property and office space it furnishes are being used for their intended purposes. In its most recent decision addressing this issue, however, the Supreme Court has held that a public employee can have, depending upon the specific circumstances, a reasonable expectation of privacy in his/her desk, office, and filing cabinet. The Court also recognized a greater right of inspection by a supervisor than by a law enforcement officer (*O'Connor v. Ortega*, 480 U.S.C. § 709 (1987)).
- B. Assistant United States Attorney and Assistant Inspector General for Investigations approval is required before *any* search of Government property is undertaken.

004.270

(b) (7)(E)

[Redacted]

004.280 Audit Assistance in Criminal Investigations

- A. On occasion, an OI investigation may need Office of Audit (OA) assistance or may disclose administrative control and operational deficiencies that need audit attention. It is essential that such matters be brought to the attention of appropriate OA and OI officials, and handled in a uniform manner.
- B. The AIGI may request from the Assistant Inspector General for Audit any assistance required in carrying out investigations.
- C. When a FD needs audit assistance, to include financial forensic assistance, the SAC should forward his/her request for audit assistance via memorandum (see [Exhibit 4-20](#)) to the AIGI through the SAC or Director of IAD. This request should describe the nature of the assistance requested and how audit services could assist in the investigation. The information should include:
 - 1. Reason for assistance needed: the memorandum must include a reasonably detailed statement of the background of the case and nature of assistance needed.

2. Description and location of evidence: the memorandum must advise of the type of evidence being reviewed (i.e. electronic records, paper records/documents, etc); how the evidence was obtained (voluntary, search, grand jury, or inspector general subpoena); approximate volume of evidence to be reviewed; location of evidence; and whether the assistance is needed onsite in the field or can the review be conducted at OA Headquarters. The memorandum must also advise of the number of beneficiaries, claims, or entities involved.
 3. Offense(s): Include a citation of the primary alleged offense/violations and fraud loss.
 4. Duration and Dates: the memorandum must state the length of time needed for the assistance, the period to be reviewed, and desired completion date.
 5. Name of the OI supervisor who will be managing the investigation.
 6. Other: the memorandum must advise of other items for consideration, such as unusual expenses above the normal costs of business.
- D.** The SAC or Director of IAD will review the request and forward to the AIGI through the DAIGIs for final approval and forwarding to OA. For assistance with Organizational Representative Payee investigations, the SAC should forward the memorandum to the AIGI through the SAC or Director of IAD copying the SAC of CID.
- E.** When OA refers a matter to OI that may have criminal or civil potential, OI will accept the referral. OI action may include the opening of an investigation and/or the referral of the matter to another agency. If the matter is to be referred to another agency, OI will make the referral and will serve thereafter as the contact point with such agency.
- F.** When a FD has identified an administrative control or operational deficiency that may need audit attention, the SAC should forward the identified issue via memorandum to the SAC or Director of IAD. IAD will present all approved issues to OA for consideration. IAD will inform the submitting FD whether Audit will include the issue in their Audit work plan.

004.290 Responding to National/Critical Incidents (National Incident Response Plan)

- A.** In responding to incidents having national impact or deemed to have high-profile interest to the OIG, SSA or other key stakeholders, and in which OI is an active law enforcement participant, to include providing investigative support activities, the following protocols will be implemented.
- B.** OI response procedures, protocols, expectations, and communications will be dictated based upon the designated OIG response level: “*Level I*” or “*Level II*”. The Assistant Inspector General for Investigations (AIGI) or designated Deputy Assistant Inspector General for Investigations (DAIGI), in consultation with the Inspector General (IG) or Deputy IG, will be the deciding official in designating a “*Level I*” or “*Level II*” incident response and determining the activation of the National Incident Response Plan.
- C.** **“*Level I*” National Incident:** Definition- major law enforcement incidents (which may include OIG operations), acts of domestic terrorism, or natural/man-made disasters/emergencies having national implications, national media interests, or deemed high-interest by government officials to include members of Congress, the IG/DIG or SSA; *in which the OIG provides an active, significant investigative role in support of the incident.*

1. Field Division Responsibilities:

- a.** The Field Division (FD) Special Agent-in-Charge (SAC) will immediately make verbal contact with the AIGI/DAIGIs upon an incident occurring within their FD.
- b.** The SAC will designate a FD representative (ASAC/RAC or Senior SA) to serve as a single point-of-contact (POC) for disseminating information to OI Headquarters (HQ).
- c.** The SAC or their designee (ASAC/RAC) will be responsible for conducting an initial assessment of the incident in order to establish an initial plan of action. The FD SAC or their designee will provide OI HQ with the action plan as soon as practical, once the initial assessment is completed. The action plan notification will include a determination of the OI FD resources needed to address the incident, as well as an accountability/status report of all FD personnel within the specific geographical area impacted by the event.
- d.** The SAC or their designee (ASAC/RAC or FD POC) in consultation with the AIGI/DAIGIs will determine whether implementation of the FD Continuity of Operations Plan (COOP), or a devolution of the FD or OI office to a designated site (i.e. emergency relocation site), is required. Before a final decision is made, the AIGI/DAIGIs will discuss COOP implementation with the IG/DIG for concurrence.
- e.** The SAC or their designee (ASAC/RAC or FD POC) will also conduct ongoing assessments throughout the course of OI's involvement in this incident, and coordinate with OI HQ to make appropriate adjustments.
- f.** The FD POC will provide timely updates and communication with OI HQ as to all pertinent activity and/or information. Status updates will be provided as urgent/significant activity/information is collected, and at a minimum twice daily (morning and afternoon report), or as designated by the AIGI/DAIGIs.
- g.** The SAC or their designee (ASAC/RAC) will coordinate and assign OI FD agents to any appropriate law enforcement task force (e.g. Joint-Terrorism Task Force), joint investigative team, or command center (OI Special Agent GS-13 or above).
- h.** Provide for 24-hour OI FD agent coverage at all assigned posts-of-duty, as warranted.

2. Headquarters Responsibilities:

- a.** The AIGI and/or DAIGIs will coordinate with the IG or his designee to initiate activation of the OIG's Incident Coordination Center (ICC). Activation of the ICC will occur within one-hour of OI HQ notification of an incident. Upon activation, procedures are to be followed in accordance with existing ICC protocols.
- b.** The AIGI and/or DAIGIs or their designee(s) will participate in any formal and/or informal briefings with the IG, DIG, Commissioner of SSA, SSA executives, and other external stakeholders, as needed.
- c.** The AIGI and/or DAIGIs will assess any need for activation of the OIG's Investigative Response Team (IRT) or any other OI FD to support incident efforts.
- d.** The DAIGIs or their designee will coordinate for any onsite OI representation at the Federal Bureau of Investigation's (FBI) Strategic Information and Operations Center (SIOC), if required.

- e. The AIGI or their designee will coordinate with the OIG Immediate Office if there is a need to activate the OI HQ COOP.
- f. Provide for 24-hour HQ coverage within the Crisis Center or other posts-of-duty, as warranted.
- g. Criminal Investigations Division (CID):
 - (1) The SAC of CID or their designee (ATSAC) will coordinate with the DAIGIs on all field activity related to the incident.
 - (2) Assign appropriate CID staff (at a minimum, one desk officer) to the ICC and prepare all ICC SITREPs/Operational Status Reports with input from all OIG ICC representatives.
 - (3) Serve as the OIG representative at the SSA Sensitive Compartmented Information Facility (SCIF) on the SSA main campus, to include the handling of classified emails and communications.
 - (4) Coordinate with PAD in the activation and notification of IRT members, if applicable.
 - (5) Provide ongoing OI HQ field support for all OI FDs not directly involved in the incident.
- h. Intelligence and Analysis Division (IAD):
 - (1) The SAC or Director of IAD or their designee (ATSAC) will coordinate with the DAIGIs on all analytical support.
 - (2) Assign appropriate IAD staff to the ICC.
 - (3) Provide HQ analytical support to the OI FD(s).
 - (4) Conduct proactive computer queries and matches of SSA records to develop or support investigative leads.
 - (5) Provide any computer forensic support to develop or support investigative leads.
- i. Policy and Administration Division (PAD):
 - (1) The SAC of PAD or their designee (ATSAC) will coordinate with OI executives in the set-up and activation of the OIG's ICC. Set-up will include ensuring all necessary coordination with other OIG HQ components for the infrastructure of all ICC resources, to include personnel and equipment.
 - (2) Provide HQ logistical support to the ICC and OI FD(s) involved in the incident.
 - (3) Coordinate with CID in the activation and notification of IRT members, if applicable.
 - (4) In the event of a COOP (HQ level or FD), provide assigned OI COOP functions, to include required notifications (Everbridge System).
 - (5) Provide ongoing OI HQ logistical support for all OI FDs not directly involved in the incident, including keeping them apprised of the current situation.

- D. “Level II” National Incident:** Definition- major law enforcement incidents, acts of domestic terrorism or natural/man-made disasters/emergencies having national implications, national media interests, or deemed high-interest by government officials to include members of Congress, the IG/DIG or SSA; *in which the OIG’s involvement would be peripheral in scope or deemed to be a conduit in disseminating (SSA or OIG-related) information to the appropriate Federal/State/local law enforcement agency(ies), the OIG, SSA or other external stakeholders.*

1. Field Division Responsibilities:

- a. The FD SAC or their designee (ASAC/RAC or Senior SA) will serve as a single point-of-contact (POC) for disseminating information to OI Headquarters (HQ). The designated POC will be based upon the event, and determined by the SAC with AIGI/DAIGI approval.
- b. The SAC or their designee (ASAC/RAC) will be responsible for conducting an initial assessment of the incident in order to establish an initial plan of action, to include a determination of OI FD resources needed to address the incident.
- c. The SAC or their designee (ASAC/RAC) will also conduct ongoing assessments throughout the course of OI’s involvement in this incident, and coordinate (through the FD POC) with OI HQ to make appropriate adjustments.
- d. The FD POC will provide timely updates and communication with OI HQ as to all pertinent activity and/or information. Status updates will be provided as urgent/significant activity/information is collected, and at a minimum, on a daily basis, or as designated by the AIGI/DAIGIs.

2. Headquarters Responsibilities:

a. CID:

- (1) Serve as the OI HQ liaison with the OI FD(s) involved in the incident.
- (2) Designate the appropriate CID desk officer to serve as the primary OI HQ POC.
- (3) Coordinate investigative activity (through the FD POC) with the OI FD(s) involved in the incident.
- (4) Provide timely updates and communication for dissemination to the OIG Immediate Office, other OIG components, and OI FDs. Status updates will be provided as urgent/significant activity/information is collected, and at a minimum, on a daily basis, or as designated by the AIGI/DAIGIs.
- (5) The CID SAC or their designee will coordinate with the AIGI and/or DAIGIs to determine whether to institute the use of OI’s Situational Reports (SITREPs) for information reporting. (See SAH Section 003.220.C for SITREP distribution protocol.)

b. IAD:

- (1) Provide any required HQ analytical support to the OI FD(s).
- (2) Conduct any required proactive computer queries and matches of SSA records to develop or support investigative leads.

(3) Provide any required computer forensic support to develop or support investigative leads.

c. PAD:

(1) Provide any required HQ logistical support to the OI FD(s).

(2) Provide personnel to support OI HQ in its endeavor to develop or support investigative leads.

Chapter 4 — **EXHIBITS**

- [4-1 — Federal Employee Advice of Rights \(Form OI-15\)](#)
- [4-2 — Federal Employee Advice of Rights – Spanish \(Form OI-15 S\)](#)
- [4-3 — Kalkines \(Form OI-14\)](#)
- [4-4 — Kalkines- Spanish \(Form OI-14 S\)](#)
- [4-5 — Report of Alleged SSA Employee Misconduct](#)
- [4-6 A — Model Referral Letter to SSA – SSA action needed](#)
- [4-6 B — Model Referral Letter to SSA – No SSA action needed](#)
- [4-7 — Request for Information or Assistance \(Form OI-56\)](#)
- [4-8 — Union Representative Advisory to SSA Employee \(Form OI-80\)](#)
- [4-9 — Non-Criminal Background Investigation: Education](#)
- [4-10 — Non-Criminal Background Investigation: Employment](#)
- [4-11 — Non-Criminal Background Investigation: Neighborhood](#)
- [4-12 — Confidential Informant Data \(OI-27\)](#)
- [4-13 — Agreement to Provide Information \(OI-27A\)](#)
- [4-14 — Confidential Informant Contact Record \(OI-27B\)](#)
- [4-15 — Confidential Source Registration Card \(OI-27C\)](#)
- [4-16 — Threat/Assault – Interview Worksheet](#)
- [4-17 — Relevant Statutes](#)
- [4-18 — AIMS, GAM 12.06](#)
- [4-19 — Consent to Search Computers/Electronic Media](#)
- [4-20 — Request for Audit and Financial Forensic Assistance – Memorandum \(Form OI-93\)](#)
- [4-21 — Category 1 – Threat Notification Report \(Form OI-95\)](#)

Exhibit 4-1



WARNINGS AND ASSURANCES TO EMPLOYEE REQUESTED TO PROVIDE INFORMATION ON A VOLUNTARY BASIS (GARRITY)

You are being asked to provide information as part of an investigation being conducted by the Office of the Inspector General into alleged misconduct and/or improper performance of official duties. This investigation is being conducted pursuant to the Inspector General Act of 1978, as amended.

This is a voluntary interview. Accordingly, you do not have to answer questions. No disciplinary action will be taken against you solely for refusing to answer questions.

Any statement you furnish may be used as evidence in any future criminal proceeding or agency disciplinary proceeding, or both.

ACKNOWLEDGEMENT

I understand the warnings and assurances stated above and I am willing to make a statement and answer questions. No promises or threats have been made to me and no pressure or coercion of any kind has been used against me.

Office of the Inspector General
Special Agent/Interviewer

Employee's Signature

Witness: _____

Date: _____

Time: _____

Location: _____

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.



**ADVERTENCIAS Y GARANTIAS AL EMPLEADO(A) AL CUAL SE LE SOLICITA
PROVEER INFORMACION DE MANERA VOLUNTARIA (GARRITY)**

A usted se le esta solicitando proveer información como parte de una investigación llevada a cabo por la Oficina del Inspector General acerca de una alegada conducta impropia y/o un desempeño indebido de las funciones oficiales. Esta investigación se está llevando a cabo conforme al Acta del Inspector General de 1978, según enmendada.

Esta es una entrevista voluntaria. Por lo tanto, usted no tiene que responder a las preguntas. No se tomaran medidas disciplinarias en su contra por solo negarse a responder a las preguntas.

Cualquier declaración que usted proporcione puede ser utilizada como evidencia en el futuro en caso que haya un procedimiento criminal o procedimiento administrativo, o ambos.

RENUNCIA

Yo entiendo las advertencias y garantías indicadas arriba y Estoy dispuesto(a) a hacer una declaración y a contestar preguntas. No se me ha hecho ninguna promesa ni amenaza y no se ha utilizado presión ni coerción alguna en mi contra.

Oficina del Inspector General
Investigador/Entrevistador

Firma del Empleado(a)

Testigo: _____

Fecha: _____

Hora: _____

Lugar: _____

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

Exhibit 4-3



**WARNINGS AND ASSURANCES TO EMPLOYEE REQUIRED TO
PROVIDE INFORMATION (KALKINES)**

You are being asked to provide information as part of an investigation being conducted by the Office of the Inspector General into alleged misconduct and/or improper performance of your official duties.

The purpose of this interview is to obtain information which will assist in the determination of whether administrative action is warranted. This investigation is being conducted pursuant to the Inspector General Act of 1978, as amended.

- You are going to be asked a number of specific questions concerning the performance of your official duties.
- You have a duty to cooperate with and participate in this interview, and agency disciplinary action, including dismissal, may be undertaken if you refuse to cooperate and participate.
- You have a duty to reply to these questions, and agency disciplinary action, including dismissal, may be undertaken if you refuse to answer, or fail to reply fully and truthfully.
- The answers you furnish and any information or evidence resulting therefrom may be used in the course of civil or administrative proceedings.
- Neither your answers nor any information or evidence which is gained by reason of such statements can be used against you in any criminal proceedings, except that if you knowingly and willfully provide false statements or information in your answers, you may be criminally prosecuted for that action.

ACKNOWLEDGMENT

I have read the above warnings or they have been read to me, and I have been afforded the opportunity to ask questions about them. I understand my rights and I am willing to make a statement and answer questions.

Office of the Inspector General
Special Agent/Interviewer

Employee's Signature

Witness: _____

Date: _____

Time: _____

Location: _____

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.



ADVERTENCIAS Y GARANTIAS AL EMPLEADO(A) AL QUE SE LE REQUIERE PROVEER INFORMACIÓN (KALKINES)

A usted se le requiere proveer información como parte de una investigación llevada a cabo por la Oficina del Inspector General acerca de alegada conducta impropia y/o el desempeño indebido de sus funciones oficiales.

El propósito de esta entrevista es obtener información la cual asistirá en la determinación de si una acción administrativa es justificada. Esta investigación se está llevando a cabo conforme al Acta del Inspector General de 1978, según enmendada.

- A usted se le va a hacer preguntas específicas referentes al desempeño de sus deberes oficiales.
- Usted tiene el deber de cooperar y participar en esta entrevista, y la agencia puede tomar acciones disciplinarias, incluyendo el despido, si usted se rehúsa a cooperar y participar.
- Usted tiene el deber de responder a estas preguntas, y la agencia puede tomar acciones disciplinarias, incluyendo el despido, si usted se rehúsa a contestar o falla en responder completa y verazmente.
- Las respuestas que usted ofrezca y cualquier información o evidencia que resulte de sus respuestas pueden ser utilizadas en el curso de procedimientos civiles o administrativos.
- Ni sus respuestas ni cualquier información o evidencia obtenida por razón de sus declaraciones pueden ser utilizadas en su contra en un procedimiento criminal, con la excepción de que, usted pudiera ser procesado criminalmente si usted con conocimiento y voluntariamente proporciona información o declaraciones falsas en sus respuestas.

RECONOCIMIENTO

Yo he leído las advertencias antedichas o se me han leído a mí, y se me ha dado la oportunidad de hacer preguntas acerca de las mismas. Yo entiendo mis derechos y estoy dispuesto(a) a hacer una declaración y a contestar preguntas.

Oficina del Inspector General
Investigador/Entrevistador

Firma del Empleado(a)

Testigo: _____
Hora: _____

Fecha: _____
Lugar: _____

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.



Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: June 30, 2015

Refer To: OI Allegation Number

To: Name of Eastern or Western Deputy Assistant Inspector General for Investigations
Deputy Assistant Inspector General for Investigations – Eastern or Western Field Operations
Office of Investigations

Thru: Name of Special Agent-in-Charge
Title (Special Agent-in-Charge)
Headquarters Division (i.e. Criminal Investigations Division)

From: Name of Special Agent-in-Charge
Title (Special Agent-in-Charge)
Field Division (i.e. Chicago Field Division)

Subject: Report of Alleged SSA Employee Misconduct

Pursuant to Section 004.055 of the Special Agent Handbook, I am providing the following information relating to possible misconduct by a Social Security Administration (SSA) employee.

- A. Employee's name, position title, grade, and organizational component:
- B. Date complaint received or incident discovered:
- C. OI allegation or case number and case agent's name:
- D. Description of suspected violation:
- E. Action the FD has taken or plans to take (include dates):
- F. Other Significant Factors:
 - 1. Media Interest:
 - 2. Relation to Other Investigations:
 - 3. Monetary Impact:
- G. Indicate if FD has any objections to OIG HQ notifying the employee's senior management of the existence of the complaint:

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.



Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: _____ Refer To: <OI Case Number>

To: Name of Regional Commissioner
SSA Region (do not indicate Region #)

From: Name of Special Agent-in-Charge and e signature /s/
_____ Field Division

Subject: Results of Employee Investigation (Assistant District Manager John Doe, Laredo District Office)

CONFIDENTIAL

The Social Security Administration, Office of the Inspector General, Office of Investigations (SSA/OIG/OI)_____ Field Division (OI/_FD) has completed its investigation into the allegations concerning SSA employee _____, (*Employee's title*), (*Office location*).

(Provide a detailed summary of all investigative activity conducted, to include all pertinent information, such as results of interviews, reviewing of records, etc.)

Information has been modified where necessary to protect (1) the identity of individuals who have been granted specifically-requested confidentiality; (2) the identity of individuals who may be subjected to physical harm if their identity is disclosed; (3) grand jury information; and/or (4) novel investigative techniques, the disclosure of which could jeopardize future investigations.

You will note that Privacy Act warnings as to the disclosure of this information appear throughout the document. While this information is a sensitive document, please do not feel constrained with regard to its use for legitimate Agency purposes, including any administrative action that might result from the employee's conduct. The OIG takes no position with respect to the imposition of SSA administrative actions against the employee.

(If investigation uncovers wrongdoing, include the following language:)

In light of the sensitive nature of this information, I suggest that you maintain a list of those SSA officials to whom this information is disseminated. Please provide the OIG with a written response to this memorandum within 60 days of receipt. Your response should detail the final disposition or proposed administrative action to be taken against the employee.

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.**

(If investigation does not uncover wrongdoing, include the following language:)

In light of the sensitive nature of this information, I suggest that you maintain a list of those SSA officials to whom this information is disseminated. The findings of this investigation did not substantiate the allegation(s) against _____; therefore, no written response regarding administrative action against the employee is necessary.

(Statement as to whether or not supporting documents, e.g. Federal Employee Advise of Rights-Garrity, Kalkines Warnings, Miranda Warnings, Written Statement, etc. are attached). Please note, copies of Reports of Investigation pertaining to this investigation may be provided upon request.

If you have any questions regarding this memorandum or any of the supporting documentation, please contact me at _____.

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.



Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: _____ Refer To: <OI Case Number>

To: Name of Deputy Commissioner
Name of Office (i.e. Office of Operations)

From: Name of Assistant Inspector General for Investigations
Assistant Inspector General for Investigations

Subject: Results of Employee Investigation (Assistant District Manager John Doe, Dallas Region)

CONFIDENTIAL

The SSA/OIG, Office of Investigations, _____ Field Division (OI/_FD) has completed its investigation of _____, (*Employee's title*), (*Office location*).

(Detailed summary of information contained in SAC Summary Memorandum)

Along with this memorandum, you will find a copy of the memorandum from our __FD Special Agent-in-Charge, (*SAC's Name*), to (*Name of Region*) Regional Commissioner (*RC's name*), regarding the conclusion of the (*Employee's title and last name*) investigation.

You will note that Privacy Act warnings as to the disclosure of this information appear throughout the document. While the information is a sensitive document, please do not feel constrained with regard to its use for legitimate Agency purposes, including any administrative action that might result from the employee's conduct. The OIG takes no position with respect to the imposition of SSA administrative actions against the employee.

In light of the sensitive nature of this information, I suggest that you maintain a list of those SSA officials to whom this information is disseminated.

If you should have any additional questions regarding this investigation, please contact me at _____.

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

REQUEST FOR INFORMATION OR ASSISTANCE

TO:

The Inspector General of the Social Security Administration, pursuant to the authority contained in 5 U.S.C., Appendix 3, requests that you furnish information and/or assistance as follows:

Pertinent sections of the United States Code are being provided to you as part of this request. The request is made for official and/or law enforcement purposes, and in connection with an official investigation being conducted by our office.

CAUTION. Representatives of the Office of the Inspector General are required to display their official identification to you when personally requesting information or assistance.

Requested by: _____
(Name and Title)

Region _____ **-SSA OIG/OI**

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

UNION REPRESENTATIVE ADVISORY TO SSA EMPLOYEE

During an interview undertaken as part of an official Social Security Administration (SSA), Office of the Inspector General (OIG) investigation, the individual serving as your union representative has been advised that he or she has engaged in activity that has interfered with the OIG's legitimate interest in achieving the objective of the investigation. In order to avoid an adversarial confrontation and to achieve the objectives of the investigation, you are being offered the choice of (1) continuing this interview without the participation of your union representative or (2) discontinuing the interview, thereby foregoing the opportunity to be interviewed in connection with this matter.

ACKNOWLEDGEMENT

Having read this advisory, I choose to:

_____ Continue with the OIG interview without the participation of a union representative.

_____ Forego the opportunity to be interviewed in connection with this investigation.

Name of Employee

Employee Signature

Name of Special Agent

Signature of Special Agent

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.



Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

EDUCATION INVESTIGATION

NAME OF APPLICANT:

CASE NUMBER:

DATE OF INVESTIGATION:

INVESTIGATED BY:

FIELD DIVISION/OFFICE:

A. Applicant's attendance at the below listed school has been verified:

Name of school:

Location of school (City, State):

Dates of attendance:

Major, degree, and date of degree:

Additional information:

Class standing:

Grade average:

Honors and awards:

B. Have there been any academic/honor council, violations/suspensions, etc.?

C. The above scholastic information was furnished by (Name and Title):

D. Campus security check

No Derogatory Information

Derogatory Information (see comments)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Information Not Available

E. The above scholastic information was furnished by;

Name:

Title:

F. Campus security check

No Derogatory Information

Derogatory Information (see comments)

Information Not Available

Confidentiality Requested By:

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

EMPLOYMENT INVESTIGATION

NAME OF APPLICANT:

CASE NUMBER:

DATE OF INVESTIGATION:

INVESTIGATED BY:

FIELD DIVISION/OFFICE:

Applicant's employment reflects the following as indicated on their eQIP:

Name and address of employer:

Dates of employment:

Position and salary:

Reason for leaving:

Eligible for re-employment: Yes / No (Explain why)

Employment Inquiries

Interview the supervisor indicated on the applicant's eQIP and at least one co-worker regarding the applicant. If you are unable to conduct any of the interviews (i.e. supervisor listed no longer employed with company, or current supervisor cannot confirm knowledge of applicant, etc.), please provide an explanation. The following should be considered when conducting these interviews:

- Length of time supervisor and coworker has known the applicant and frequency of their contact with the applicant (i.e. daily, weekly, monthly).
- Describe the applicant's character, reputation, integrity, loyalty, and/or additional information deemed appropriate?
- Whether they recommended the applicant for a position of trust or sensitive position with the United States Government.

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

Exhibit 4-10

SOCIAL SECURITY
Office of the Inspector General

Supervisor's Name:
Address:
Comments/Findings:
Confidentially Requested:

Coworker's Name:
Address:
Comments/Findings:
Confidentially Requested:

Unemployment Inquiries - Individual listed as "Verifier"

Interview the "Verifier" indicated by the applicant on their eQIP that can confirm any period(s) of unemployment exceeding 60 days. If you are unable to conduct the interview, please provide an explanation. The following should be considered when conducting this telephonic or in-person interview:

- Length of time having known the applicant and frequency of contact with the applicant (i.e. daily, weekly, monthly).
- Verify/confirm periods of unemployment and activities conducted while unemployed.
- Verify applicant's means of support during their unemployment.
- Description of applicant's character, reputation, integrity, and loyalty and/or additional information deemed appropriate?
- Whether they recommended the applicant for a position of trust or sensitive position with the United States Government.

Name:
Address:
Comments/Findings:
Confidentiality Requested:

<p>This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is <u>FOR OFFICIAL USE ONLY</u>, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.</p>

SOCIAL SECURITY
Office of the Inspector General

NEIGHBORHOOD INVESTIGATION

NAME OF APPLICANT:

CASE NUMBER:

DATE OF INVESTIGATION:

INVESTIGATED BY:

FIELD DIVISION/OFFICE:

APPLICANT'S ADDRESS:

APPLICANT'S PERIOD OF RESIDENCE:

Neighborhood inquiries have been made as shown below. (Use one sheet for each period of residence).

Rental Property Inquiry

If the applicant is a renter, interview the property owner or rental office. Provide the contact name and address below. At the minimum, you should inquire about the following:

- Applicant's rental history (consistent rental payment, late rental payments, and/or delinquencies).
- Whether there have been any complaints about the applicant.

Name:

Address:

Comments/Findings:

Police Department Inquiry

Contact the local police department for any dispatch reports or calls for service at the applicant's residence (i.e. domestic disturbances and/or complaints) Provide the police department/precinct's name, name of contact, address, and any findings below.

Name of Police Department/Precinct:

Contact Name:

Address:

Comments/Findings:

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

Neighborhood Inquiries

Interview at least two neighbors regarding the applicant. If you are unable to conduct the interviews, please provide an explanation. The following should be considered when conducting these interviews:

- Length of time neighbor has known the applicant and frequency of neighbor's contact with the applicant (i.e. daily, weekly, monthly).
- Describe the applicant's character, reputation, integrity, and loyalty and/or additional information deemed appropriate?
- Whether they recommended the applicant for a position of trust or sensitive position with the United States Government.

Name:
Address:
Comments/Findings:
Confidentiality Requested:

Name:
Address:
Comments/Findings:
Confidentiality Requested:

Individual listed under "Person Who Knew You" indicated by the applicant

Interview the individual provided under the "Person Who Knew You" as indicated on the applicant's eQIP that can verify the applicant resides/resided at the address provided. If you are unable to conduct the interview, please provide an explanation. The following should be considered when conducting this telephonic or in-person interview:

- Length of time having known the applicant and frequency of contact with the applicant (i.e. daily, weekly, monthly).
- Description of applicant's character, reputation, integrity, and loyalty and/or additional information deemed appropriate?
- Whether they recommended the applicant for a position of trust or sensitive position with the United States Government.

Name:
Address:
Comments/Findings:
Confidentiality Requested:

<p>This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is <u>FOR OFFICIAL USE ONLY</u>, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.</p>

CONFIDENTIAL INFORMANT DATA						RESTRICTED INFORMATION		
Date:		Informant No.:				PHOTO		
Name (First, Middle, Last):								
Nicknames/Aliases/AKA:								
DOB or Age	Sex:	Height:	Weight:	Hair:	Eyes:			
Race:		FBI No.:						
Local or State Criminal I.D. Numbers:								
Other I.D. Numbers (Soc. Sec., Drivers License, etc.):								
Address:			Telephone:					
Occupation:								
Employer and Address:								
Other Agencies Using Informant:								
Crime Categories in Which Informant is Knowledgeable and/or Can be of Assistance:					Geographic Area Where CI can be of Assistance:			
Contact Arrangement:								
Alternate Contact Arrangement:								
Contact Special Agent and Domicile:			Alternate Contact Special Agent and Domicile:					
Other Agents Aware of Informant's Activity:			Others Who Know Informant's Activity and/or Whereabouts:					
Completed by:			Division:					
Deactivation Record: Reason for Deactivation: Services no longer required <input type="checkbox"/> or for cause <input type="checkbox"/> Explain: Deactivation approved by: _____ Date Deactivated: _____ <div style="text-align: center;">SAC/ASAC/RAC</div>								

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

AGREEMENT TO PROVIDE INFORMATION

The undersigned understands and agrees to the following conditions in furnishing information and assistance to the Social Security Administration (SSA) Office of the Inspector General (OIG).

1. I must not engage in any unlawful acts, except as specifically authorized by the Office of the United States Attorney and the SSA OIG. I am subject to prosecution for any unauthorized unlawful acts.
2. I must provide truthful information at all times.
3. I must abide by the instructions of the SSA OIG and must not take or seek to take any independent action on behalf of the United States Government.
4. I understand that I am not an employee of the United States Government, and may not represent myself as such.
5. I must not engage in witness tampering, witness intimidation, entrapment, or the fabrication, alteration, or destruction of evidence. If I do this, I may be prosecuted under the applicable Federal or State law.
6. I understand that I am liable for any taxes that may be owned on moneys the United States Government pays me.
7. I understand that the SSA OIG cannot guarantee any rewards, payments, or other compensation to me.
8. Any representation to be made on my behalf with regard to any pending judicial matters shall be at the discretion of the SSA OIG, and no guarantee can be given as to the outcome of any prosecutive action or sentencing.
9. I understand that no promises or representations can be made to me regarding any possible alien status or right to enter or remain in the United States.
10. I request the SSA OIG to protect my identity from disclosure to the maximum extent permitted by law but understand that it cannot be guaranteed. I understand that the information and assistance I provide to the SSA OIG may be used in a judicial proceeding and that I may be called upon to testify.
11. I may not enter into any contracts or incur any obligations on behalf on the United States Government, except as specifically instructed and approved by the SSA OIG.
12. I will not carry a firearm or other deadly weapon in connection with my cooperation with the SSA OIG.

SOCIAL SECURITY
Office of the Inspector General

13. I cannot reveal this special relationship with SSA OIG to anyone without specific authorization from an authorized representative of SSA OIG.
14. I will be fully accountable for any funds provided me by SSA OIG during the performance of this assistance, and will promptly return all unused funds.
15. I must carefully protect the confidential information revealed to me, and I fully realize that a large measure of responsibility for maintaining the confidentiality of this relationship is mine.
16. I will immediately report any threats or any adverse circumstances that occur as a result of my special relationship with SSA OIG.

This agreement entered into by _____ Date _____
(Signature)

(Print Name)

Witnessed by _____
(Signature)

(Print Name)

SOCIAL SECURITY
Office of the Inspector General

CONFIDENTIAL SOURCE REGISTRATION CARD

SSA OIG Case Number:

Primary SA Name/Domicile/Phone Number:

Name of Confidential Source:

Telephone Number:

Method of Contact:

Record of Payments

<u>Date</u>	<u>Case Number</u>	<u>Amount</u>	<u>Reason for Payment</u>
1.			
2.			
3.			
4.			
5.			

ADMINISTRATIVE FILE#

SOCIAL SECURITY
Office of the Inspector General

THREAT/ASSAULT
INTERVIEW WORKSHEET

(b) (7) (E)



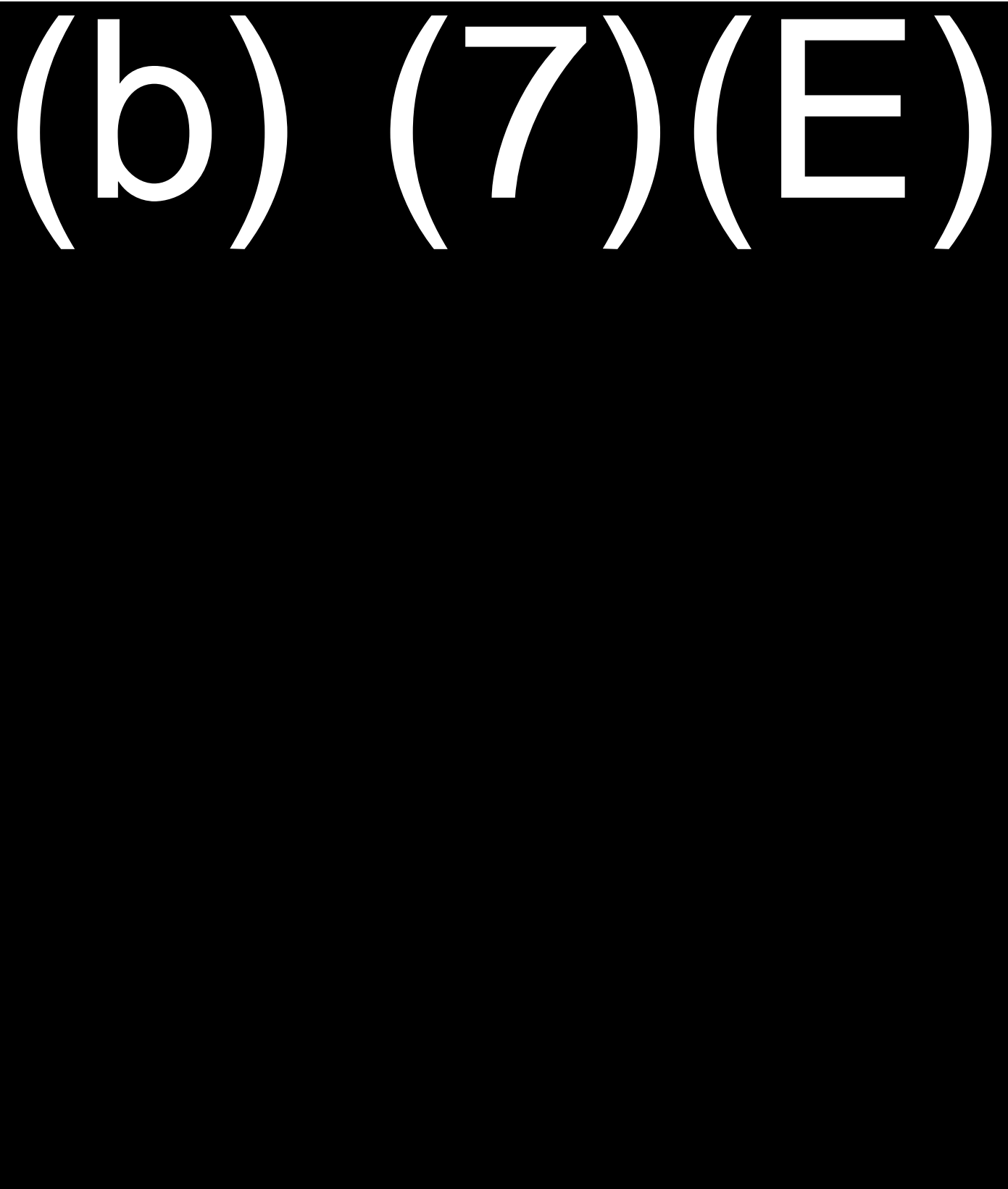
SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)



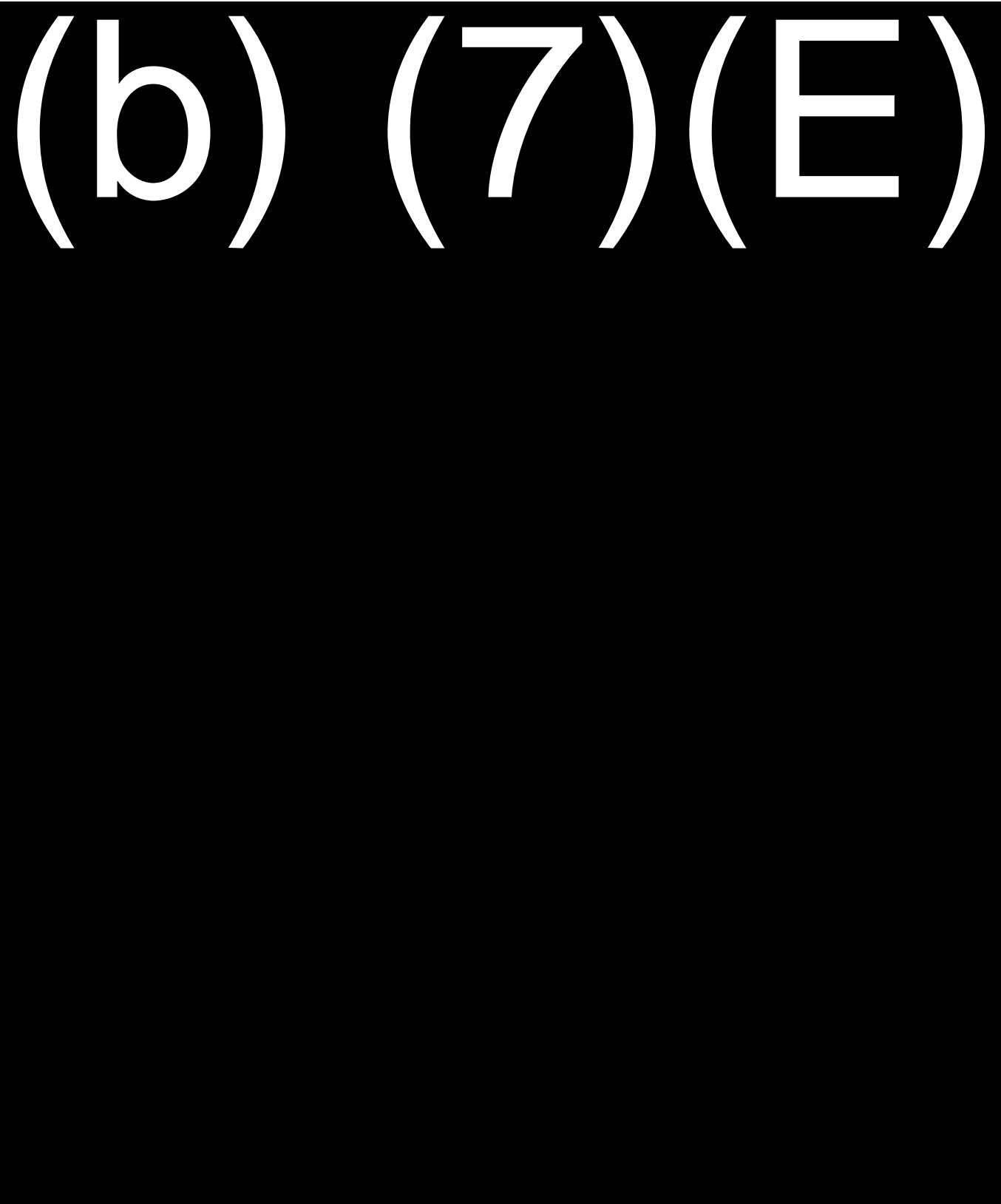
SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)



SOCIAL SECURITY
Office of the Inspector General

SOCIAL/ENVIRONMENTAL FUNCTIONING



SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)



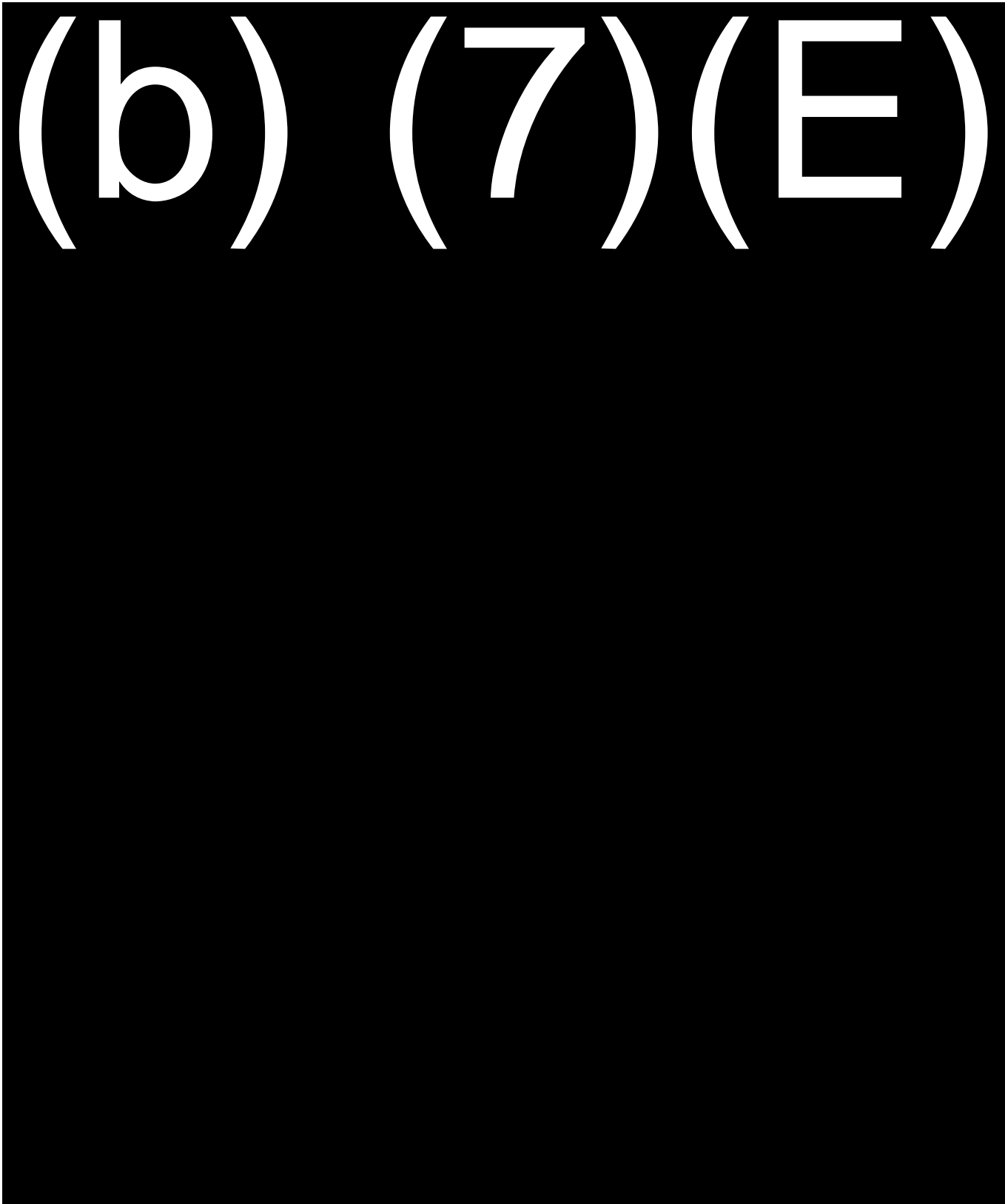
SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)



SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)



SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)



SOCIAL SECURITY
Office of the Inspector General

CURRENT EVALUATION



Special Agent: _____

Office: _____

Date: _____

Witness: _____

Date: _____

Approved by: _____

SAC/ASAC

Date: _____

SOCIAL SECURITY
Office of the Inspector General

Relevant Statutes

41 CFR 102-74.390 – loitering, exhibiting disorderly conduct or exhibiting other conduct on property which (a) creates loud or unusual noise or a nuisance; (b) unreasonably obstructs the usual use of entrances, foyers, lobbies, corridors, offices, elevators, stairways, or parking lots; (c) otherwise impedes or disrupts the performance of official duties by government employees; or (d) prevents the general public from obtaining the administrative services provided by the property in a timely manner.

28 CFR 64.1 – This regulation designates categories of federal officers and employees in addition to those already designated by the statute, who will be within the protective coverage of 18 U.S.C. 1114, which prohibits the killing or attempted killing of such designated officers and employees. The categories of federal officers and employees covered by section 1114 are also protected, while they are engaged in or on account of the performance of their official duties, from a conspiracy to kill, 18 U.S.C. 1117; kidnapping, 18 U.S.C. 1201(a)(5); forcible assault, intimidation, or interference, 18 U.S.C. 111; and threat of assault, kidnap or murder with intent to impede, intimidate, or retaliate against such officer or employee, 18 U.S.C. 115(a)(1)(B). In addition, the immediate family members of such officers and employees are protected against assault, kidnap, murder, attempt to kidnap or murder, and threat to assault, kidnap, or murder with intent to impede, intimidate, or retaliate against such officer or employee, 18 U.S.C. 115(a)(1)(A). The protective coverage has been extended to those federal officers and employees whose jobs involve inspection, investigative or law enforcement responsibilities, or whose work involves a substantial degree of physical danger from the public that may not be adequately addressed by available state or local law enforcement resources.

28 CFR 64.2 - Designated officers and employees.

The following categories of federal officers and employees are designated for coverage under section 1114 of title 18 of the U.S. Code: (a) Judges and special trial judges of the U.S. Tax Court; (b) Commissioners and employees of the U.S. Parole Commission; (c) Attorneys of the Department of Justice; (d) Resettlement specialists and conciliators of the Community Relations Service of the Department of Justice; (e) Officers and employees of the Bureau of Prisons; (f) Criminal investigators employed by a U.S. Attorney's Office; and employees of a U.S. Attorney's Office assigned to perform debt collection functions; (g) U.S. Trustees and Assistant U.S. Trustees; bankruptcy analysts and other officers and employees of the U.S. Trustee System who have contact with creditors and debtors, perform audit functions, or perform other investigative or enforcement functions in administering the bankruptcy laws; (h) Attorneys and employees assigned to perform or to assist in performing investigative, inspection or audit functions of the Office of Inspector General of an "establishment" or a "designated Federal entity" as those terms are defined by section 11 and 8E, respectively, of the Inspector General Act of 1978, as amended, 5 U.S.C. app. 3 section 11 and 8E, and of the Offices of the Inspector General of the U.S. Government Printing Office, the Merit Systems Protection Board, and the Selective Service System. (i) Employees of the Department of Agriculture at the State, district or county level assigned to perform loan making, loan servicing or loan collecting function; (j) Officers and employees of the

SOCIAL SECURITY
Office of the Inspector General

Bureau of Alcohol, Tobacco and Firearms assigned to perform or to assist in performing investigative, inspection or law enforcement functions; (k) Federal air marshals of the Federal Aviation Administration; (l) Employees of the Bureau of Census employed in field work conducting censuses and surveys; (m) Employees and members of the U.S. military services and employees of the Department of Defense who: (1) Are military police officers, (2) Have been assigned to guard and protect property of the United States, or persons, under the administration and control of a U.S. military service or the Department of Defense, or (3) Have otherwise been assigned to perform investigative, correction or other law enforcement functions; (n) The Director, Deputy Director for Supply Reduction, Deputy Director for Demand Reduction, Associate Director for State and Local Affairs, and Chief of Staff of the Office of National Drug Control Policy; (o) Officers and employees of the Department of Energy authorized to carry firearms in the performance of investigative, inspection, protective or law enforcement functions; (p) Officers and employees of the U.S. Environmental Protection Agency assigned to perform or to assist in performing investigative, inspection or law enforcement functions; (q) Biologists and technicians of the U.S. Fish and Wildlife Service who are participating in sea lamprey control operations; (r) Uniformed and nonuniformed special police of the General Services Administration; and officers and employees of the General Services Administration assigned to inspect property in the process of its acquisition by or on behalf of the U.S. Government; (s) Special Agents of the Security Office of the U.S. Information Agency; (t) Employees of the regional, subregional and resident offices of the National Labor Relations Board assigned to perform investigative and hearing functions or to supervise the performance of such functions; and auditors and Security Specialists of the Division of Administration of the National Labor Relations Board; (u) Officers and employees of the U.S. Nuclear Regulatory Commission: (1) Assigned to perform or to assist in performing investigative, inspection or law enforcement functions or (2) Engaged in activities related to the review of license applications and license amendments; (v) Investigators employed by the U.S. Office of Personnel Management; (w) Attorneys, accountants, investigators and other employees of the U.S. Securities and Exchange Commission assigned to perform or to assist in performing investigative, inspection or other law enforcement functions; (x) **Employees of the Social Security Administration assigned to Administration field offices, hearing offices and field assessment offices;** (y) Officers and employees of the Tennessee Valley Authority authorized by the Tennessee Valley Authority Board of Directors to carry firearms in the performance of investigative, inspection, protective or law enforcement functions; (z) Officers and employees of the Federal Aviation Administration, the Federal Highway Administration, the National Highway Traffic Safety Administration, the Research and Special Programs Administration and the Saint Lawrence Seaway Development Corporation of the U.S. Department of Transportation who are assigned to perform or assist in performing investigative, inspection or law enforcement functions; (aa) **Federal administrative law judges appointed pursuant to 5 U.S.C. 3105;** and (bb) Employees of the Office of Workers' Compensation Programs of the Department of Labor who adjudicate and administer claims under the Federal Employees' Compensation Act, the Longshore and Harbor Workers' Compensation Act and its extension, or the Black Lung Benefits Act.

18 USC 1114 – Protection of officers and employees of the United States.

Whoever kills or attempts to kill any officer or employee of the United States or of any agency in any branch of the United States Government (including any member of the uniformed services) while such

SOCIAL SECURITY
Office of the Inspector General

officer or employee is engaged in or on account of the performance of official duties, or any person assisting such an officer or employee in the performance of such duties or on account of that assistance, shall be punished--(1) in the case of murder, as provided under section 1111; (2) in the case of manslaughter, as provided under section 1112; or (3) in the case of attempted murder or manslaughter, as provided in section 1113.

18 USC 115 – Influencing, impeding, or retaliating against a federal official by threatening or injuring a family member.

(a)(1) Whoever--(A) assaults, kidnaps, or murders, or attempts or conspires to kidnap or murder, or threatens to assault, kidnap or murder a member of the immediate family of a United States official, a United States judge, a Federal law enforcement officer, or an official whose killing would be a crime under section 1114 of this title; or (B) threatens to assault, kidnap, or murder, a United States official, a United States judge, a Federal law enforcement officer, or an official whose killing would be a crime under such section, with intent to impede, intimidate, or interfere with such official, judge, or law enforcement officer while engaged in the performance of official duties, or with intent to retaliate against such official, judge, or law enforcement officer on account of the performance of official duties, shall be punished as provided in subsection (b). (2) Whoever assaults, kidnaps, or murders, or attempts or conspires to kidnap or murder, or threatens to assault, kidnap, or murder, any person who formerly served as a person designated in paragraph (1), or a member of the immediate family of any person who formerly served as a person designated in paragraph (1), with intent to retaliate against such person on account of the performance of official duties during the term of service of such person, shall be punished as provided in subsection (b). (b)(1) An assault in violation of this section shall be punished as provided in section 111 of this title. (2) A kidnapping, attempted kidnapping, or conspiracy to kidnap in violation of this section shall be punished as provided in section 1201 of this title for the kidnapping, attempted kidnapping, or conspiracy to kidnap of a person described in section 1201(a)(5) of this title. (3) A murder, attempted murder, or conspiracy to murder in violation of this section shall be punished as provided in sections 1111, 1113, and 1117 of this title.(4) A threat made in violation of this section shall be punished by a fine under this title or imprisonment for a term of not more than five years, or both, except that imprisonment for a threatened assault shall not exceed three years. (c) As used in this section, the term--(1) "Federal law enforcement officer" means any officer, agent, or employee of the United States authorized by law or by a Government agency to engage in or supervise the prevention, detection, investigation, or prosecution of any violation of Federal criminal law; (2) "immediate family member" of an individual means--(A) his spouse, parent, brother or sister, child or person to whom he stands in loco parentis; or (B) any other person living in his household and related to him by blood or marriage; (3) "United States judge" means any judicial officer of the United States, and includes a justice of the Supreme Court and a United States magistrate judge; and (4) "United States official" means the President, President-elect, Vice President, Vice President-elect, a Member of Congress, a member-elect of Congress, a member of the executive branch who is the head of a department listed in 5 U.S.C. 101, or the Director of the Central Intelligence Agency.

(d) This section shall not interfere with the investigative authority of the United States Secret Service, as provided under sections 3056, 871, and 879 of this title.

SOCIAL SECURITY
Office of the Inspector General

18 USC 876 – Mailing threatening communications.

Whoever knowingly deposits in any post office or authorized depository for mail matter, to be sent or delivered by the Postal Service or knowingly causes to be delivered by the Postal Service according to the direction thereon, any communication, with or without a name or designating mark subscribed thereto, addressed to any other person, and containing any demand or request for ransom or reward for the release of any kidnapped person, shall be fined under this title or imprisoned not more than twenty years, or both.

Whoever, with intent to extort from any person any money or other thing of value, so deposits, or causes to be delivered, as aforesaid, any communication containing any threat to kidnap any person or any threat to injure the person of the addressee or of another, shall be fined under this title or imprisoned not more than twenty years, or both.

Whoever knowingly so deposits or causes to be delivered as aforesaid, any communication with or without a name or designating mark subscribed thereto, addressed to any other person and containing any threat to kidnap any person **or any threat to injure the person of the addressee or of another**, shall be fined under this title or imprisoned not more than five years, or both.

Whoever, with intent to extort from any person any money or other thing of value, knowingly so deposits or causes to be delivered, as aforesaid, any communication, with or without a name or designating mark subscribed thereto, addressed to any other person and containing any threat to injure the property or reputation of the addressee or of another, or the reputation of a deceased person, or any threat to accuse the addressee or any other person of a crime, shall be fined under this title or imprisoned not more than two years, or both.

18 USC 111 – Assaulting, resisting, or impeding certain officers or employees.

(a) In General.--Whoever--

(1) forcibly assaults, resists, opposes, impedes, intimidates, or interferes with any person designated in section 1114 of this title while engaged in or on account of the performance of official duties; or

(2) forcibly assaults or intimidates any person who formerly served as a person designated in section 1114 on account of the performance of official duties during such person's term of service, shall, where the acts in violation of this section constitute only simple assault, be fined under this title or imprisoned not more than one year, or both, and in all other cases, be fined under this title or imprisoned not more than three years, or both.

(b) Enhanced Penalty.--Whoever, in the commission of any acts described in subsection (a), uses a deadly or dangerous weapon (including a weapon intended to cause death or danger but that fails to do so

SOCIAL SECURITY
Office of the Inspector General

by reason of a defective component) or inflicts bodily injury, shall be fined under this title or imprisoned not more than ten years, or both.

42 USC 1320a-8b (Section 1129B of the Social Security Act)

Section 206 of the *Social Security Protection Act of 2004* – Public Law 108-203, signed by President Bush on March 2, 2004.

ATTEMPTS TO INTERFERE WITH ADMINISTRATION OF SOCIAL SECURITY ACT

Whoever corruptly or by force or threats of force (including any threatening letter or communication) attempts to intimidate or impede any officer, employee, or contractor of the Social Security Administration (including any State employee of a disability determination service or any other individual designated by the Commissioner of Social Security) acting in an official capacity to carry out a duty under this Act, or in any other way corruptly or by force or threats of force (including any threatening letter or communication) obstructs or impedes, or attempts to obstruct or impede, the due administration of this Act, shall be fined not more than \$5,000, imprisoned not more than 3 years, or both, except that if the offense is committed only by threats of force, the person shall be fined not more than \$3,000, imprisoned not more than 1 year, or both. In this subsection, the term 'threats of force' means threats of harm to the officer or employee of the United States or to a contractor of the Social Security Administration, or to a member of the family of such an officer or employee or contractor.

18 USC 1001 – Statements or entries generally.

(a) Except as otherwise provided in this section, whoever, in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States, knowingly and willfully

- (1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact;
- (2) makes any materially false, fictitious, or fraudulent statement or representation; or
- (3) makes or uses any false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry; shall be fined under this title or imprisoned not more than 5 years, or both.

(b) Subsection (a) does not apply to a party to a judicial proceeding, or that party's counsel, for statements, representations, writings or documents submitted by such party or counsel to a judge or magistrate in that proceeding.

(c) With respect to any matter within the jurisdiction of the legislative branch, subsection (a) shall apply only to -

- (1) administrative matters, including a claim for payment, a matter related to the procurement of property or services, personnel or employment practices, or support services, or a document required by law, rule, or regulation to be submitted to the Congress or any office or officer within the legislative branch; or

SOCIAL SECURITY
Office of the Inspector General

(2) any investigation or review, conducted pursuant to the authority of any committee, subcommittee, commission or office of the Congress, consistent with applicable rules of the House or Senate

18 USC 2261A – Interstate domestic violence.

(a) Offenses. -

(1) Travel or conduct of offender. -

A person who travels in interstate or foreign commerce or enters or leaves Indian country with the intent to kill, injure, harass, or intimidate a spouse or intimate partner, and who, in the course of or as a result of such travel, commits or attempts to commit a crime of violence against that spouse or intimate partner, shall be punished as provided in subsection (b).

(2) Causing travel of victim. -

A person who causes a spouse or intimate partner to travel in interstate or foreign commerce or to enter or leave Indian country by force, coercion, duress, or fraud, and who, in the course of, as a result of, or to facilitate such conduct or travel, commits or attempts to commit a crime of violence against that spouse or intimate partner, shall be punished as provided in subsection (b).

(b) Penalties. -

A person who violates this section or section 2261A shall be fined under this title, imprisoned

-

(1) for life or any term of years, if death of the victim results;

(2) for not more than 20 years if permanent disfigurement or life threatening bodily injury to the victim results;

(3) for not more than 10 years, if serious bodily injury to the victim results or if the offender uses a dangerous weapon during the offense;

(4) as provided for the applicable conduct under chapter 109A if the offense would constitute an offense under chapter 109A (without regard to whether the offense was committed in the special maritime and territorial jurisdiction of the United States or in a Federal prison); and

(5) for not more than 5 years, in any other case, or both fined and imprisoned.

SOCIAL SECURITY
Office of the Inspector General

MANUAL: General Administration
CHAPTER: 12 Field Administration
INSTRUCTION NO.: 06

SUBJECT: Physical Security Action Plan
Audience: General (g)
Level: SSA
Date: 05/06/2003

INQUIRIES: Questions regarding the content of this issuance should be directed to the Office of the Deputy Commissioner for Finance, Assessment and Management (ODCFAM), Office of Facilities Management (OFM), Office of Protective Security Services (OPSS), 410-965-4544.

12.06.00 Table of Contents

- 12.06.01 Purpose
- 12.06.02 Applicability
- 12.06.03 Policy
- 12.06.04 Responsibility
- 12.06.05 Planning
- 12.06.06 Essential Elements of the Physical Security Action Plan
- 12.06.07 Physical Security Action Plan Considerations
- 12.06.08 Physical Security Action Plan Review and Approval
- 12.06.09 Physical Security Action Plan Implementation
- 12.06.10 Authority

12.06.01 Purpose

A. The Physical Security Action Plan (PSAP) is a written plan prepared for each Social Security Administration field office and each Office of Disability Adjudication and Review hearing office or facility to ensure facilities, records, equipment, employees and the public are adequately protected. The PSAP contains security policies and procedures and is used to direct the actions of employees in emergencies, and to ensure prompt coordinated steps for obtaining assistance. To complement this AIMS Instruction, the templates for two new handbooks have been developed and will be distributed under separate cover.

1. The Employee Handbook contains all information pertinent to the local office and should be shared and understood by employees. Managers must provide employees a copy of the Employee Handbook, discuss it with them at least annually and encourage them to familiarize themselves with the content.

SOCIAL SECURITY
Office of the Inspector General

The Employee Handbook contains the following:

? Administrative safeguards for sensitive items such as the office safe, sensitive documents, and highly pilferable for office supplies.

? Physical safeguards such as facility access, key control, duress alarm systems, contract guard duties, Occupant Emergency Organization, security alerts and incident reporting, disaster contingency plans, response to biological/chemical threats, etc.

2. The Managers Handbook is for managers responsible for developing and/or implementing their office required physical and administrative safeguards. It is restricted to management only and is used as a basis for required physical and administrative safeguards for the office. The Managers Handbook contains logs, lists of CPR and first-aid trained employees and other sensitive information that may not be shared with employees. The PSAP requirements and handbooks must be reviewed semi-annually, at a minimum, and revised whenever changes to the office or national security alert levels occur.

The Managers Handbook contains the following:

? Physical safeguards such as annual PSAP updates, contract guard duties, SSA physical security policies/procedures, incident reporting and response, Occupant Emergency Organization Program requirements, response to chemical/biological threats, etc.

? Administrative safeguards such as annual security awareness training and discussions with employees, security briefings for new employees, management procedures for safeguarding sensitive items such as the office safe, keys, sensitive documents, etc.

B. Managers must revise their current PSAP to incorporate the new requirements. Managers may, of course, attach documents to the PSAP as additional chapters dealing with other types of security (such as programmatic security), but the information in them should not be commingled with the PSAP.

12.06.02 Applicability

The requirement for a PSAP applies to the following:

- A. All Regional Offices
- B. All Program Service Centers
- C. Data Operations Center
- D. All Teleservice Centers
- E. All Field Offices (including contact and resident stations)
- F. Office of Disability Adjudication and Review (ODAR), Falls Church, Virginia

SOCIAL SECURITY
Office of the Inspector General

- G. All ODAR Hearings Offices (including remote hearings sites)
- H. Regional Office of Quality Assurance and Performance Assessment Satellite Offices

12.06.03 Policy

Designated management officials (for large facilities) or office managers must develop a written PSAP. The Plan must incorporate security measures that apply specifically to the facility and immediate surrounding area. Frequent reviews of the PSAP are necessary to gauge the effectiveness of procedures, to incorporate adjustments to the office's physical configuration and to ensure employees receive adequate training in security and safety practices. Revisions or modifications are to be made to the PSAP whenever there are significant personnel, environmental or procedural changes. At a minimum, the PSAP must be assessed and revised as appropriate, annually. PSAPs must be developed immediately for all new offices and revised upon relocation or whenever events occur that affect existing provisions.

12.06.04 Responsibility

- A. The Office of Facilities Management (OFM), Office of Protective Security Services (OPSS) is responsible for developing PSAP policies and procedures, providing guidance on PSAP development and issuing annual reminders to managers to update PSAPs.
- B. Designated officials at large sites and facility managers at all other sites have the primary responsibility for formulating the PSAP and determining subordinate duties within the Plan.
- C. Management must review the contents of the Plan at least annually with all employees and volunteers, and with new employees as they report for duty as part of their orientation.

12.06.05 Planning

A. Safety and security measures that focus on prevention are the best way to provide maximum employee safety. The first step in planning is to contact local law enforcement officials (police, sheriff, etc.) to advise them of the nature of SSA operations, the clientele with whom SSA does business, and any existing or potential problems. Law enforcement is to be asked about the degree of protection they can provide. This source is to be pursued diligently and contact regularly maintained. If local law enforcement cannot furnish the level of protection needed, they are to be asked to recommend other options.

B. Assistance may also be requested from the following:

- 1. Federal Protective Service (FPS)

SOCIAL SECURITY
Office of the Inspector General

2. Area/State Director
3. Physical Security Coordinator
4. Regional Chief Administrative Law Judge
5. Regional Office, Quality Assurance and Performance Assessment
6. Regional Office, Office of the Inspector General
7. OPSS/OFM

12.06.06 Essential Elements of the Physical Security Action Plan

A. The PSAP identifies:

1. Who is responsible for activities identified in the PSAP, including alternates where necessary;
2. The physical location of all personnel in the office;
3. Emergency communications (duress alarm, verbal code, intercom, fire alarm, etc.);
4. Evacuation procedures and routes from the facility;
5. Employee emergency training;
6. Procedures for reporting incidents with applicable follow-up actions;
7. Emergency telephone numbers;
8. What response will be provided by local emergency services;
9. The anticipated time frame for emergency response; and
10. Any additional emergency resources that may be available during times of increased threats.

B. Information in the PSAP is to include:

1. Office location;
2. Crime level indication, including a history of the types of criminal or disruptive incidents in the neighborhood;
3. Emergency planning information received from law enforcement;
4. A copy of the office floor-plan with emergency routes highlighted; and
5. Availability of building security personnel.

12.06.07 Physical Security Action Plan Considerations

A. Potentially Dangerous Situations

1. "Buddy Systems" are to be instituted to help employees maintain awareness of a potentially hazardous situation. Management, employees and guards must take appropriate precautions when alerted to disruptive or threatening situations involving claimants. If necessary, additional security should be arranged with local law enforcement or FPS.
2. Methods of service other than face-to-face interviewing should be considered when a client has been identified as disruptive (Refer to memorandum dated February 4, 1998 entitled

SOCIAL SECURITY
Office of the Inspector General

"Agency Policy and Guidelines on Handling Repetitive Threatening Behavior or Uncontrollable Clients," available by contacting OFM/OPSS (410) 965-4544).

B. Arrests of Non-Social Security Administration (SSA) Employees in SSA/ODAR Occupied Facilities

1. If law enforcement is to be contacted, management should make the contact. Bargaining unit employees will not be required to contact law enforcement officials or to participate in the detention of any individual.
2. In situations where SSA management becomes aware that law enforcement personnel will attempt to arrest an individual while on SSA-occupied premises, SSA management must take appropriate actions to minimize harm to employees consistent with Article 9 of the SSA/AFGE National Contract. NOTE: This should only occur when all other avenues are unfeasible.
3. Managers should consider appropriate arrangements such as alterations to the normal office work processes to minimize exposure of employees to potential dangers inherent in arrest situations. Where an arrest cannot be avoided, in accordance with the National Agreement, Article 9, Section 10, management must discuss the situation with the designated AFGE representative(s) as soon as possible.
4. The office guard(s) must coordinate with SSA managers if they are informed of plans to arrest someone in the office. Such coordination will provide the manager an opportunity to take precautionary measures.
5. Management must work closely with the local FPS and/or police to obtain a general status of an arrest (e.g., whether an individual was taken into custody, jailed or released) to properly assess the need for additional or continuing precautionary measures.

C. Tier 1 Security Enhancements

Management is to ensure that, in SSA offices dealing with the public, the following mandatory Tier 1 security enhancements are in place:

1. Duress (panic) alarms at all workstations used for interviewing the public. This also includes the reception counter and the private interview room in field offices.
2. Peepholes in exterior and interior doors as needed (and installed at wheel chair height if appropriate). ODAR hearing rooms are to have peepholes which look into the rooms.
3. Locks and panic bars on exterior and interior doors as needed. Locks are to meet the security locking requirements in the current SSA or ODAR Space Allocation Standards (SAS). Due to

SOCIAL SECURITY
Office of the Inspector General

technology developments, types of locks may be changed as long as the intent of the SAS is met. Locks are to be installed in accordance with local fire and building codes.

4. Intrusion detection system

5. Security lighting (interior and exterior) at building entrances and in parking areas controlled by SSA for employee and visitor safety.

D. Tier 2 Security Enhancements

Although not mandated, management is to consider the following Tier 2 enhancements:

1. Emergency lighting to provide sufficient lighting for employees to safely evacuate the office during power failures and other emergencies;

2. Emergency power back-up systems for critical security systems such as the intrusion detection system;

3. Closed circuit television (CCTV) systems (Refer to OFM memorandum dated April 25, 2000 entitled "Use of CCTVs Within SSA/ODAR Offices", available by contacting OPSS (410) 965-4544); and

4. Physical modifications to the space, such as the installation of barrier walls, Plexiglas reception windows, separate restrooms for the public, etc.

E. Contract Guards

Contract guards work with SSA managers but are usually hired by and under the direction of FPS. If the office has guard service, a copy of the guard's post orders is to be obtained from the guard or from FPS. Managers are to be familiar with the guard's responsibilities and authority as described in the post orders. Although FPS is responsible for providing guard service and developing post orders, managers should work with the region and FPS to make sure the guard's post orders are site specific, up-to-date and adequately reflect guard duties. (Refer to OPSS Security Information Bulletin dated February 1998 entitled "Guard Service-Roles and Responsibilities", available at OFM/OPSS website.) Managers may not ask the guard to perform duties other than those described in the post orders. Complaints about unsatisfactory guard service or problems are to be referred to the local GSA Physical Security Specialist before escalating issues to higher management authorities within GSA.

F. Walls/Partitions/Furniture

SOCIAL SECURITY
Office of the Inspector General

The office layout must promote maximum protection for employees and Privacy Act information. Walls, partitions and furniture arrangements can help control access to and departure from the office.

G. Periodic Review/Assessments

1. Management must periodically review/assess the level of protection needed by the office (including contact stations and remote hearing sites). The assessment must include an evaluation of physical and protective measures such as electronic systems (duress alarms, intrusion detection systems, closed circuit television systems) and guard service. If the office has guard service, managers must review how the guard is positioned to oversee office activity. Since most incidents occur in the reception area, the principal guard post should be located there. When planning new space configurations for the office, managers are to ensure that adequate space is allotted for a guard in the reception area.
2. Annual physical security assessments (e.g., OSCAR review, reviews by security contractors or OPSS staff) may be conducted. (Refer to AIMS, MRM, SSA.g:04.50, SSA Physical and Protective Security Program.) Part 6 of the OSCAR may be used to satisfy the annual assessment requirement.

H. Crime Prevention and Employee Security Awareness Program

Management must regularly conduct crime prevention awareness training for the staff. (Refer to memorandum dated July 23, 2000 entitled "Crime Prevention Training" available by contacting OFM/OPSS (410) 965-4544 and AIMS MRM SSA.g:04.54, Physical Security and Personal Protection.) Management may request local resources to provide additional security training. Sources include FPS, local law enforcement, mental health agencies, the fire department, the Employee Assistance Program (EAP), etc. Videos on security can be obtained from the Regional Offices and the Office of Training in headquarters.

The PSAP must reflect what training was given and when it was given.

I. Response to Biological/Chemical and Anthrax Threats

If an employee reports an incident of possible exposure to biological and chemical contaminants, management must take prompt and decisive action. (Refer to Memoranda dated October 17, 2001 "Management Responsibilities for Possible Exposure to Biological Threats via Mail", and November 16, 2001 "Supplemental Mail Handling Procedures".) Copies may be obtained by contacting OPSS at (410) 965-4544. Management should make the following sequence of calls to the authorities if they receive a threat, in the order shown:

SOCIAL SECURITY
Office of the Inspector General

1. Local Police/Fire Department/Emergency Medical Service (usually "911")
2. Local Federal Bureau of Investigation
3. Federal Protective Service
4. Local Office of Inspector General
5. SSA Regional Physical Security Officer (contacts OPSS)
6. Any other contacts in your PSAP (e.g., building landlord)
7. Line Management (e.g., higher levels, District Office (DO), Area Director)

12.06.08 Physical Security Action Plan Review and Approval

A. When a PSAP is created, updated or otherwise revised, management must provide a copy to the designated union representative for review. Management will address any concerns raised by the union representative prior to finalization. If management and the union representative cannot agree on how to resolve differences of opinion on the PSAP's content, the issue should be submitted to the Regional Commissioner, the Regional Office of Disability Adjudication and Review, or the Director, Regional Office of Quality Assurance and Performance Assessment, who will determine what action to take after discussing the submission with appropriate regional union officials.

NOTE: If management and the union disagree about a portion of the PSAP, move only that portion forward for resolution. The remainder of the PSAP will be implemented.

B. Once the PSAP is approved locally, it will be sent to the next higher management official for review and approval. PSAPs for new and relocated facilities must be developed and approved within 45 days of occupancy. Existing PSAPs are to be reviewed at least annually by the facility designee or manager and revised whenever necessary due to major changes in office space, circumstances surrounding an incident, and/or significant personnel changes.

C. PSAPs will also be reviewed during site visits by authorized personnel from headquarters and regional offices or during security reviews performed by outside contractors.

12.06.09 Physical Security Action Plan Implementation

A. PSAPs must be implemented immediately after approval. A copy or copies of the approved PSAP must be forwarded through appropriate management channels to the regional physical security coordinator for review. The PSAP is a living document and must be changed as circumstances change.

B. Management will annually review non-sensitive sections of the PSAP with employees during security awareness meetings, with new employees entering on duty, and with all employees when significant changes in the Plan occur or when otherwise determined necessary. Copies of the PSAP must be designated "For Official Use Only", and employees must be warned

Exhibit 4-18

SOCIAL SECURITY
Office of the Inspector General

the PSAP is not to be removed from the office. Posting of applicable portions of the PSAP on a bulletin board must be restricted to employee (not public) areas.

12.06.10 Authority

The Code of Federal Regulations, Title 41, Chapter 101-20.103.

SOCIAL SECURITY
Office of the Inspector General

CONSENT TO SEARCH COMPUTERS/ELECTRONIC MEDIA

I _____,

hereby grant _____, a Special Agent with the Social Security Administration Office of the Inspector General and any other employees designated to assist, consent to conduct a complete search of a computer, described as

and any and all electronic storage devices including, but not limited to, hardware and all equipment which can collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, optical, or similar computer impulses or data, cellular phones, pagers, PDAs (personal digital assistant), and related communication devices and all removable computer media associated with the above referenced computer, and to make a bit stream copy of any and all electronic storage devices and removable computer media associated with the above described computer for purposes of further analysis. The Social Security Administration Office of the Inspector General has complete, unreviewable discretion to determine what communication devices and removable computer media are considered *related* devices and media for the purpose of this search (as referenced above). This search is to include all areas of the hard drive and removable media, whether password protected or encrypted, including but not limited to hidden partitions, directories, files, erased files, deleted files, files marked for deletion, slack space, and unallocated space on the drive and other electronic storage devices and media.

I further authorize the above Agent of the Social Security Administration Office of the Inspector General to remove, take with them, retain custody over and search any property in conjunction with the copying and/or searching of the above information sought by the Agent, including, but not limited to, the above referenced computer and all electronic storage devices and removable media associated with the above described computer and peripherals. I also affirmatively represent that I am the lawful owner of the above described computer and/or associated property, electronic storage devices, removable media or peripherals or are otherwise authorized to provide this consent, and that I have lawful possession and control over it for purposes of this consent to search.

I have been advised by Special Agent _____, and fully understand that I have the right to refuse my consent. I also understand that I have the right to be present at the time of any searches which are conducted and I expressly waive any rights I may have to be physically present during any searches which are conducted pursuant to this consent to search. I give this consent to search freely and voluntarily without fear, threat, coercion or promises of any kind.

Date: _____

Time: _____

Person providing consent: _____

Witness: _____

Witness: _____



MEMORANDUM

Date: ENTER INFO

Refer To:

To: Click here for SAC's Name

From: (b) (6)
Assistant Inspector General for Investigations

Thru: Special Agent-in-Charge, Intelligence and Analysis Division

Subject: Request for Audit and Financial Forensic Assistance

Case Number: (Input OI Case Number)

Brief description of case:

1. Reason for Assistance Needed:
2. Description and Location of Evidence: (to include number of beneficiaries, claims, or entities involved)
3. Offense(s):
4. Duration and Dates for Assistance:
5. Name of OI Supervisor Overseeing the Investigation
6. Additional Items for Consideration and/or Unusual Expenses:

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

CATEGORY 1- THREAT NOTIFICATION REPORT

INCIDENT: Choose an item.

DATE/TIME: Click here to enter a date.

LOCATION: Click here to enter text.

SUBJECT(S):

Name: Click here to enter text.

DOB: Click here to enter text.

SSN: Click here to enter text.

Address: Click here to enter text.

Vehicle Info.: Click here to enter text.

Name: Click here to enter text.

DOB: Click here to enter text.

SSN: Click here to enter text.

Address: Click here to enter text.

Vehicle Info.: Click here to enter text.

Photo: 

INCIDENT SUMMARY: Click here to enter text.

RESPONSE: Give name of agency or person.

- FPS:** Click here to enter text.
- State/County/Local Police:** Click here to enter text.
- Onsite Guard:** Click here to enter text.
- Other Federal Law Enforcement:** Click here to enter text.
- Fire Department:** Click here to enter text.
- Paramedics:** Click here to enter text.

Exhibit 4-21



Functioning drop down menus available on attachment.



TNR (rev
9-7-11).docx

INVESTIGATIVE PROJECT MANAGEMENT

005.000 Investigative Projects

- A.** Investigative projects are local, regional, and/or national operations that address fraud and abuse in Social Security Administration (SSA) programs and operations. These projects are coordinated and managed by the Intelligence and Analysis Division (IAD).
- B.** Investigative projects may originate in the Office of Investigations (OI) Field Divisions or may be developed by CID.
- C.** All investigative projects are reviewed by the Office of Counsel to the Inspector General (OCIG) and require final approval of the Assistant Inspector General for Investigations (AIGI) or his/her authorized designee.

005.010 Investigative Projects Originating in OI Headquarters

- A.** IAD staff members liaise with members from various components at SSA Headquarters (HQ), as well as the Office of the Inspector General (OIG), Office of Audit. IAD seeks ideas on how to identify programs that are more susceptible to fraud, waste and/or abuse, and how changes in laws and regulations can be used to reduce fraud within SSA programs.
- B.** Investigative projects, or ideas for new projects, are assigned to IAD staff member to develop. The Director or Special Agent-in-Charge (SAC) of IAD presents proposals to the appropriate DAIGI. Projects deemed to have merit are presented to the Inspector General (IG).
- C.** Once IAD has established viable investigative leads, IAD will work with the OI Field Divisions to refer those leads for potential investigation.

005.020 Requests from Field Divisions to Establish Investigative Projects

- A.** There may be times, such as during the investigation of a particular case, when a field division (FD) discovers a program vulnerability that is susceptible to fraud, or a new data source that when matched with SSA's records could identify potential fraud. FDs are encouraged to develop these into Investigative Projects.
 - 1.** To request establishment of an Investigative Project, a memorandum must be submitted to the IAD Director or SAC for review and approval with a copy to the appropriate CID Regional Desk Officer. The memorandum should follow the format set forth in [Exhibit 5-0](#), Request

for Approval to Establish Investigative Project. Once reviewed and approved, the request is provided to OCIG for review and approval and submitted to the AIGI for final approval.

2. The memorandum must be approved prior to the sharing of any data between OIG and an external source. This includes making a request for such data in anticipation of an approved request.
3. The memorandum must address the potential to conduct a sampling in order to test the feasibility of the proposed Investigative Project. Following are three options for meeting this requirement:
 - a. Provide data regarding prior successful Investigative Projects of a similar nature;
 - b. Provide prior case examples that are directly related to the Investigative Project being proposed; or,
 - c. State that a sample dataset will be obtained and used to conduct a review for investigative leads. The results of that review will be extrapolated to the full universe of data to determine the feasibility of proceeding with the investigative project.

B. The Investigative Project Proposal will be processed as follows:

1. Proposal will be sent to IAD Director or SAC. The Director or SAC will route the proposal to the IAD Special Projects Administrator/Coordinator (SPA/C) for review.
2. The SPA/C will forward the proposal to IAD Director/SAC for further review and approval for routing to the Office of Counsel to the Inspector General (OCIG).
3. The SPA/C will request a legal opinion on the proposal from OCIG. OCIG has up to 30 days to review the proposal. OCIG will send their response to the SPA/C.
4. The SPA/C will forward the proposal through the IAD Director/SAC to the DAIGI for approval.
5. The DAIGI will forward the project to AIGI for final approval.
6. IAD will inform the SAC of the AIGI's decision regarding performing the Investigative Project.
7. The AIGI will inform the IG of the approved Investigative Project.

C. IAD will provide a copy of approved Investigative Projects to the appropriate FD SAC. IAD will assign a staff member to assist the FD with implementation and to track project results. IAD assistance typically includes data runs/data matching and sharing "lessons learned" from similar projects already performed in other geographic areas. In addition, IAD will evaluate local projects to determine whether national implementation is advisable.

D. Request for NICMS Investigative Project Code

1. Upon request, an Investigations Analyst within IAD will provide the project manager with a National Investigative Case Management System (NICMS) project code. This code will be a two-character entry on the NICMS case-opening screen. Once a project identifier has been assigned, any case initiated under the scope of the project will list the project identifier on the case opening screen when initiating the investigation. A separate case number will **not** be opened solely to document the existence of the project. If the investigative project falls under one of the Office of Investigations (OI) National Operations (i.e., Fugitive Felons, Cooperative Disability Investigations Program (CDI), etc.), enter the National Operation code in the **National Oper** field and the investigative project identifier in the **Local Proj** field in NICMS.
2. In order for NICMS to capture all cases associated with the projects, use of the project identifiers is imperative. If an investigative project requires cases to be opened in multiple

FDs, the FD that opened the project must ensure that all participating FDs use the project identifier in all related cases.

005.030 Cooperative Disability Investigations Program

- A.** The Cooperative Disability Investigations (CDI) program is a joint effort by SSA, the SSA OIG, State Disability Determination Services (DDS), and State or local law enforcement agencies to efficiently pool resources for the purpose of preventing fraud in SSA’s Title II and Title XVI disability programs and related Federal and State programs. The CDI program’s primary objectives are to:
1. provide the State Disability Determination Services (DDS) with investigative evidence for use in making timely and accurate disability eligibility determinations;
 2. seek criminal and/or civil prosecution of applicants and beneficiaries, and refer cases for consideration of Civil Monetary Penalties and administrative sanctions when appropriate; and
 3. identify, investigate, and seek prosecution of third parties (i.e. doctors, lawyers, interpreters, and other third parties) who facilitate and promote disability fraud (see [Exhibit 5-1](#), Guide to Third Party Facilitator Investigations).
- B.** Oversight of operational and administrative activities of the CDI Units (CDIU) is shared by OI (the CDI Assistant to the Special Agent-in-Charge represents OIG/OI), the Office of Disability Determinations (ODD), and the Office of Public Service, and Operational Service (OPSOS).
- C.** The basic CDIU should consist of at least five individuals: an OIG Special Agent (SA), two State or local law enforcement officers, one DDS Examiner or Analyst, and a Management Support Specialist or equivalent from SSA.
- D.** The OIG SA assigned to the CDIU will serve as the Team Leader and will act to ensure that the CDI program accomplishes its mission. The OIG SA will be the CDIU’s final decision-making authority regarding the CDIU’s day-to-day operations, subject to OIG management oversight. The OIG SA’s specific responsibilities and duties will include:
1. conducting investigations of cases referred to the CDI Unit, in accordance with investigative procedures specified in the OIG Special Agent Handbook and/or procedures developed specifically for the CDI program. The OIG Special Agent, subject to OIG management oversight, will be responsible for resolving conflicts between CDI investigative procedures and those investigative procedures used by local law enforcement officials;
 2. pursuing criminal and/or civil prosecution under both Federal and State laws, Civil Monetary Penalty (CMP), and administrative remedies for those instances when the evidence supports the existence of material misrepresentations regarding benefit eligibility, fraud, and/or similar fault;
 3. reporting the results of investigations to the State DDS for its use in making timely and accurate disability eligibility determinations;

4. coordinating interaction with State and Federal law enforcement entities, including the U.S. Department of Justice;
5. ensuring that all participating staff receive sufficient training regarding SSA's disability programs and relevant sections of SSA's Program Operations Manual System (POMS) including, but not limited to, Disability Insurance Chapter 230, Section 25, Fraud or Similar Fault ([DI 23025.001](#) et seq.);
6. ensuring that referrals are handled appropriately and assigned a case number for tracking purposes;
7. ensuring that the CDIU is responsive to State DDS management needs and concerns subject to the limitations regarding the CDIU's prohibition against making recommendations or providing opinions regarding disability eligibility;
8. ensuring that the CDIU is in compliance with reporting requirements;
9. ensuring all statistical accomplishments in NICMS are recorded accurately; and
10. ensuring that costs do not exceed the funding made available by SSA.

E. The State and/or local law enforcement investigators' duties and responsibilities will include:

1. conducting disability fraud investigations of referred cases in accordance with those procedures developed specifically for the CDIU;
2. reporting the results of investigations to the State DDS for its use in making timely and accurate disability eligibility determinations; and
3. using their existing arrest authority granted under the laws of the State to further the CDI program's mission.

F. (b) (7)(E) [Redacted]

G. CDI activities are designed to reduce processing times and streamline case processing. (b) (7)(E) [Redacted]

H. CDI teams are designed to provide greater investigative support of the disability decision-making process to facilitate correct and timely decisions. DDS adjudicators refer suspicious claims for investigation using guidance found in the POMS. The SSA Fraud Hotline and SSA field offices may also refer disability fraud allegations to the appropriate CDIU. This enhances the ability to identify fraud at the onset to prevent payment on fraudulent initial applications, and ensures

timely investigation and termination when fraud is detected during continuing disability reviews or as a result of investigations based on SSA Fraud Hotline or Field Office (FO) referrals.

- I. In areas not covered by a CDIU, suspected fraud cases are referred to OI for investigation.
- J. The CDI program helps to ensure benefits are awarded only to the deserving individuals for whom they are intended. This enhances the integrity of SSA programs, promotes solvency of the SSA Trust Fund, preserves public confidence in SSA's stewardship, helps State-run public assistance programs reduce fraud, and reinforces the vigilance of DDS and SSA field staff.

005.040 Fugitive Felon Program

- A. The Personal Responsibility and Work Opportunity Reconciliation Act of 1996, Public Law 104-193 ([PL 104-193](#)), was enacted on August 22, 1996. Section 202(a) of this law amends Title XVI of the Social Security Act (Act) to make a person ineligible to receive Supplemental Security Income (SSI/T16) payments during any month in which the recipient:
 - 1. flees to avoid prosecution for a crime that is a felony (or in New Jersey, a 1st- through 4th-degree crime) under the laws of the place from which the person flees;
 - 2. flees to avoid custody or confinement after conviction for a crime that is a felony (or in New Jersey, a 1st- through 4th-degree crime) under the laws of the place from which the person flees; or
 - 3. violates a condition of probation or parole imposed under Federal or State law.
 - Under Section 202(b) of the law, the Social Security Administration (SSA) must furnish (upon written request) the current address, Social Security number (SSN), and photograph (if applicable) of an SSI recipient to any Federal, State, or local law enforcement officer, if such SSI recipient is a fugitive felon or a parole or probation violator.
- B. The Social Security Protection Act (SSPA) of 2004, Public Law ([PL](#)) [108-203](#), was enacted on March 2, 2004. Section 103 of this law, which went into effect April 1, 2005, amends the Act to make a person ineligible to serve as a Representative Payee (Rep Payee) during any month in which the Rep Payee:
 - 1. flees to avoid prosecution for a crime that is a felony (or in New Jersey, a 1st- through 4th-degree crime) under the laws of the place from which the person flees; or
 - 2. flees to avoid custody or confinement after conviction for a crime that is a felony (or in New Jersey, a 1st- through 4th-degree crime) under the laws of the place from which the person flees.
 - 3. Section 103 of the law, pertaining to Rep Payees only, does not allow for the disclosure of information, or loss of eligibility to serve as a fiduciary for fugitives wanted for violating probation and/or parole.

C. Section 203 of PL 108-203, which went into effect on January 1, 2005, amends the Act to make a person ineligible to receive Old Age, Survivors and Disability Insurance (OASDI/T2) benefits during any month in which the beneficiary:

1. flees to avoid prosecution for a crime that is a felony (or in New Jersey, a 1st- through 4th-degree crime) under the laws of the place from which the person flees;
2. flees to avoid custody or confinement after conviction for a crime that is a felony (or in New Jersey, a 1st- through 4th-degree crime) under the laws of the place from which the person flees; or
3. violates a condition of probation or parole imposed under Federal or State law.
4. for the purpose of payment of benefits only, Title II beneficiaries are not considered to be "fugitive felons" if their warrants exist for less than 30 days. This is per the statute, not any policy created by SSA or OIG. The statute (Social Security Act, Section 202(x)(1)(A)) reads, in part, as follows:

Limitation on Payments to Prisoners, Certain Other Inmates of Publicly Funded Institutions, Fugitives, Probationers, and Parolees

"(x)(1)(A) Notwithstanding any other provision of this title, no monthly benefits shall be paid under this section or under section 223 to any individual for any month ending with or during or beginning with or during a period of more than 30 days throughout all of which such individual—

iv) is fleeing to avoid prosecution, or custody or confinement after conviction, under the laws of the place from which the person flees, for a crime, or an attempt to commit a crime, which is a felony under the laws of the place from which the person flees, or, in jurisdictions that do not define crimes as felonies, is punishable by death or imprisonment for a term exceeding 1 year regardless of the actual sentence imposed, or

(v) is violating a condition of probation or parole imposed under Federal or State law."

5. Thus, it is not appropriate to claim savings for Title II fugitives whose warrants exist for less than 30 days, because SSA will not suspend benefits in these cases. SSA's Fugitive Felon SSA Control File (FFSCF) system will not allow notices to be sent, or benefits to be suspended in cases where a Title II beneficiary has an active felon or probation/parole violation warrant lasting less than 30 days.

D. Fugitive felons and parole or probation violators are identified through computer matching operations and individual referrals to OI. It is OI's responsibility to conduct data sharing efforts with warrant issuing agencies, resolve identity issues and confirm the status of warrants prior to referral to SSA. SSA maintains responsibility for administrative actions concerning benefit suspensions.

E. SSA has initiated contact with State and local law enforcement officials to identify fugitive felons and parole or probation violators through Computer Matching Agreements. OI has entered into Memoranda of Understanding (MOU) with the United States Marshals Service, the Federal

Bureau of Investigation (FBI), and the Criminal Justice Information Services (CJIS) which oversee the National Crime Information Center (NCIC) to obtain their wanted persons files.

1. (b) (7)(E) [Redacted]

2. (b) (7)(E) [Redacted]

3. (b) (7)(E) [Redacted]

4. (b) (7)(E) [Redacted]

5. (b) (7)(E) [Redacted]

6. In addition to adding Title II beneficiaries and Rep Payees to the Fugitive Felon Program, the SSPA also allows the Commissioner of Social Security to continue payments to fugitives if *Good Cause* is found. For a discussion of *Good Cause*, please see SSA POMS at [GN02613.025](#).

F. OIG field agents generally work two types of Fugitive Felon cases: field-generated fugitive cases and egregious felony cases. The following guidance provides instructions on how to process Field-Generated Fugitive Felon cases, how to process Egregious Felony Cases, and how to claim statistics related to Fugitive Felon Cases.

G. Field Generated Fugitive Felon Cases

1. Prior to opening a field-generated Fugitive Felon case, a NICMS Fugitive Search should be conducted to determine if the potential field-generated fugitive subject is currently a subject in an active electronic Fugitive Felon HQ case. (b) (7)(E) [Redacted]

(b) (7)(E)

2. (b) (7)(E)

3. (b) (7)(E)

4. In order to properly create Fugitive Felon Cases in NICMS with access to the Fugitive Screens, a case must be OPENED from an Allegation as a Fugitive Case in the following manner:

a. Agents should complete the Allegation Process in NICMS as follows:

1) (b) (7)(E)

2) (b) (7)(E)

3) Choose the appropriate Program Category(s) as follows:

- a. (b) (7)(E)
- b. (b) (7)(E)
- c. (b) (7)(E)
- d. (b) (7)(E)
- e. (b) (7)(E)

4) (b) (7)(E)

5) (b) (7)(E)

b. When the SAC/ASAC reviews the Allegation and decides to create a Fugitive Case in the Case Creation Screen in NICMS, the following should be completed:

1) (b) (7)(E)

2) (b) (7)(E)

3) (b) (7)(E)

4) (b) (7)(E)

(b) (7)(E)

- c. The onus for correctly creating a fugitive felon subject in NICMS is solely on the SAC/ASAC that converts the allegation into a case. (b) (7)(E)

1) Once the case has been opened in the manner described above, the case agent can locate the applicable Fugitive Screens in NICMS by:

a. (b) (7)(E)

b. (b) (7)(E).

c. (b) (7)(E)

d. (b) (7)(E).

e. (b) (7)(E)

f. (b) (7)(E)

g. (b) (7)(E)

2) (b) (7)(E)

3) (b) (7)(E)

4) (b) (7)(E)

- 5) (b) (7)(E) [Redacted]
- a. (b) (7)(E) [Redacted]
- b. (b) (7)(E) [Redacted]
- c. (b) (7)(E) [Redacted]
- d. (b) (7)(E) [Redacted]
- e. (b) (7)(E) [Redacted]
- f. (b) (7)(E) [Redacted]
- g. (b) (7)(E) [Redacted]
- h. (b) (7)(E) [Redacted]
- i. (b) (7)(E) [Redacted]
- j. (b) (7)(E) [Redacted]
- 6) (b) (7)(E) [Redacted]
- 7) (b) (7)(E) [Redacted]
- 8) (b) (7)(E) [Redacted]

H. Egregious Felon Case Procedures

1. In addition to field-generated Fugitive Felon cases, agents also have the option of working cases involving fugitives who are wanted for egregious offenses. These cases are identified by OCRM AMFED at OI HQ and forwarded to the SAC and Fugitive Coordinator of the appropriate Field Division each month. They are referred to as “Egregious Felony” cases. Any fugitive subject opened as a case in the field for which a current active headquarters-based fugitive case is already open should also be processed in the manner described below, whether or not the crime is considered egregious.

2. For the purposes of this program, egregious felonies include homicide, kidnapping, sexual assault, armed robbery, arson, and failing to register as a sex offender. These six categories are comprised of 78 different offense codes in NCIC.
3. (b) (7)(E) [REDACTED]
4. (b) (7)(E) [REDACTED]
 - a. (b) (7)(E) [REDACTED]
 - b. (b) (7)(E) [REDACTED]
 - c. (b) (7)(E) [REDACTED].
 - d. (b) (7)(E) [REDACTED]
5. Egregious Felony cases should only be opened in the field if OIG agents physically participate in the arrest of the fugitive, or belong to a task force that arrests the fugitive as a result of OIG data sharing efforts. Otherwise, a local case should not be opened because the HQ based case suffices for purposes of data sharing efforts with the warrant issuing agency, and for referring the fugitive to SSA for suspension activity.
6. (b) (7)(E) [REDACTED]
7. The case agent must not enter any information for the Egregious Felony case in the Fugitive Screens in NICMS.
8. If an Egregious Felony case is opened by an agent in the field, and the case agent or a member of a task force to which the agent belongs participates in the arrest of the fugitive felon, the case agent should email the apprehension information for the original fugitive case subject to (b) (7)(E) [REDACTED] (b) (7)(E) [REDACTED]
9. If a field agent opens an Egregious Felony case but fails to assist the LEA in the arrest and apprehension of the fugitive felon, no monetary statistics should be claimed for the Egregious Felony case. AMFED will process the original Fugitive Felon case normally, and will refer the subject to SSA after 60 days have expired. The Egregious Felony case should be closed.

- I. When claiming statistical accomplishments for fugitive felon cases, the statistics noted below should be entered in the NICMS case screens.

1. Claiming Arrests

ARRESTS should only be claimed for a fugitive felon in NICMS if an OIG agent physically arrests the individual. Physical arrests should be entered in the *Criminal Development* screen in NICMS. **“Physically participates in an arrest”** is defined as personally taking a subject into custody as part of a primary arrest team. As an example, three agents who effect the arrest of a subject within a residence, two going through the front door and one covering the back door, act as a primary arrest team. As a second example, two agents who arrest a subject during a worksite enforcement operation, one handcuffing the subject while the second agent covers, act as a primary arrest team.

On the other hand, performing perimeter security duties during a worksite enforcement operation does not constitute physical participation in an arrest unless the agent meets the parameters outlined in the first part of this definition. Finally, actions related to the issuance of a summons do not constitute physical participation in an arrest.

2. Claiming Fugitive Apprehensions

- a. APPREHENSIONS should be claimed in NICMS if an OIG agent physically arrests a fugitive felon (as defined above). Apprehensions should be entered in the *Criminal Disposition* screen in NICMS. A *Final Action Date* is required.
- b. Agents are required to enter data in NICMS to record fugitive apprehensions by selecting “FUGIT APPREHENSION” under “Type” on the *Subject Data* section of the *Criminal Disposition* screen.

3. Claiming Monetary Statistics

- a. Monetary statistics may be claimed if the case agent physically participates in the apprehension of a fugitive.
- b. If the case agent simply shares information with the warrant issuing agency, regardless of whether or not the fugitive is apprehended, monetary statistics should not be claimed. Agents must participate in the apprehension of a fugitive in order to justify the claiming of monetary statistics.
- c. Projected savings for both Field-Generated and Egregious Felony cases are calculated as follows: the difference of 24 months **minus** (-) the number of months that the warrant remains outstanding, **multiplied by** (x) the monthly benefit amount. No savings will be claimed when the warrant is in existence over 24 months.

4. If claiming monetary statistics is warranted as described above, the following statistics should be claimed in the NICMS screens of the field-generated FFP cases:

- a. Savings should be claimed on the *Monetary Info* screen.
- b. Fraud Loss (if an overpayment is posted to the SSID/MBR) should be claimed on the *Monetary Info* screen.

- c. Scheduled Recovery (if an overpayment is posted to the SSID/MBR) should be claimed on the *Monetary Info* screen.

5. Claiming Positive Actions

For fugitive felon cases, positive actions can occur in one of the following ways:


1. If an OI investigation results in action by SSA to suspend or reduce a beneficiary's monthly payments.
2. If an OI investigation results in an overpayment recovery.

Detailed information regarding the claiming of positive actions is found in the **NICMS User Manual** on the Employee Resource Center under *Policies and Procedures>Investigative Policies and Procedures Manual*. See Part 2: Case Management.

J. Non SSA Fugitive Arrests/Task Force Participation

1. In order to document OIG agent participation in the arrest of non SSA fugitive felons (non Title II beneficiaries, non Title XVI recipients, and non Rep Payees) during Fugitive Task Force operations, case(s) should be opened using the Program Suffix "Y" (Task Force Investigation). It is critical that cases for these types of subjects NOT be opened using Program Suffix "X" or National Operation Code of "AJ."
2. For non-SSA fugitive subjects, no statistics should be claimed. Arrests and Apprehensions should not be entered into NICMS, and Positive Actions should not be claimed. Descriptions of the events surrounding arrests of non-SSA fugitive subjects should be entered into NICMS to record actions taken by OIG agents in these instances.

K. Ramifications of the *Fowlkes* decision in the Second Judicial Circuit.

1. Fowlkes was a Title XVI fugitive felon residing in New York, and wanted in Virginia, whose benefits were suspended for fugitive felon status. Fowlkes contested the suspension of his SSI benefits for being a fugitive felon on the grounds that he was not "fleeing" as defined by statute, 42 U.S.C. § 1382(e)(4)(A), or as defined by SSA's regulation, [20 C.F.R. § 416.1339\(b\)\(1\)](#).
2. On 12/6/05, the 2nd Circuit Court of Appeals ruled in Fowlkes' favor. The Court found SSA's implementing regulation stricter than the statute in that it required "the issuance of a warrant or order issued by a court or other authorized tribunal on the basis of a finding that an individual fled or was fleeing from justice."
3. SSA's current operational policy only calls for the existence of an active warrant for a person to be considered a "fleeing" fugitive felon.
4. (b) (7)(E) 

5. (b) (7)(E) [Redacted]

6. (b) (7)(E) [Redacted]

005.050 SSN Misuse and Identity Theft

- A. IAD is responsible for coordinating with components within OIG and SSA on projects that evaluate and refine SSA’s enumeration process.
- B. IAD works with SSA on systems enhancements to identify Social Security number (SSN) misuse during the enumeration process and to stop the issuance of new SSNs and cards to individuals and addresses where fraud is involved.

1. SSA Long Term Fraud

(b) (7)(E) [Redacted]

2. Comprehensive Integrity Review Program (CIRP)

The CIRP module was implemented by SSA to identify addresses that receive new and replacement SSN cards based on fraudulent documents.

a. (b) (7)(E) [Redacted]

- b. If possible, the SSA FO resolves the questions surrounding the alert and the matter is closed.
- c. If circumstances indicate potential fraud, SSA FOs contact OIG and refer the matter to OIG via SSA Form E8551. All CIRP data is available on the OIG Global Server under the directory “CIRP,” in the Multiaddress.xls file.

3. Special Indicators

(b) (7)(E) [Redacted]

(b) (7)(E)

In March 2007, in compliance with the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), in addition to the seven special indicators that previously existed, SSA added two new indicators: (b) (7)(E)

(b) (7)(E)

a. (b) (7)(E)

b. (b) (7)(E)

c. (b) (7)(E)

(b) (7)(E)

Examples of when NOT to complete the “Fraudulent SSNs” Screen:

- (b) [Redacted]
- [Redacted]
- [Redacted]

d. (b) (7)(E) [Redacted]

4. Requesting Cross/Uncross of SSN

(b) (7)(E) [Redacted]

(b) (7)(E) [Redacted]

005.060 Deceased Auxiliary Beneficiary Project (BIC D) - National Operation Code "DA"

A. The Deceased Auxiliary Beneficiary Project, known as "BIC D," was developed to prevent and detect fraud, waste and abuse against SSA's Old-Age, Survivors and Disability Insurance (OASDI) program. This project involves computer analysis of SSA payment records and death information. Specifically, the names of Title II auxiliary beneficiaries, primarily beneficiary identification code (BIC) "D" (widows/widowers) and "W" (disabled widows/widowers), in current pay status on the Master Beneficiary Record (MBR) are compared against the Numerical Identification (Numident) file. The objective is to determine whether Title II benefits continue to be paid after the death of the auxiliary beneficiary has been posted to his/her Numident record. The project has uncovered many instances of payments to deceased widows via direct deposit to dormant accounts, as well as recovery of actual checks in their original envelopes from family members. Additionally, criminal cases have been developed involving subjects who withdrew from a joint bank account thousands of dollars in SSA benefits paid to their deceased mothers or fathers.

B. (b) (7)(E) [Redacted]

C. (b) (7)(E) [Redacted]

1. (b) (7)(E) ;
2. (b) (7)(E) ;
3. (b) (7)(E)
4. (b) (7)(E)

(b) (7)(E)

- D.** This project requires close coordination with the Bureau of Vital Statistics (BVS) in each of the States to obtain death certificates for the beneficiaries or otherwise verify the date of death. Another method to obtain BVS information is through SSA's Access to State Records Online (SASRO). Each OI Field Division will have the ability to directly access their own State's BVS data.
- E.** IAD works closely with the Field Division Coordinators to discuss and share strategies on the most effective methods to enhance our investigative activities and opportunities.
- F.** Cases will be input into NICMS using the National Operation Code "DA" and the appropriate local project code as indicated on the case opening screen and on each individual subject screen. The codes will already be entered in the NICMS upload, and should propagate onto the case screens. The codes will assist us in tracking statistical achievements.
- G.** If it is established that the beneficiary is alive, the OI FD will refer the matter to the local SSA office and advise that the Numident record is in error.
- H.** In some cases local prosecutors have agreed informally to prosecute these cases by bundling them together.

005.070 Residency Fraud

- A.** Residency verification projects are related to the SSI program, which requires that recipients not be absent from the United States for more than 30 consecutive days. Typical projects have included:
 1. SSA contract residency verification projects along our northern and southern borders that are potential sources for investigations.
 2. SSI Eligibility Review Projects, conducted jointly by OI and SSA, focus on SSI recipients (b) (7)(E)
- B.** The Department of Treasury Financial Crimes Enforcement Network (FinCEN) is available to provide assistance with residency fraud projects. FinCEN representatives are able to conduct financial and foreign travel queries on subjects.

Homeland Security Projects

A. In carrying out its duty to prevent and detect waste, fraud, and abuse in the Social Security Administration (SSA) and its programs, the Office of Investigations (OI) also has a responsibility to identify, investigate, and report activities and actions that have an impact on the homeland security of the United States. OI's Homeland Security Program focuses on those who attempt to obtain or use false or fraudulent Social Security numbers (SSN). The intent for which the SSN is sought is the determining factor as to whether or not the investigation of the event is considered to be part of the OI Homeland Security Program. (b) (7)(E)

[Redacted]

B. During the course of an investigation, OI agents must decide if the investigation fits the broad criteria established under the OI Homeland Security Program as described above. Agents must track their work in this program by having the investigation assigned the National Operation Code for Homeland Security (HS).

C. Projects that fall within the OI Homeland Security (HS) Program require a written plan/memorandum, which should be submitted to OI-HQ via IAD. The plan/memorandum should follow the format set forth in [Exhibit 5-0](#), Request for Approval to Establish Investigative Project, and must be submitted to the Director or SAC, with a copy to the appropriate regional desk officer, Criminal Investigations Division (CID), and Outlook mailbox ^Investigative Projects. The plan/memorandum should be directed to the appropriate DAIGI. Prior to implementing any Homeland Security project, the Office of Counsel to the Inspector General (OCIG) must review the project plan and the appropriate DAIGI must approve it.

The proposed plan should address the following issues:

1. (b) (7)(E) [Redacted]
2. (b) (7)(E) [Redacted]
3. (b) (7)(E) [Redacted]
4. (b) (7)(E) [Redacted]
5. (b) (7)(E) [Redacted].

D. Projects that typically are identified as Homeland Security projects include those involving:

- (b) (7)(E)
- [Redacted]
- [Redacted]
- [Redacted]

█ (b) (7)(E)

█ [REDACTED]

E. Projects that require the review/verification of a large number of SSNs are to be coordinated with IAD. However, no requests for SSN verifications should be made to IAD until the appropriate DAIGI approves the project plan. In addition, for those projects which do not require SSN verification assistance from IAD, Field Divisions will not initiate their own SSN verifications until the appropriate DAIGI approves of the project plan.

F. (b) (7)(E) [REDACTED]

G. Photocopies of SS-5 forms can be obtained from the Security Records Center (SRC) in Boyers, Pennsylvania (Boyers). Boyers processes requests that are received via the SS-5 Reprints online application process, fax, or e-mail.

1. SS-5 Reprints Application Instructions (preferred method)

Prior to accessing the site, you should have the Numident available for the record(s) you are requesting.

The website address is (b) (7)(E) This will take you directly to the SS-5 Reprints Homepage. The system automatically recognizes your pin and worksite address information. Authorized users are then able to submit requests. If you are not identified as an authorized user, you are instructed to contact the Office of Central Operations (OCO) Help Desk, via the email link provided, to request user authorization.

(b) (7)(E) [REDACTED]

(b) (7)(E) [REDACTED]

(b) (7)(E) [REDACTED]

2. FAX and E-mail Instructions

In addition to the online request method, requests for SS-5 photocopies may also be faxed or e-mailed directly to Boyers. Boyers will reply by faxing the photocopies directly to the specified office(s). In most instances, the photocopies will be sent within 24 hours.

(b) (7)(E)

Contact your CID regional desk officer should any issues arise that need to be coordinated through Headquarters.

- H.** Projects that result in the indictment and planned arrest of individuals associated with facilities as identified in paragraph D above require advanced notification to IAD prior to the execution of the operation. The information to be forwarded to IAD includes:
1. the date the operation is to commence;
 2. the number of individuals indicted and a breakdown of the charges (i.e. 10 persons indicted on Title 18 1001 or 1546 violations, five persons indicted on Title 42 violations); and
 3. whether or not the United States Attorney's Office (USAO) plans to issue a press release, and if so, the name and contact number of the USAO Public Affairs Officer (PAO). The PAO information will be forwarded to the Public Affairs Officer, Office of the Inspector General, for coordination purposes.
- I.** IAD has been tasked with monitoring the execution of any HS project. On the date of the operation, IAD will man and coordinate a Headquarters Command Center. The FD must provide IAD with periodic updates as to how the operation is progressing. During and immediately following the execution of the operation, the Special Agent or designee must provide updates to the IAD staff member, including details concerning the numbers of individuals arrested (and on which violations), any incidents, and media coverage. Also, fax a copy of the Press Release to the IAD staff member at (b) (7)(E). Finally, forward details of any subsequent arrests made after the execution of the operation to the attention of the IAD staff member.
- J.** (b) (7)(E) The total number of these apprehensions and any unusual incidents that occurred during the operation will be recorded in the OI-4 Report of Investigation for this operation.
- K.** Any arrest claimed must have a charge that specifically pertains to SSA violations and the case file must then contain the information listed in Chapter 3, Section 003.140, B1.

005.085 **Worksite Enforcement Operations**

- A.** Worksite Enforcement Operations conducted with the DHS-Homeland Security Investigations are tracked under NICMS National Operation Code "WE," which should be used for all allegations and cases generated for this type of operation.
- B.** Protocol for developing a worksite enforcement project with ICE is as follows:

1. (b) (7)(E)
2. (b) (7)(E)
3. (b) (7)(E)
4. (b) (7)(E)

C. The FD should provide IAD with updates as to any significant investigative activities conducted throughout the course of the operation.

005.090 Intelligence and Analysis Division

A. The Intelligence and Analysis Division (IAD) obtains and analyzes data for the Office of Investigations. IAD staff can extract information from SSA data repositories to facilitate investigations and anti-fraud projects. Upon Field Division request, IAD can also analyze the extracted data, through analytical techniques such as link analysis, timelines, histograms, as well as providing written reports detailing the analytical findings.

B. In order to start the processing of an information technology request, submit an OI-70 Request for Data/Data Analytics (see [Exhibit 5-2](#)) via e-mail to the IAD Director or SAC with a “cc” to the IAD Project Manager (currently (b) (6)) and Lead IT Specialist (currently (b) (6)).

C. Special Requirements

1. Enumeration Verification System (EVS) Input Requirements - If the record count is less than (b) (7)(E) records, receiving your input data in an Excel spread sheet is preferred, either as an email attachment, or on a CD-ROM if the file is large. SSA/OIG’s network will not allow email attachments larger than (b) (7)(E). ZIPPING to compress the file so it can attach to the email works too. Submit files of (b) (7)(E) or more records in a “dbf” (dBASE) or “mdb” (Access) database file. Password protect file attachments in order to safeguard Personally Identifiable Information.

Do not send multiple files for a single project. Combine multiple files into one file.

a. (b) (7)(E)

1. (b) (7)(E)

2. (b) (7)(E)

3. (b) (7)(E)

(b) (7)(E) [Redacted]

4. (b) (7)(E) [Redacted]

b. (b) (7)(E) [Redacted]

2. Technical questions can be directed to IAD's IT Specialists.

Chapter 5 — **EXHIBITS**

[5-0 — Request for Approval to Establish Investigative Project](#)

[5-1 — Guide to Third-Party Facilitator Investigations](#)

[5-2 — Request for IAD IT Support \(OI-70\)](#)

[5-3 — Request for Approval of Special Investigative Operation](#)

[5-4 — Cross/Uncross SSN Request](#)

OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

XXX Field Division

MEMORANDUM

Date: Refer To: SAH 005.020

To: (b) (6)
Assistant Inspector General for Investigations

Thru: Name of DAIGI
Deputy Assistant Inspector General for Investigations
Western or Eastern Field Operations

From: Special Agent-in-Charge
XXX Field Division – XXX Office

Subject: Request for Approval to Establish Investigative Project

Case No: XXX-XX-XXXXXX (if applicable)

Following is a request for approval to establish an Investigative Project.

1. Program Affected:

2. Project Name:

3. Case Agent, Field Division

4. Reason for Project:

The request must include a reasonably detailed statement of the background of the case/situation, and relate the circumstances for establishing a project.

a. Review of Investigation/Issue to Date:

b. Scope/National Implication of Project:

The information contained in this document is legally privileged and confidential information. If the reader of this document is not the intended recipient, you are hereby notified that any dissemination, distribution or copy of any part of this document is strictly prohibited. Public availability to be determined under 5 U.S.C. 552.

OFFICE OF INVESTIGATIONS

XXX (Office Address)

City, State & Zip Code



XXX Field Division

- c. Objectives:**
- d. Future Plans:**
- 5. Offense/Statutes:**

Include the *citations* of all anticipated offenses.
- 6. Location of Project:**

The request must specify the location and primary judicial district where the project will take place.
- 7. Names:**

The names of the expected targeted individuals and/or enterprises in the project must be provided, of applicable.
- 8. Test Samples**

Address the potential to conduct a sampling in order to test the feasibility of the proposed Investigative Project. Prior successful cases may serve as the “sample.”
- 9. Potential for CMPPA**

Address whether this proposal may require the use of a computer matching agreement.
- 10. Trial Attorney Approval:**

The request must state that the facts of the investigation have been discussed with the United States Attorney, Assistant United States Attorney (AUSA), or other authorized prosecuting attorney for the judicial district where the project will occur. Identify the attorney by name, and state that the attorney has specifically approved the activity (include the date of the approval).
- 11. Unusual Expenses:**

If it is anticipated that the project will incur expenses that are above normal costs of business, the request must show the projected costs in detail; include travel, per diem, supplies, and equipment necessary for the operation.
- 12. Other Law Enforcement Agencies Involved:**
- 13. Shared Data:**

Address whether nor not data will be shared with another agency, and if so, what data will be shared. Example: Disclosure of SSA data from OIG case file will be made only in accordance with existing laws, regulations, and policies, including the Special Agent Handbook. SSN verification data pertaining only to potential SSN misuse violations will be shared with the Department of Veterans Affairs OIG and the USAO. Tax return information from SSA’s database is not anticipated to be accessed for this project; however, if it is, it will be disclosed only to the Department of Justice, and only as necessary for the proper administration of the Social Security Act.

THIRD PARTY FACILITATOR INVESTIGATIONS

(b) (7) (E)



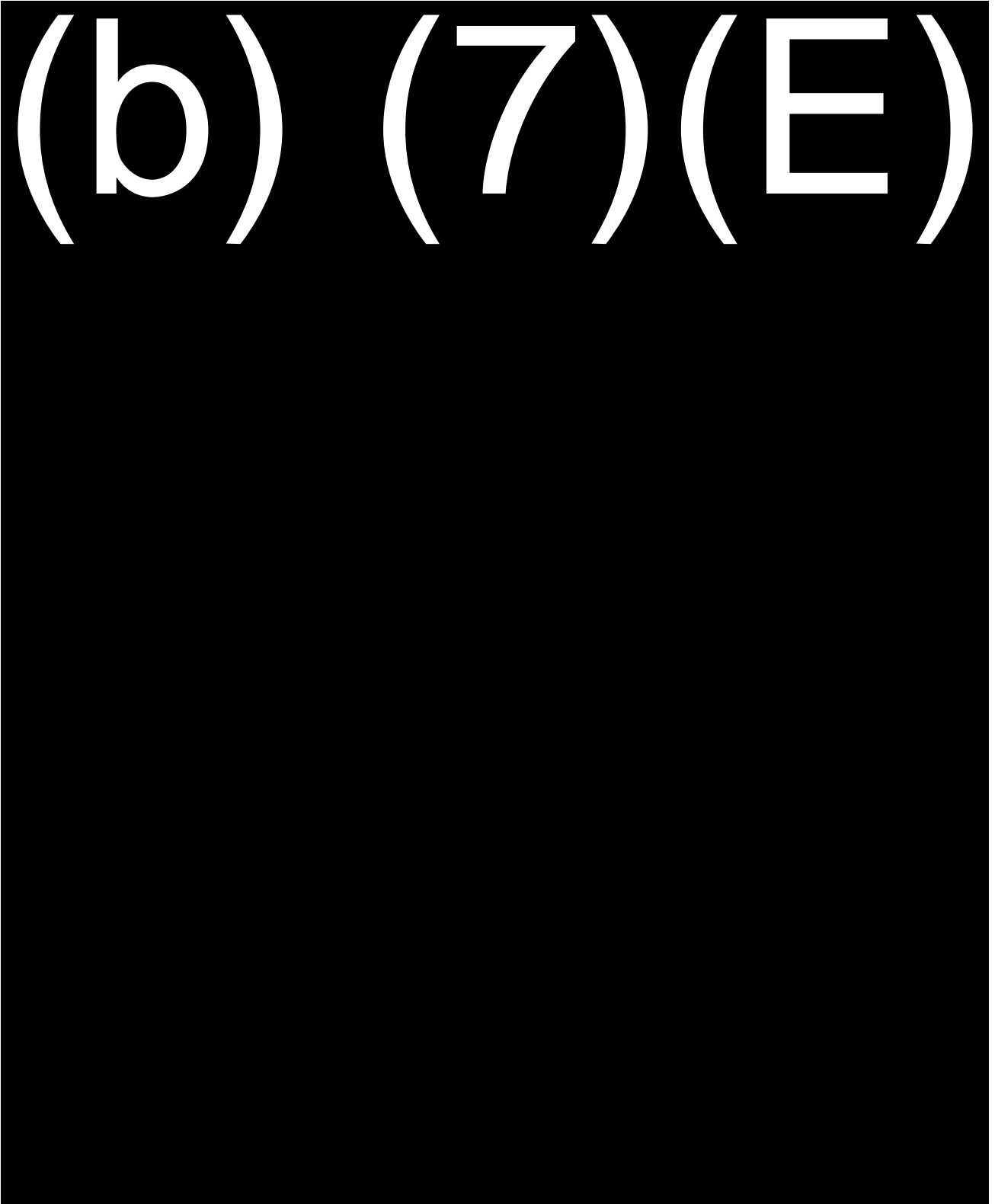
(b) (7) (E)



(b) (7) (E)



(b) (7) (E)

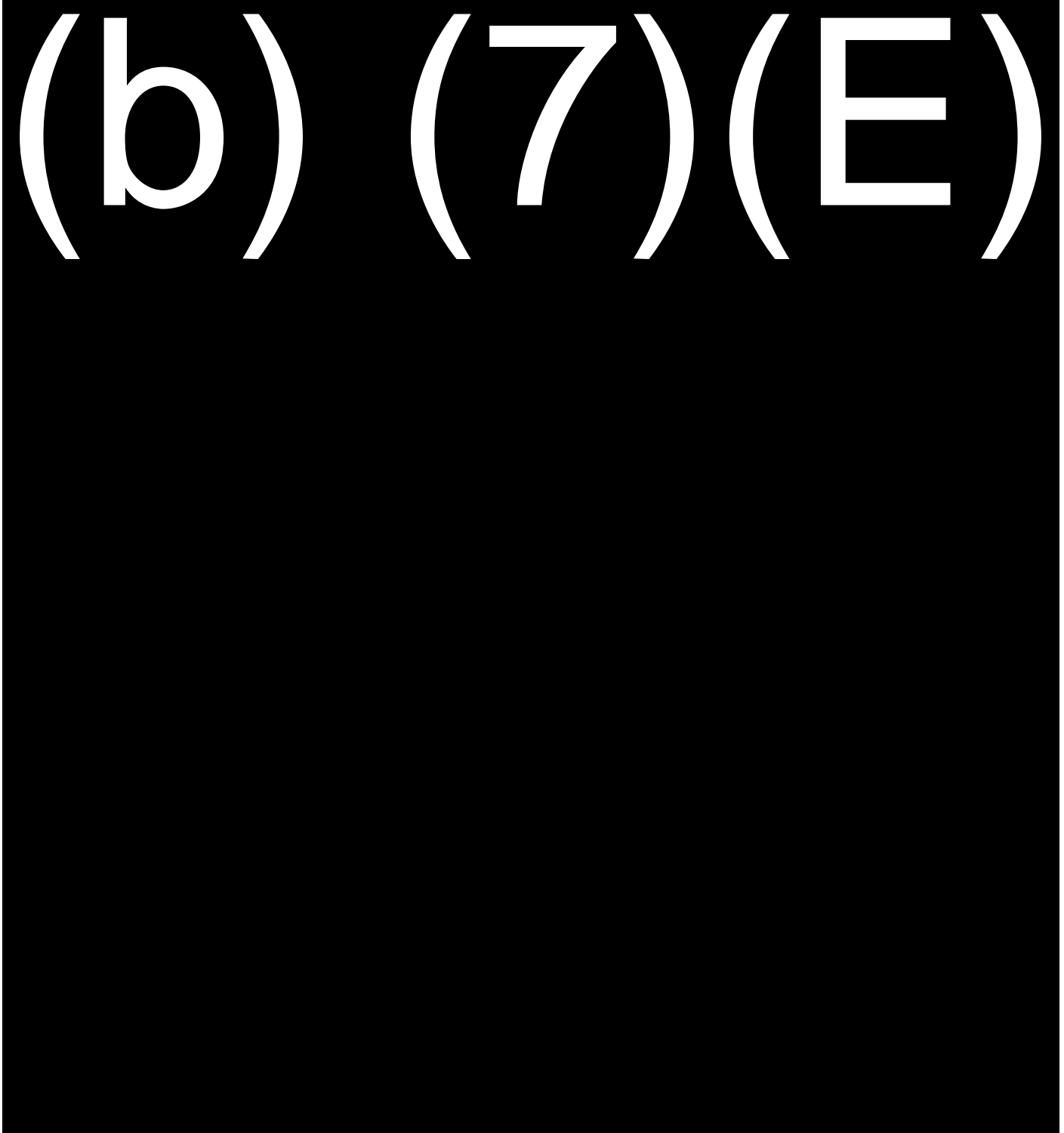




Office *of the* Inspector General

SOCIAL SECURITY ADMINISTRATION

Request for Data/Data Analytics



OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

XXX Field Division

MEMORANDUM

Date: Refer To: SAH 005.080

To: **(b) (6)**
Assistant Inspector General for Investigations

Thru: Name of DAIGI
Deputy Assistant Inspector General for Investigations
Western or Eastern Field Operations

From: Special Agent-in-Charge
XXX Field Division – XXX Office

Subject: Request for Approval of Special Investigative Operation

Case No: XXX-XX-XXXXX

RE: Alleged Identity Theft / SSN Misuse by Employees of XXX (Company Name)

1. Reason for Activity:

The request must include a reasonably detailed statement of the background of the case, and relate the circumstances requiring the operation. A description of proposed methods should also be included. The following items are pertinent to the request:

- Must articulate suspicion of SSN violations, i.e. 42 USC §408
- Probable Cause
- Preliminary work completed by ICE/participating agencies
- SSA/OIG involvement
- The employer/management officials should be a “Target” of the investigation
- Size/universe of SSNs being misused

2. Offense:

Include the *citations* of all alleged offenses. (Start with 42 USC §408)

The information contained in this document is legally privileged and confidential information. If the reader of this document is not the intended recipient, you are hereby notified that any dissemination, distribution or copy of any part of this document is strictly prohibited. Public availability to be determined under 5 U.S.C. 552.

OFFICE OF INVESTIGATIONS

XXX (Office Address)

City, State & Zip Code



XXX Field Division

3. Danger/ Contingency Plans:

Potential/anticipated danger and actions to protect any participant in an undercover or special operation must be noted in this section. The request must also state the intended contingency plans, that an OI-17 has been prepared and is on file, or that a tactical plan will be prepared by the lead agency and will be on file prior to the initiation of the operation.

4. Location of Operation:

The request must specify the location and primary judicial district where the operation will take place. If the location changes, notice should be given promptly to the approving DOJ and OI HQ officials.

5. Duration and Dates:

The request must state the day the operation is scheduled to begin. The request must show the anticipated starting and ending dates of the activity.

6. Names:

The names of the expected targeted individuals and/or enterprises in the operations must be provided.

7. Trial Attorney Approval:

The request must state that the facts of the investigation have been discussed with the United States Attorney, Assistant United States Attorney (AUSA), or other authorized prosecuting attorney for the judicial district where the activity will occur, and that the prosecutor will consider charging and prosecuting SSN violations, i.e. 42 USC §408. Identify the attorney by name, and state that the attorney has specifically approved the activity (include the date of the approval).

8. Unusual Expenses:

It is anticipated that the operation will incur expenses that are above normal costs of business, the request must show the projected costs in detail; include travel, per diem, supplies, and equipment necessary for the operation.

9. Other Law Enforcement Agencies Involved:

10. Shared Data:

Disclosure of SSA data from the OIG case file will be made only in accordance with existing laws, regulations, and policies, including the Special Agent Handbook. SSN verification data pertaining only to potential SSN misuse violations will be shared with ICE and the USAO. Tax return information from SSA's database is not anticipated to be accessed for this operation; however, if it is, it will be disclosed only to the Department of Justice, and only as necessary for the proper administration of the Social Security Act.

OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

XXX Field Division

**THIS CROSS/UNCROSS REQUEST IS LIMITED TO OIG OFFICE OF INVESTIGATION CASES ONLY.
NOT AUTHORIZED FOR USE BY OIG OFFICE OF AUDIT CASES.**

Prepared by:

SSN Holders Name:

Address:

Telephone:

FIRST NAME	MIDDLE NAME	SURNAME	DOB MO-DAY-YR	SEX	SSN

REMARKS

ATTACHMENTS HERE:

(b) (7)(E)

RO ENUMERATION COORDINATOR RESPONSE:

ACCESS TO SOCIAL SECURITY INFORMATION

006.000 **Introduction**

The system of records used by the Social Security Administration (SSA) to create, maintain, categorize, track, revise, and amend the accounts of over 500 million individuals (to date) is complicated and complex. It is incumbent on the Agency and the Office of the Inspector General to safeguard this vast array of personal information and to disclose such data to other entities only to the extent permitted by law. This chapter has been designed to summarize the relevant disclosure laws and policies and to guide special agents through the maze of SSA computer screens, sub-screens and acronyms. This chapter will enable special agents to quickly and successfully obtain the information necessary to successfully conclude investigations associated with individuals and entities alleged to have violated civil laws, criminal laws and/or administrative policies related to the SSA.

- A. Numerous Acts have been passed by Congress to protect the privacy of information held by governmental agencies and financial institutions, as that information relates to American citizens and Foreign Nationals. Those Acts include the Social Security Act, as amended, the Right To Privacy Act of 1974, the Right To Financial Privacy Act, the Social Security Independence and Program Improvements Act of 1994, and Title 20 of the Code of Federal Regulations. Those Acts and regulations, the policies contained within the SSA's Program Operations Manual System (POMS) and the SSA OIG/OI *Special Agent Handbook (SAH)* serve to inform, advise and alert OIG's special agents to the restrictions associated with accessing SSA records, as well as to the release of that information to other parties.
- B. **All unauthorized access into, and/or releases of information from, the system of records maintained by SSA are serious.** The final determination as to whether a *particular* access and/or release rises to the level of criminal misconduct only speaks to the seriousness of the violation. The **minimum** penalty for **any** form of unauthorized access and/or release of SSA information is a two (2) day suspension from Federal service without pay. The potential **maximum** penalty is incarceration, fine, and termination from Federal service. **Do not** access SSA records and/or release any SSA information unless you are **absolutely certain** that you are legally authorized to do so. If in doubt, consult your ASAC/RAC or the Office of Counsel to the Inspector General (OCIG).
- C. All OIG employees are required to adhere to the guidelines established by SSA's Office of the Chief Information Officer (OCIO) regarding safeguarding Personally Identifiable Information (PII) while in transit or outside of secure SSA space. (See section [006.160](#) of this chapter for additional details.)

006.010 Disclosure of Records and Information by OIG Special Agents

A. Disclosure from OIG Records

1. Disclosure of information by OIG SAs is limited. There are rare circumstances in which OIG SAs may disclose information to law enforcement and other Federal, State and local agencies. The most frequently encountered situations are addressed in this chapter; any disclosure not permitted by this chapter may be made only after consultation with OCIG.
2. There are three broad categories of permissible disclosures from OIG records by OIG SAs.

a. Open Joint Investigations

Any information contained in an open OI investigative case file may be disclosed to officials of another Federal, State or local law enforcement agency **if**:

1. the information in question is not “tax return” information provided to SSA by the Internal Revenue Service; *and*
2. SSA OIG and the requesting agency are conducting the investigation jointly, and SSA OIG is actively involved; *and*
3. the requested information is relevant to an enforcement proceeding, investigation, or prosecution within the requesting agency’s jurisdiction.

b. Consent

Records in OI’s possession (including those incorporated in open or closed investigative case files) may be disclosed by OIG SAs, **if**:

1. the information in question is not “tax return” information provided to SSA by the Internal Revenue Service; *and*
2. the individual consents in writing, and OCIG confirms that the written consent is legally sufficient (Form SSA-3288, [Exhibit 6-44](#), should be used whenever possible); *and*
3. the records are reviewed by OCIG, in consultation with OI, prior to their release to ensure that any necessary redactions are made.

- c. Other** – In very narrowly defined instances, disclosures that do not fall under either of the above categories may be made. Such disclosures require consultation with OCIG, and in some cases, SSA. If an SA feels that disclosure is warranted in a situation that does not fit the parameters described above, he or she should consult with their ASAC/RAC and contact OCIG for further guidance.

B. Disclosure from SSA Records

Generally, only SSA may disclose information directly from SSA records. There are only two situations in which OIG SAs may make such disclosures:

1. In extremely rare circumstances (e.g., immediately after September 11, 2001), the Inspector General will request that the Commissioner exercise *ad hoc* authority to disclose information that would generally be protected from disclosure by SSA's regulations. Should such an emergency arise, SAs should immediately contact their supervisor(s) for further consultation with OCIG and the AIGI and/or the IG.
2. Under the terms of a Memorandum of Understanding (MOU) between SSA and OIG, OIG SAs may verify for Federal, State, and local law enforcement officials whether a given name and SSN match. In order to utilize this authority, the request must:
 - a. be in writing via mail or fax;
 - b. be on the official letterhead of the requesting agency;
 - c. be signed by a law enforcement official;
 - d. include the name and SSN to be reviewed; and
 - e. include a certification that the individual in question is suspected of misusing an SSN or committing another crime against a Social Security program.

The procedures and recordkeeping requirements for SSN verifications run pursuant to the MOU are set forth in section 006.025 below.

006.015 Disclosure of Tax Return Information

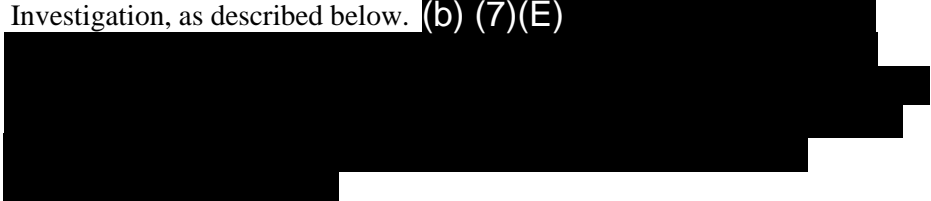
- A. The Internal Revenue Code strictly limits the disclosure of "tax return" information contained in SSA (and OIG) records. No disclosure of such information may be made except as permitted under [26 U.S.C. § 6103](#).
- B. Pursuant to 26 U.S.C. § 6103, the OIG may disclose tax return information from its files *only*:
 1. to the Department of Justice (including the FBI and United States Attorneys); *and*
 2. if the disclosure is for the purpose of administering the Social Security Act.
- C. "Tax Return" information includes:
 1. wage amounts from a W-2 statement or an SSA-794;
 2. names and/or addresses of employers and their employees that appear on summary or detailed earnings query responses or on earnings record forms; and
 3. debtors' addresses that may appear on the response to a query that displays tax refund offset activity.

006.020 Penalties for Unlawful Disclosure

The *Social Security Independence and Program Improvements Act of 1994* increased the penalty for unlawful disclosures of SSA and/or IRS information from a misdemeanor to a felony (Section 1106 of the Social Security Act). As such, SAs are advised to consult with OCIG any time a question arises as to the propriety of a disclosure.

006.025 SSN Verification Policy

A. Memorandum of Understanding

1. Pursuant to a Memorandum of Understanding between the Social Security Administration (SSA) and the SSA Office of the Inspector General (OIG), the OIG has the delegated authority to verify Social Security number (SSN) information for Federal, State, and local law enforcement agencies. Under the MOU, OIG Special Agents, with approval from that Special Agent's Special Agent-in-Charge (SAC), may verify that a name and SSN do or do not match upon proper request from a law enforcement agency.
2. This policy pertains only to requests for SSN verification; existing disclosure policy remains in place for requests for any other information from SSA or OIG records.
3. This policy permits verification only as to individuals who are under active Investigation, as described below. (b) (7)(E)

4. This policy does not apply if the SSN has never been issued, or if the individual is deceased.

B. Proper SSN Verification Requests

1. Before an OIG Special Agent (SA) may provide SSN verification information, he or she must be in receipt of a proper law enforcement request. The request must be:
 - In writing;
 - On official letterhead of the requesting agency (a fax cover sheet is NOT adequate for this purpose);
 - Signed by a supervisory law enforcement official. Example: Assistant Special Agent-in-Charge (ASAC)/Resident Agent-in-Charge (RAC) level (or equivalent), if a Federal law enforcement agency, and at the level of Sergeant (or equivalent) or above, if a State/local law enforcement agency. (*Note: Requests in which a law enforcement official signs “on behalf of” the appropriate supervisor, as outlined above, will meet this requirement, as long as the supervisor’s name and title are included.*);

- Include the name and SSN to be reviewed (verification of an individual request is limited to 20 name and SSN combinations or less; requests exceeding this amount must be approved by the SAC or Director of the Intelligence and Analysis Division (IAD)); and
 - Include a certification that the individual about whom information is sought (*the individual under investigation is not necessarily the individual whose SSN is being verified; e.g. if an individual under investigation is found in possession of multiple genuine or counterfeit SSN cards, OI may verify whether or not the names/SSNs on the cards match*) is suspected of misusing an SSN or committing another crime against a Social Security program (*i.e. there must be a statement that the requesting law enforcement agency is investigating or prosecuting fraud or another criminal activity under statutes within their jurisdiction which involves SSN misuse or another crime against a Social Security program*).
2. The request may be sent by mail or via facsimile.

C. Responses to Verification Requests

1. SSN verification limit (per individual law enforcement agency request) and authorizing official
 - a. Twenty or less must be approved by a designated official in the OI office in which the request is received. In field divisions (FD), the SAC may review the requests personally or delegate that authority to an ASAC or a RAC. In offices with an ASAC or RAC, the ASAC or RAC may be delegated by the SAC to review such requests. In offices without an ASAC or RAC, the senior SA may be delegated by the SAC to review such requests.
 - b. Requests over 20 must be submitted through the designated OI FD official and approved by the SAC of IAD.
2. Once approval is obtained, any qualified OI employee may query the numident or alphident databases and obtain the necessary information to verify that the name and SSN do or do not match. The employee conducting the query must enter the letters "LEVER," "JTTF," or "FBI" in the unit field for SSN verification to indicate that the query was conducted for a law enforcement agency, a Joint Terrorism Task Force or the Federal Bureau of Investigation, respectively.
3. The SSN verification may be communicated to the requesting law enforcement official in writing or verbally. If the communication is verbal, the original request shall be marked by the SA making the response to include the name of the SA, the date of the response, the substance of the response (match or non-match), and the name of the law enforcement official to whom he or she spoke.
4. Once a response has been made, the original request, together with the written response (if any) shall be forwarded to the SAC for the FD to which the responding SA is assigned.

D. Reporting Requirement

1. Under the terms of the MOU, the OIG is required to report annually to the Commissioner the number of SSN verifications made to law enforcement agencies.
2. Not later than 10 days after the end of each fiscal year (FY), the SAC of the Criminal Investigations Division (CID) shall forward to the Deputy Assistant Inspector General for

Investigations—Field Operations a total number of requests received (and responses made, if this number is different) during the FY. This data will be based upon a query of the total SSN verifications done by OIG personnel that were designated with an applicable unit designation (i.e. LEVER, JTTF, FBI) at the time the query was requested from SSA records.

3. Each SAC shall keep a master file of all requests (and responses) for SSN verification. Records from each FY shall be retained for a period of one year from the end of that FY. Thus, records from FY 2012 may be destroyed on October 1, 2013.

E. Opening Investigations

1. It is not necessary to open an investigative file on each SSN verification request or to log each request into the National Investigative Case Management System (NICMS).
2. In the event that a request raises issues of fraud against SSA such that an investigation is warranted, a case may be opened and, if worked jointly with the requesting agency, additional information may be shared consistent with Section 006.010.

3. (b) (7)(E) [REDACTED]

F. Improper or Fraudulent Requests

1. (b) (7)(E) [REDACTED]

2. (b) (7)(E) [REDACTED]

006.030 Access Documentation

- A. OI personnel should access SSA’s Modernized Claims System (MCS) only when there is a suspected Social Security Act violation and an allegation or case number has been assigned.
- B. OIG/OI will be required by SSA to verify the validity of each query. The following steps should be taken to establish an audit trail on queries requested:
 1. Each OIG/OI employee should have his/her own PIN and use only his/her own PIN.
 2. When requesting a query from the SSA MCS, the OIG/OI employee must indicate in the unit field on the query screen the five-digit case file number or allegation number of the case/allegation for which he/she is requesting the query. (b) (7)(E) [REDACTED]

006.040 Certifications

- A. SACs shall certify the validity of each MCS query made by their staff monthly. Generally, the data is available for review by the fifth working day of each month.
- B. Every OI employee must sign the OIG Annual Systems Security Certification (see [Exhibit B](#) of the *OIG Administrative Policy & Procedures Manual* Chapter 7, “Employee Conduct”):
 - 1. within 30 days of his/her entry-on-duty date; and
 - 2. each subsequent year by the end of October.

SACs are responsible for ensuring that the signed forms are properly maintained in their divisions. More information is available in [section 7-60](#) of the *OIG Administrative Policies and Procedures Manual*.

006.050 Control of SSA’s Claims, Files, and Documents

- A. Under Social Security law, persons seeking to establish entitlement to benefits must file an application. After an individual files a claim for those benefits at a local Social Security office and that office has developed all relevant aspects of the claim, the file will be maintained either electronically or in a paper folder. If paper, the paperwork is maintained in separate locations depending on the SSA program involved.
- B. Title II case files are sent to one of six SSA Program Service Centers (PSCs), according to the SSN, for review and payment. The following link can be used to verify accuracy of PSC contact information: **(b) (7)(E)**
 - 1. Social Security retirement and survivors benefits are processed for payment from one of five SSA PSCs. The applicable PSC that handles an individual’s claim is determined by the first three digits of a person’s SSN. There is an Integrity Staff or Integrity Branch in each of these SSA PSCs that can be contacted should the SA need a file that was not forwarded to them with the allegation. These PSCs are:
 - a. Account Number Breakdown: **(b) (7)(E)**

Northeastern Program Service Center (NEPSC)

New York (NEPSC)
Social Security Administration
Center for Security and Integrity
26 Federal Plaza
Room 40-160A
New York, NY 10278

Telephone: (212) 264-2604

Fax: (212) 264-0916

- b. Account Number Breakdown: (b) (7)(E)

Mid-Atlantic Program Service Center (MATPSC)

Philadelphia MATPSC
Social Security Administration
Office of the Regional Commissioner
Center for Security and Integrity
Attn: (b) (6)
P.O. Box 8788
Philadelphia, PA 19101

Phone: (215) 597-1014
Fax: (215) 597-5203

- c. Account Number Breakdown: (b) (7)(E)

Great Lakes Program Service Center (GLPSC)

Chicago GLPSC
Social Security Administration
Center for Security and Integrity
P.O. Box 87479
Chicago, IL 60680

Phone: (312) 575-4120
Fax: (312) 575-4121

- d. Account Number Breakdown: (b) (7)(E)

Southeastern Program Service Center (SEPSC)

Atlanta SEPSC
Social Security Administration
Center for Security and Integrity
Birmingham Social Security Center
1200 Rev. Abraham Woods Jr. Blvd.
Birmingham, AL 35285

Fax: (205) 801-1332

- e. Account Number Breakdown: (b) (7)(E)

Mid-America Program Service Center (MAMPSC)

Kansas City MAMPSC
Social Security Administration
Center for Security and Integrity

MAMPSC
P.O. Box 15625
Kansas City, MO 64106

Telephone: (816) 936-5555
Fax: (816) 936-5573

- f. Account Number Breakdown: (b) (7)(E)

Western Program Service Center (WPSC)

San Francisco WNPSC
Social Security Administration, SFRO
Center for Security and Integrity
P.O. Box 4206
San Francisco, CA 94804

Fax: (510) 970-2644

After being processed, benefits are paid from one of the United States Treasury Disbursing Centers around the country, depending on the SSN.

2. Title II disability cases are processed in the Office of Central Operations (OCO), Baltimore, Maryland, and United States Treasury checks for these payments are issued from the United States Treasury Disbursing Center, Philadelphia, Pennsylvania. The claims folders for disability cases in which the subject is under the age of 55 are maintained in the OCO Megasite. The Center for Security and Integrity (CSI) assist OIG in retrieving disability folders for cases under investigation.

Office of Central Operations (PC7 or PC8)

Social Security Administration
Office of Central Operations
Center for Security and Integrity
1500 Woodlawn Drive or P.O. Box 32921
1500 Woodlawn Drive
Room 7040 SWT
Baltimore, MD 21241

Fax: (410) 966-3554

When an individual who is receiving disability payments reaches age 55, the claims folder is transferred from OCO in Baltimore to one of the respective PSCs, depending on the claimant's SSN.

3. Criminal Investigations versus Administrative Determinations

- a. Disability investigations must address the fraud loss ("overpayment" in SSA terminology). CSI is the component of SSA responsible for terminating benefits and establishing when SSA can collect a Title II overpayment. Although the overpayment

calculations provided by SSA Field Offices are useful in developing a criminal case, the final determination as to entitlement and overpayment are the responsibility of CSI.

- b.** Information developed during an investigation may establish that an individual made a false statement for which the person can be prosecuted. However, a false statement conviction ([18 U.S.C. § 1001](#)) does not necessarily translate into fraud under SSA's regulations. The final determination as to entitlement and overpayment issues, which are administrative in nature, is made by CSI.
- c.** SAs working Title II disability investigations should contact CSI to determine how SSA's regulations will be applied in the particular case. Issues of evidence required for suspension or termination of benefits and computation of recoverable overpayments should be discussed.
- d.** SAs may contact CSI to discuss specific title II disability cases. If the individual staff member is not available, contact the Integrity Team Leader at:

P.O. Box 32906
1500 Woodlawn Drive
Room 7040 SWT
Baltimore, MD 21241
(410) 966-3554
e-mail: ||OCO Integrity Branch
FAX: (410) 966-3859

- 4.** Time factors involved in obtaining a disability folder and/or determination from HQ:
 - a.** The CSI has agreed to give OI's requests first priority.
 - b.** Requests for files will be responded to the day the call is made.
 - c.** Determinations and overpayment calculations for everything except medical eligibility will be completed in three weeks or less.
 - d.** Medical eligibility determinations will take longer, as they must be referred to the Disability Determination Service for medical review.
 - e.** Requests should be made to the CSI directly instead of the local district office (DO). The staff contact may need to see copies of certain documents from the investigation in order to make a determination or compute an overpayment, but should not need the entire claim file except in very unusual circumstances.
 - f.** Questions or problems concerning OI's involvement in title II disability investigations can be referred to the OI's representative to the OCO's work group through your Regional ASAC.
- C.** Applications for benefits and related documents for Supplemental Security Income (SSI) payments are either electronically stored, or consist of a paper file that is housed in the Social Security District/Branch Office (SSADO) which has administrative jurisdiction of the claim. If

the Title XVI files are not housed in the SSADO, usually that office can obtain the file for the OIG OI from the staging facility that does have it.

- D. It is essential that OI maintain SSA's paper files in the proper order, and return SSA's case files or documents to SSA once OI's actions are completed or as circumstances may otherwise require. When an original document is being removed from the SSA file, a copy of the original is to be temporarily placed in the SSA file as a precaution against total loss of the document. The copy will be annotated to show the location of the original.
- E. OI will honor an SSA request for the return of a claims file for necessary administrative action by SSA, even though an OI investigation is under way. Prior to returning the claims file, photocopy any documents in the file that are essential to OI's case.
- F. Upon completion of OI's investigation and any subsequent case actions, return all original SSA documents to the claims file, removing any photocopies that OI may have placed there in substitution.

006.055 **[Payment Extracts](#)**

- A. A payment extract is a record of payments made to beneficiaries by SSA. Payment extracts from SSA are certified records showing benefits paid to an individual during a set period of time and the name of the financial institution to which the money was deposited, if applicable. A certified payment document is intended to serve as a legal document that can be used in a court of law. These extracts are generally acceptable as evidence at fraud hearings in lieu of certified photocopies of checks and in lieu of testifying by the SSA official identified as the keeper of record. If all that is needed by the SA is a regular overpayment calculation, then see Chapter 004.030.F.5 of this Handbook. Additional information regarding payment extracts can be found in SSA's Program Operations Manual System (POMS), section GN 02406.147.
- B. SSA will provide certified payment extracts to the Office of the Inspector General upon request. SSA will produce most extracts within 20 working days from the receipt of the request. However, this timeframe may be longer if the period of time the overpayment request covers is exceptionally long. In cases where the request will exceed the 20-day timeframe, an SSA program analyst will contact the requesting SA, explain the reason for the delay, and provide a revised timeframe. Mail or fax a request letter (see [Exhibit 6-0](#), [Form OI-85](#)) for certified payment extracts to SSA for Title II Benefit payments. Requests for Title XVI payment extracts must be mailed or faxed to SSA. Address the requests as follows:

1. Title II Benefit Payments

Requests must be mailed or faxed to the Payment Service Center's (PSC) Regional Center for Security and Integrity (CSI) which has jurisdiction over the beneficiary's record (the PSC of jurisdiction is identified on the beneficiary's Master Beneficiary Record-MBR). See Section 006.050B1 for PSC contact addresses. In order for the CSI to manage the workflow and track the requests, SAs are not to email or fax requests to specific SSA employees, based upon a prior working relationship. All requests must go the appropriate Regional CSI.

2. Title XVI Benefit Payments

Mail or fax the request to the Regional Office of jurisdiction. Regional Office addresses follow:

Region 1 – Boston

Social Security Administration
JFK Federal Building
Room 1925
Boston, MA 02203
Fax: (617) 565-9359

Region 2 – New York

Social Security Administration
Center for Programs Support
Room 4060
26 Federal Plaza
New York, NY 10278
Fax: (212) 264-2071

Region 3 - Philadelphia

Office of the Regional Commissioner/Seventh Floor
Center for Programs Support
P.O. Box 8788
Philadelphia, PA 19101
Fax: (215) 597-2989

Region 4 - Atlanta

Social Security Administration
Center for Programs Support
Atlanta Regional Office
Suite 22T64
61 Forsyth Street, S.W.
Atlanta, GA 30303-8907
Fax: (404) 562-1325

Region 5 - Chicago

CRSI/SSI
PO Box 8280
Chicago, IL 60680-8280
Fax: (312) 575-4245

Region 6 - Dallas

SSA, MOS, CPS, SSI
1301 Young St, Ste 670
Dallas, TX 75202-5433
Fax: (214) 767-1348
Phone: (214) 767-4224

Region 7 – Kansas City

Center for Programs Support
ATTN: Certification Request
Room 1073, 601 E 12th St

Kansas City, MO 64106
Fax: (816) 936-5951

Region 8 - Denver

Social Security Administration - CPS
1001 17th Street
Denver, CO 80202
Fax: (303) 844-4280

Region 9 – San Francisco

Social Security Administration, SFRO
Center for Programs Support, 6th Fl
PO Box 4206
Richmond, CA 94804
Fax: (510) 970-8101
Attn: Regional Privacy Act Coordinator

Region 10 - Seattle

Social Security Administration, SPST
Suite 2900, MS 303A
701 5th Avenue
Seattle, WA 98104-7075
Fax: (206) 615-2643

**006.060 Requests for Testimony or Information/Records Needed from SSA for Prosecution
of Open SSA OIG Cases/Investigations**

- A. OI agents shall prepare written requests to SSA for testimony from SSA employees, or for information/records **not otherwise readily available (see below)**, for prosecutions in connection with open SSA OIG investigations, in accordance with the procedures set forth below. Note: Prosecutorial authorities may also elect to submit a subpoena with the written requests.

Written requests for information/records in accordance with the above policy and procedures are only contemplated when records are not readily accessible by other means. If certified records are otherwise available through other SSA sources, such as through field office direct requests, CSI, CPS or through SSA Web Apps, no written request pursuant to the above policy and procedures is necessary.

- B. When local, State, or Federal prosecutorial authorities seek agency testimony or information/records not otherwise available¹ for use in a legal proceeding (such as for a trial, a matter before a grand jury, or for a deposition in a civil matter) and OIG has an open investigation, the following policy applies if SSA testimony and/or information/records is needed:
1. The prosecutorial authority will work through OIG to obtain the necessary testimony and/or information/records.

¹ **Note:** Written requests for information/records in accordance with the above policy and procedures are only contemplated when records are not readily accessible by other means. If certified records are otherwise available through other SSA sources, such as through field office direct requests, CSI, CPS or through SSA Web Apps, no written request pursuant to the above policy and procedures is necessary.

2. OIG will submit a written transmittal using the *Request for Testimony and/or Information/Records Form* ([Exhibit 6-45 Form OI- 96](#)), which shall be sent via email to the SSA office from whom testimony and/or information/records are sought and the appropriate applicable office of the OGC Regional Chief Counsel (See link to potential contacts. <http://sharepoint.ba.ssa.gov/ogc/intranet/orcc.aspx>) or the Office of General Law (See link to potential contacts. <http://sharepoint.ba.ssa.gov/ogc/intranet/ogl.aspx>) stating the following:
 - a. The case caption – including a statement of whether the matter is a criminal or civil prosecution;
 - b. Name of the prosecutorial authority (including contact information of lead prosecutor);
 - c. A brief explanation of the testimony and/or information being requested, including the name of the employee being requested to testify (if applicable) and sufficient information to identify the individual about whom testimony or information is being requested, such as name, social security number and date of birth;
 - d. If the request is for testimony from a specific employee, include a brief explanation of why the testimony of that particular employee is required. Otherwise, describe the testimony needed, and SSA, in consultation with OIG, will identify the employee who possesses the necessary expertise and information, and will testify;
 - e. State whether the records sought must be certified;
 - f. Whether the agency or an agency employee is a party in the matter;
 - g. If SSA or an SSA employee is not a party, provide sufficient information to explain why providing the records or testimony is in SSA's interest (i.e., SSN fraud or benefit fraud is involved, needed for an open OIG investigation, etc.);
 - h. That OIG has an open investigation;
 - i. The name of the OIG special agent assigned to the investigation;
 - j. Date of expected testimony; and
 - k. Date of expected production of information/records.
3. The written transmittal will serve as the basis for OGC to determine whether the disclosure of the requested testimony and/or information/records is appropriate. Therefore, neither a subpoena nor official letter from the prosecutorial authority is required.
4. The requested testimony and/or information/records is presumed appropriate for disclosure if it is being requested as a result of a criminal or civil matter stemming from an OIG investigation as indicated in 2 h. above.
5. If OGC determines that the agency cannot comply with the request, within five business days of that determination, OGC will notify, in writing, the Counsel to the Inspector General (CIG). The writing will include the basis for not disclosing the information/records or providing the testimony. The notification may be by email. The CIG will provide a cc of the denial to the applicable OIG agent and CID at (b) (7)(E) upon receipt from OGC.

6. If any issues arise with regard to the production of information/records or testimony, contact the OCIG attorney on call at (b) (7)(E) for guidance.

006.065 Annotating “Special Message” Field of Benefit Records

- A. SAs can request that SSA annotate the “special message” field on its automated benefit records of Title II or Title XVI beneficiaries/recipients. The special message can be used to request that the SSA contact OI when the following events occur:
 1. (b) (7)(E)
 2. (b) (7)(E)
 3. (b) (7)(E)
- B. When requesting a special message through an SSA DO, the SA should request that the special message be entered as a “CIP-M” action on the DO’s data communications utility.
- C. When requesting a special message through the SSA PSC, the SA should request that the special message be entered through the PSC’s “NIXDORF” procedure.
- D. For Title II claims, the special message should conclude with a statement or phrase: “Do not replace OIG data” or “Retain OIG data.”
- E. For Title XVI claims, the special message field is an overlay field and cannot be preserved if a subsequent message is entered.

006.070 The Computer Matching and Privacy Protection Act

A. Overview

The *Computer Matching and Privacy Protection Act of 1988* (CMPPA) amends the *Privacy Act of 1974* and substantially limits Federal agencies’ use of computerized records covered by the Privacy Act. The CMPPA requires agencies to enter into detailed written agreements whenever certain automated Federal records are matched against records from other Federal and State/local databases.

This section outlines the circumstances in which a proposed match for a special investigative project would be covered by the CMPPA. Any unauthorized match and/or disclosure of covered records is a *serious* violation of the Privacy Act and subjects the Inspector General to civil liability. Accordingly, any matches of computerized records contemplated by OIG SAs that *may* implicate the CMPPA must be approved by OI management in consultation with OCIG.

B. Covered Matches

1. The CMPPA covers two kinds of matching programs: (1) matches involving Federal benefits programs, and (2) matches involving records obtained from Federal personnel or payroll systems of records.

2. **Federal Benefits Match** - Any match that meets the following four criteria:
 - a. **Computerized Comparison of Data** – a comparison of: (1) two or more Federal systems of automated records maintained by agencies that are subject to the Privacy Act, *or* (2) a Federal system of records with automated records maintained by a State or local government agency; *and*
 - b. **Federal benefit program** – matches involving records from a Federal benefits program which provides cash or in-kind assistance to individuals; *and*
 - c. **Matching purpose** – the purpose of the match is to: (1) establish or verify initial or continuing eligibility for Federal benefit programs; *or* (2) verify compliance with statutory or regulatory requirements of Federal benefit programs; *or* (3) recoup payments or delinquent debts under a Federal benefit program; *and*
 - d. **Covered subjects** – matches involving: (1) applicants for Federal benefit programs; *or* (2) Federal program beneficiaries; *or* (3) providers of services that support Federal benefit programs, *e.g.*, health care providers.

3. **Federal Personnel or Payroll Records Match** – Any match that meets the following criteria:
 - a. **Computerized Comparison of Data** – a comparison of: (1) two or more Federal systems of automated personnel or payroll records maintained by agencies that are subject to the Privacy Act, *or* (2) a Federal system of personnel or payroll records with automated records maintained by a State or local government agency (*Note: An internal agency match involving such Federal records is not exempt*); *and*
 - b. **Matching purpose** – the purpose of the match is: (1) done for other than “routine administrative purposes”; *or* (2) to take any adverse action (financial, personnel, or disciplinary) against Federal personnel; *and*
 - c. **Covered subjects** – matches involving: (1) officers/employees of the U.S. Government; *or* (2) members of the uniformed services; *or* (3) individuals entitled to retirement benefits under any Federal government retirement program, to include survivor’s benefits.

4. In the event that a special investigative project implicates the CMPPA, OCIG will coordinate with the appropriate SSA officials to execute an agreement.

C. Excluded Matches

1. The CMPPA does not apply to certain narrowly defined types of automated matches. Generally, the two exclusions that OIG SAs routinely encounter are the following:
 - a. **Law enforcement investigative matches** – matches performed in support of civil or criminal law enforcement activities are excluded if:
 1. the match flows from an investigation already underway involving a named person(s); *and*

2. the match is done for the purpose of gathering evidence against a named person(s).
 - b. **Internal Agency matches** – matches that use only internal Agency records are excluded, provided that if the records relate to Federal personnel, there is no intent to take adverse financial, personnel, or disciplinary action against those individuals.
2. If an SA has any doubt as to whether a proposed match is excluded from the CMPPA’s coverage, he/she should consult with OI management and/or OCIG.

D. Disclosure of Match Results

The results of computerized matches performed pursuant to a CMPPA agreement shall only be disclosed in accordance with the disclosure rules set out in Section 006.010.

006.080 Full Titles of Selected Acronyms

<u>Acronym-Title</u>	<u>Description or Use</u>
AACT – Abbreviated Account Query	Title II Summary Query
ADM – Assistant District Manager	SSA Position Title
ALPH – Alphident (Alpha Index Query)	Query by Name
BIC – Beneficiary Identification Code	Beneficiary Identifier
CDR – Continuing Disability Review	SSA Activity
CDRCF – Continuing Disability Review Control File	SSA Documentation
CNQY – Consolidated Query	Simultaneous Queries
CPS – Critical Payment System	Emergency Payments
CR – Claims Representative	SSA Position Title
DACUS – Death Alert Control and Update System	National Death File
DEQY – Detail Earnings Query	Employer and Earnings
DI – Disability Insurance	SSA Title II/XVI Programs
DIB – Disability Insurance Benefits	Entitlements
DM – District Manager	SSA Position Title
DO – District Office	SSA Facility
DOC – District Office Code	SSA Facility Identifier
DOORS – Detailed Office/Organization Support	SSA Facility Locator System
DXQM – Data Exchange Query Menu	Other Agency Records
EIN – Employer Identification Number	Numerical Designation for Employers
ERQY – Employer Report Query	Employer Information
FACT – Full Account Query	Full Title II Query
FOFM – Field Office Folder Movement	Tracking System
IBIQ – Interstate Benefit Inquiry Query	State Wage and Unemployment Information
MBA – Monthly Benefit Amount	Monthly Payment
MBR – Master Benefit Record	Master Title II File
MCS – Modernized Claims System	SSA System Title
MDI – Modernized Data Input	Title II Inputs
MDW – Modernized Development Worksheet	SSA Development Tool
MFQM – Master File Query Menu	Query Sub-Menu

MFQY – Master File Query	Title II/XVI Queries
MISM – Miscellaneous Menu	Master File Miscellaneous Queries
MSOM – Modernized Systems Operations Manual	SSA Procedures
MSS – Management Support Specialist	SSA Position Title
MSSICS – Modernized SSI Claims System	Computerized Title XVI Processing
NDNH – National Directory of New Hires, Wages and Unemployment	Outside Agency Computer Match
NH – Number Holder	SSN Recipient
NUMI – Numident	SSN Record
ODIO – Office of Disability and International Operations	SSA Central Office
PCACS – Processing Center Action Control System	Folder Tracking System
PHUS – Payment History Update System	Title II Annual Benefit Statements
PUPS – Prisoner Update System	Incarceration/Warrant Tracking System
RIB – Retirement and Insurance Benefits	Types of SSA Benefits
RP – Representative Payee	Recipient of Benefits for Another Main Menu Into the RPS
RPMM – Representative Payee Main Menu	Records Concerning Representative Payees
RPS – Representative Payee System	SSA Regional Facility
PSC – Program Service Center	SSA Program
RSDI – Retirement and Survivors Disability Insurance	SSA Program
RSI – Retirement and Survivors Insurance	Financial Institution Identifier
RTND – Routing Transit Number	SSA Procedure
RZ – Re-determination	Document Verification Program
SAVE – Systematic Alien Verification for Entitlements	Employee Identifier
SEID – SSA Employee Identification	Wage/EIN Information
SEQY – Summary Earnings Query	SSA Term Related to Disability
SGA – Significant Gainful Activity	SSA Position Title
SR – Service Representative	The Agency
SSA – Social Security Administration	Title II Claims <i>In Process of Approval</i> Program Administered by the SSA
SSACCS – SSA Claims Control System	Full Individual SSI Record Request
SSI – Supplemental Security Income	SSI Query Menu
SSID – SSI Display Query	Title XVI Beneficiary Information
SSQM – SSI queries	SSA Position Title
SSR – SSI Record	Activity Related to Disability Benefits
TE – Technical Expert	
TWP – Trial Work Period	

006.090 Program Operations Manual System (POMS)

POMS is the official instruction manual of the Social Security Administration. It is accessible by computer program, Intranet, CD, or in hard copy form. Before POMS, SSA's operating instructions were in more than 200 different manuals. POMS was created to better organize and centralize the Agency's operating instructions. It contains 12 Parts, 220 Chapters, 1,565 Subchapters and 26,822 Sections.

- A.** POMS is organized by subject matter, so all instructions on a particular topic are in one place. The organizational structure of POMS is as follows:

1. **Part** - the largest division. The parts are made up of important blocks of subject areas, such as Retirement and Survivors Insurance or Systems and Methods.
2. **Chapter** - topics within each Part.
3. **Subchapter** - the next lower division, which covers topics within each Chapter.
4. **Section** - the smallest level of division by topic (many Sections have further divisions within them, referred to as subsections, that are used to help make the topic more understandable).

The topics in POMS have been organized so that the information flows from the general to the specific, providing the broad background information first then leading into more specific details.

- B. POMS' Numbering System** - The most important thing to understand about using POMS is how the numbering system works. The following is a typical reference, and what it means:

“GN 00502.001”

1. **GN** = Part
2. **005** = Chapter
3. **02.** = Subchapter
4. **.001** = Section

Note that each Part has a two-letter abbreviation ("GN" stands for "General"). While the Parts also have numbers ("GN" is Part 2), the two-letter abbreviation is shown in every cross-reference in the POMS to identify the Part. Each Chapter has a three-digit number to identify it. The chapter number is the first three digits beginning on the left. Each Subchapter has a two-digit number. It appears in the middle, just to the left of the decimal point. Each Section has a three-digit number, which appears last, to the right of the decimal point. The numbers start over again with "one" at the beginning of each Part.

- C. Searching for Information.** There are four "tools" that are available for use in locating information on a particular subject or topic. They are:

1. **Table of Contents** - Each portion of POMS has its own Table of Contents. Because all subject area instructions are together in one place, this is the best place to begin a search for information. It is usually best to start with the larger topic designation (the Part) and work down to the appropriate Chapter and Subchapter.
2. **Index** - A comprehensive index is available for each Part. Like the Table of Contents, the indexes can direct the reader to the instructions relating to the topic he/she is looking for.
3. **Cross-references** - These appear within the instructions in POMS. They direct the reader to where related instructions may be found.
4. **"Running heads"** - This is a term used to describe the way in which the section numbers are shown at the top of each page. Note that the system that is used is the same as that found in a dictionary: the number at the top of the left-hand page shows which number comes first on

that page, and the number at the top of the right-hand page shows the number that comes last on that page. The purpose is to allow the reader to discover, at a glance, what the full section range is on the page(s) that are open.

006.100 **Modernized System Operations Manual (MSOM)**

Modernizing SSA's systems has involved many projects that provide SSA with increased computer support for all of its business processes and, as a beneficial byproduct, provide the OIG with much quicker access to SSA records. Changing over from a paper process to a largely on-line process has mandated that the operational process (including duties, workflow, and general office procedures) had to change. The operations procedures in the Modernized System Operations Manual (MSOM) integrate the manual actions that must be taken with the function the system performs. In the modernized system environment, it is not possible to separate manual procedures from "systems-related procedures." The modernized system consists of computer hardware and software that enables SSA employees to perform various operations by using computer screens rather than paper. MSOM is a "menu-driven" system that is intended to guide the user through a series of screens to an ultimate destination.

006.110 **Query Master**

- A.** Query Master is an invaluable tool for SAs seeking SSA Mainframe information. Query Master is a collection of tools for Mainframe queries. The Auto Queries function obtains single or multiple queries for one or more SSNs. The queries can be viewed, printed, or saved as a file. The Disclosure Query automatically presents a Master Benefit Record (MBR), an SSI Record (SSR) and a Numident (NUMI) in a logical, easy-to-read format—all on one screen. The Query Readers translate queries into English. Double-click on a particular line, and the POMS description for that line appears. The PHUS Query Reader decodes by line or by PHUS event.
1. After logging on to the SSA Mainframe, described below, start Query Master by clicking the QM button on the Tool Bar. It is located on the far right-hand side of the tool bar, and is pictured as a yellow lightning bolt. After accessing Query Master, a blank screen will appear, with a toolbar at the top of the page dedicated to QM functions.
 2. Enter a SSN into the provided space located in the upper left-hand corner of the QM. For single SSN requests, the Auto Queries screen will then appear. It displays the type of queries that can be requested using Query Master. For Multiple SSN requests, a screen used to select or create a list of SSNs will appear before the Auto Queries screen does.
- B.** Unless routed directly to a printer, queries requested using Query Master are displayed onscreen. Queries displayed onscreen can be decoded and/or printed. To decode a query, select a line and click on the Translate button, which is pictured as an open book on the toolbar. To use the PHUS Event Reader, click on the PHUS Events button, pictured as PHUS on the toolbar, then choose a "category" of events and click on "SEE EVENTS."

006.120 **Initial Access to the SSA Mainframe**

A. SSA Main Menu

1. Upon opening the SSA computer database, the first screen to appear is the “SSA Main Menu” (see [Exhibit 6-1](#)). Virtually all SSA-related queries will be accomplished by typing the letter “A” for “Primary” next to “SELECT THE DESIRED FUNCTION.”
2. Typing “K” will direct the user to the Training “region” of the database. Typing “1” and then “N1” will direct the user to the various screens leading to the opening of the OIG’s National Investigative Case Management System (NICMS).

B. SSA Production Screen

Immediately after entering the appropriate letter into the SSA Main Menu, the user is directed to the SSA Production Screen (see *Production*, [Exhibit 6-2](#)) for authorization to access the system.

1. The user must enter his/her six-digit Personal Identification Number (PIN), which OIG management obtains from SSA Systems Security, on the line labeled “PIN.” The user must then enter their personally created, alpha-numeric password on the line labeled “PASSWORD.”
2. A security feature built into the system requires the user to create and verify a new password every 30 days. The new password must not use a majority percentage of the letters and numbers used for passwords during the previous six months. If the system determines that the proposed new password is too similar to any of the previous six passwords, it will direct the user to create and verify another password.
3. **NOTE:** All MSOM procedures are sensitive internal operating instructions, which were specifically developed to assure the integrity of program administration. These instructions, if available to unauthorized persons, could be used to perform or subvert one or more internal Social Security functions. The result could be fraud, misuse or abuse of program funds and/or Agency records. Since the entire MSOM is sensitive material, members of the general public must not be given access to it. Do not place any MSOM material in any general-access areas, such as waiting/reception areas.

C. SSA Menu (Main)

Although having essentially the same name as the opening screen (SSA Main Menu), the SSA Menu (Main) (see [Exhibit 6-3](#)) is totally different from the aforementioned screen. Further, the SSA Menu (Main) is the key gateway through which access is gained to modernized systems screens, i.e., SSN, Title II, Title XVI and wage/employment information.

1. The SSA Menu (Main) offers 35 separate functions, six of which will provide virtually all of the *available* information requested by the OIG. The relevant functions are:
 - a. **#9: Master File Query** – Although this function cannot direct Special Agents to 100% of the information they need 100% of the time, the Master File Query Menu (*MFQM*, [Exhibit 6-4](#)) *does* serve as the doorway leading to *the most* information on the majority of individuals, entities, or SSNs (see MSOM Section 206-B).

- b. **#14: RSDHI Data Inputs** – This function is notable because it directs access to the Title II Menu (*T2SM*, [Exhibit 6-5](#)) through which SAs can electronically order copies of U.S. Treasury checks via the Photocopy Request sub-screen (see *PEPH*, [Exhibit 6-6](#)) (see MSOM Chapter 216).

NOTE: The PACER system, described in SAH Chapter 7 ([section 007.110](#)), is the primary method for obtaining copies of U.S. Treasury checks.

- c. **#20: DOORS – Detailed Office/Organization Resource System** - DOORS provides SSA field office (FO) information including directions, office hours, phone extensions, time zones and E-mail addresses. The highlighted areas in the DOORS Main Screen (see *DOORS*, [Exhibit 6-7](#)) equate to requesting information on DO 669, as an example. Information is obtained by entering either the DO code or the city and state of the DO. FOADDRESS (see [Exhibit 6-8](#)) displays the requested information (see MSOM Chapter 235).
- d. **#23: Representative Payee** – The Representative Payee System (RPS) searches for data in the Master Representative Payee File (MRPF), Master Beneficiary Record (MBR) and the Supplemental Security Record (SSR). It contains information about representative payees (RP) for Title II and Title XVI payments. It specifically includes current and prior RPs, RP applicants who are not selected, and those who cannot or should not be selected as RPs (e.g., individuals convicted of a felony against SSA).

Access to that information can be obtained either through the SSA Menu (Main), or through the Master File Query Screen (MFQY), discussed in detail in section 006.050. Using the SSA Menu (Main), and after #23 has been selected, the Representative Payee Main Menu will be generated (see *PMM*, [Exhibit 6-9](#)). Once on RPMM, select *mode* #3 (Query) and then *option* #7 (Query Response), and enter the appropriate SSN (or “Y” for unknown). Those actions bring up the Query Response Selection List (see *RQSL*, [Exhibit 6-10](#)). Complete the screen by selecting the type of representative payee needed (see MSOM Chapters 238, 242, 244 and 245).

- e. **#32: Continuing Disability Review (CDR) File** – This function provides information about active CDRs *not* initiated by SSA Field Offices. Section 221(i) of the Social Security Act, as amended, requires a periodic CDR to reassess disabled beneficiaries’ eligibility at least every three years except where a finding has been made that such disability is permanent. Reviews of cases involving permanent disability are made at such times as the Commissioner determines appropriate. Section 1614(a)(3) of the Act provides for periodic review of eligibility for Supplemental Security Income, based on disability or blindness. These reviews are either called CDRs or, in the case of the age-18 review, a re-determination. The Continuing Disability Review Control File (CDRCF) screens are designed to provide the user with the ability to query the status of current Continuing Disability Reviews (CDRs). This file houses data pertaining to beneficiaries for whom CDR data is present. To update or query a record, the CDR Selection Menu (MCDR) must be used (see MSOM Chapter 185 and POMS DI 13001.001).
1. Entering #32 into the SSA Menu (Main) screen brings up the CDR Selection Menu (see *MCDR*, [Exhibit 6-11](#)). Enter #1 for “Query,” then enter the SSN, which brings up the CDR Query Screen (see *QCDR*, [Exhibit 6-12](#)) containing the requested information.

2. The CDR Query Screen (QCDR) provides a historical record of all the events entered on the control file for a particular beneficiary/recipient. Each time an update is made, a new event is created. The previous transactions remain unchanged, thus maintaining a historical record of all transactions input to the CDRCF.
- f. **#33: Prison System/Fugitive Felons** - The Prisoner systems are used to record incarceration information, effectuate suspension actions for both Title II and Title XVI payments, control reports sent to SSA by incarceration facilities, and make incentive payments to facilities reporting incarceration information. The Prisoner systems consist of two databases. The Incarceration Report Control system (IRCS) controls reports received from incarceration facilities. The Prisoner Update Processing System (PUPS) records information on an individual inmate basis, and permits the user to effectuate a suspension of Title II or Title XVI payments (see MSOM Chapter 90).
1. Entering #33 into the SSA Menu (Main) screen brings up the Prison Systems/Fugitive Felons Sub-Screen (see *PFSM*, [Exhibit 6-13](#)). Enter “1” for “Prison Systems,” after which the screen will display the Prison Systems Menu (see *PSMU*, [Exhibit 6-14](#)).
 2. The PSMU makes reference to “Reporter” and “Facility”, defined as follows:
 - a. **Reporter** – In the Prisoner System, a reporter is a for-profit or non-profit organization which enters into an agreement with SSA to provide timely reports of confinement of individuals in correctional or mental institutions. A reporter may report for one or more facilities.

In the Fugitive Felons System, a reporter is a for-profit or non-profit organization which provides reports of fugitive felons from warrant agencies. A reporter may report for one or more warrant agencies. However, SSA makes reporting agreements with the warrant agencies, not the reporters themselves.
 - b. **Facility** – A facility is a correctional institution (as described below) or a public/private mental institution that maintains confined individuals. A facility provides confined individual information to a reporter who, in turn, submits the information to SSA for matching purposes. Note that in some instances, a Reporter and a Facility may be the same organization.
2. SSA’s modernized computer system is a “menu-driven” system, which guides its users from the general to the specific through a series of screens, menus and sub-menus. The SSA Menu (Main) is the principal screen to begin that process.

006.130 Master File Query

- A. The Master File Query Menu (see *MFQM*, [Exhibit 6-15](#)) is accessed by entering #9 into the SSA Menu (Main) screen (see MSOM Chapter 206). The MFQM is a sub-menu that is used to request Master File query responses directly from the MFQM, or by using the MFQM to select another query request screen or sub-menu. The three query responses that can be requested **directly** from the MFQM are:
1. an abbreviated Master Beneficiary Record (MBR), known as AACT;

2. a full MBR, known as FACT; and
3. Title II claims status, known as SSACCS.

NOTE: These three queries are *Title II queries only*, and are discussed in more detail in the following paragraphs.

- B.** The MBR is an electronic record of payment information for every RSDI (Title II) beneficiary. Data is maintained in four parts—account data, transaction data, black lung data and IMPACC data. The account data section contains current earnings and payment information for each beneficiary. The transaction data section contains detailed information for each transaction applied to the record since the last date of microfilming (see POMS SM 00510.000 and MSOM Section 24-D-2).
- C.** The Master File Query Menu (MFQM), as a whole, is a submenu that is able to produce 26 separate types of Title II and Title XVI Master File query responses, including the three Title II queries listed above.
1. Of the 26 available queries, 13 are of significant benefit to the OIG. They are:
 - a. **#1: AACT (Abbreviated MBR)** – An AACT (Abbreviated Account Query) provides basic beneficiary/representative payee information, and payment history information for **current** payments. It is obtained by entering #1 and the beneficiary’s SSN into the MFQM. An example is contained in [Exhibit 6-16](#) (see POMS DI 21005).
 - b. **#2: FACT (Full MBR)** – A FACT (Full Account Query) provides the same information as an AACT, plus a complete historical accounting of all payments made to the beneficiary.
 - c. **#5 – NUMI (Numident)** – The Numident is a query display of information taken from an individual's application for an original SSN card and subsequent applications for replacement cards. It is accessed by entering #5 and the SSN into the MFQM, after which a preparatory screen entitled “Numident Query Sensitive Information” appears (see [Exhibit 6-18](#)). Enter #1 to have the requested information displayed on the screen, after which the actual Numident will be displayed (see [Exhibit 6-19](#), POMS RM 00209.002, and MSOM Section 207-A-1).
 - d. **#6 – ALPH (Alphident)** – The Alpha-Index File (AIF) houses the identifying information of each SSN holder. That file is based on the Russell Soundex Coding System. The advantage of that system is the grouping together, in one code group, of all surnames which have the same basic consonant sounds. When an individual's SSN is not known, but identifying information is available, the Alpha-Index Query may be used to effect an electronic search of the AIF using a search key derived from the individual's identifying information, in an effort to locate possible SSNs, of which one may belong to the individual. The search key consists of the Soundex code equivalent of the individual's surname, the first four positions of the first name, and the century, year and month of birth (POMS RM 00209.005 and MSOM Section 207-B-1).

The ALPH (Alpha-Index Query) screen is obtained by entering #6 into the MFQM (see [Exhibit 6-20](#)). Enter the available information, after which the system will display the

names and SSNs of possible matches to the search criteria. When a name is then selected, the system will display the Numident that corresponds to the selected SSN.

- e. **#7 – DXQM (Data Exchange Query Menu)** – The Data Exchange Query Menu (see *DXQM*, [Exhibit 6-21](#)) is a sub-menu that provides access for users to query data provided by other agencies. The Office of Child Support Enforcement (OCSE) provides information to the SSA on newly hired individuals and quarterly wage and unemployment data. The DHS-Homeland Security Investigations provides SSA with a means to verify documents presented as evidence of lawful immigration status or work authority in the United States. In the future, military discharge data will be available from the Veterans Benefits Administration (VBAQ) (MSOM Section 207-S-1).

From the Master File Query Menu (MFQM), select the Data Exchange Query Menu (DXQM) by entering #7. From there you the following queries can be accessed:

1. **#1 – NDNH (New Hire, Qtr Wage, Unemployment)** – The NDNH query (see [Exhibit 6-22](#)) enables users to access information on newly hired individuals and quarterly wage and unemployment information. This query can also provide *real time* access to those SSNs that have a Supplemental Security Income (SSI) business relationship with SSA. On the menu and query screens, the SSN and UNIT data fields are pre-filled from the DXQM. The Date is systems generated. If the SSN entered on the DXQM is not found on the SSR Index, the user will not be taken to the NDNH screen, but will receive the error message "SSR DOES NOT EXIST AND NO MSSICS FILE" (see MSOM Section 207-O).
2. **#3 – SAVE (Non-Immigrant Information and Alien Status Verification)** – The Systematic Alien Verification for Entitlements (SAVE) program provides a method of document verification within an automated environment. This automated verification process is available to verify Citizenship and Immigration Services (CIS) documents presented as evidence of lawful immigration status or work authority in the United States (U.S.) when an alien applies for an SSN card, or applies for Retirement Survivors Insurance (RSI) or Supplemental Security Income (SSI) benefits (POMS RM 00203.040 and MSOM Section 207-U).

The SAVE screen display (see [Exhibit 6-23](#)) is the processing vehicle used to access the CIS database. When a valid number is entered in the Alien Number or Admission Number data field on the SAVE screen, the CIS system will be accessed. All other data fields on the SAVE screen will be propagated with data taken from the CIS Central Index System – Alien Status Verification Index (ASVI) database or Non Immigrant Information System (see *NIIS*, [Exhibit 6-24](#)). If an entry in the Alien Number or Admission Number field is not a valid number, the CIS system will recognize this invalid condition and will notify SSA with the displayed edit message "INVALID ENTRY."

NOTE: SSA's Security policy prohibits direct routing of query responses from external databases to printers. The only printing option available is individual screen printing.

- g. **#8 – SEQY (Summary Earnings)** – The Summary Earnings Query (see *SEQY*, [Exhibit 6-25](#)) is a query request screen that displays reported annual wage information for a

specified SSN (see *SEQR*, [Exhibit 6-26](#)) (POMS SM 00345.900, and MSOM Section 207-D-1).

- h. #9 – DEQY (Detail Earnings)** – The Detail Earnings Query (see *DEQY*, [Exhibit 6-27](#)) is an immediate response on-line query that displays requested earnings information and related data, including employer information. The data displayed on the DEQY printout (*DEQR*, [Exhibit 6-28](#)) is extracted from the Master Earnings File (MEF) and/or the Employer Identification File (EIF) (POMS SM 00344.001, RM 01455.010, and MSOM Section 207-E-1).
- i. #10 – SSQM (SSID, SSI2, SSI3 and SSI4)** – The Supplemental Security Income Query Menu (*SSQM*) (see [Exhibit 6-29](#)) provides access to four different types of queries related to the Supplemental Security Income Record (SSR) of individual beneficiaries. The SSQM is accessed by entering #10 and an SSN into the MFQM, after which one of the following queries must be selected (POMS SM 01601.175-.280 and MSOM Section 207-F):

 - 1. #1 – SSID (Complete Record Request)** – The SSID (see [Exhibit 6-30](#)) provides an online response containing the **complete** Supplemental Security Income Record Display (SSIRD). The SSI2, SSI3 and SSI4 are smaller variations of the SSID.
 - 2. #2 – SSI2 (Selective Record Request)** – The selective request is used to obtain information in groups of related fields or segments. Use the SSI2 when only limited information is required. EXAMPLE: If only an address (ADDR) and direct deposit data (DRDP) is needed, transmit an SSI2 request for those two segments instead of an SSID request.
 - 3. #3 – SSI3 (General SSI Query)** – The general query provides a combination of current essential information sufficient to answer a high percentage of general inquiries. Replies are limited to a one- or two-page response for each eligible person.
 - 4. #4 – SSI4 (Overpayment/Re-determination Query)** – This query has been designed to assist in the processing of re-determination and overpayment actions.
- j. #11 – PHUS (PHU1, PHU2, PHU3)** – On the basis of the 1983 Amendments, Social Security benefits became subject to Federal income tax. SSA is required to provide an annual benefit statement to each Title II beneficiary who receives payment and/or is credited with a refund in a calendar year. The Payment History Update System (PHUS) database was established to be the source of the annual benefit statement. It contains a historical record of Title II payment related actions starting with the year 1984 (POMS SM 00545.001, .245, and .500, and MSOM Section 207-G-1). The PHUS query screen (see [Exhibit 6-31](#)) is accessed by entering #11 and an SSN into the MFQM, after which one of the following selections must be made (POMS SM 00545.001 and MSOM Section 207):

 - 1. #1 – PHU1 (Payment History by BIC)** – This query provides a complete PHUS record of a *specific* beneficiary for *specific* tax year(s) (see [Exhibit 6-32](#)).
 - 2. #2 – PHU2 (Payment History)** – This query provides a complete PHUS record of an *entire account*, including every beneficiary, for specific tax year(s).

3. **#3 – PHU3 (Payment History by BIC List)** – This query identifies the beneficiary or beneficiaries who have payment-related activity on the MBR/PHUS for the requested year(s).
- k. **#16 – MISM (Miscellaneous Menu)** – The Miscellaneous Menu (*MISM*) (see [Exhibit 6-33](#)) is the sub-menu used to call up Master File miscellaneous requests, the most important of which to the OIG are routing transit numbers and employer identifiers (MSOM Section 209-A-1).
1. **#12 – RTND (Routing Transit Number)** – The Routing Transit Number screen (see *RTND*, [Exhibit 6-34](#)) is a data entry screen that is used to obtain identifiers regarding financial institutions. The information on the RTN database is centered on the Financial Organization Master File (FOMF) that is provided by the Department of the Treasury (TD). Each month, TD sends a complete replacement FOMF to SSA, which is used to update the RTN database. This file consists of all FI information (i.e., RTN, FI name and address, etc.) for both *active and inactive* RTNs in the nation. Enter the routing transit number into the RTND, after which the return screen will be displayed with the requested information (see *RTNI*, [Exhibit 6-35](#)).
 2. **#13 – AEQY (Alpha Access To EIF)** – The Alpha Access to the Employer Identification System allows users to electronically obtain an Employer Identification Number (EIN) when only the employer name, and possibly State or address is known (see [Exhibit 6-36](#)), or to obtain the EIN when only the employer name is known (see [Exhibit 6-36A](#)). Either query is designed to produce the employer’s name, address and EIN (see [Exhibit 6-37](#)) (MSOM Section 209-N).
- l. **#18 – CNQY (Consolidated)** – The Consolidated Query Screen (*CNQY*) (see [Exhibit 6-38](#)) contains an options checklist of possible queries used in the initial claims process. Enter an SSN one time and indicate which queries are desired. One transaction will generate all requested queries (MSOM Section 206-C-1).

NOTE: Queries **cannot** be brought to the screen using CNQY. **All** queries will be sent to the printer previously designated for your terminal. You may select online or offline queries. Place a “Y” in the ONLINE (Y/N) field if you want to receive your queries immediately. Offline queries will be generated either later in the day, or the next day, if this field is left blank or an “N” is entered.

- m. **#19 – RPQY (Representative Payee)** – The Representative Payee System (RPS) contains information about representative payees (RP), and Title II/Title XVI beneficiaries/ recipients who have RPs. This includes current and prior RPs, RP applicants who are not selected, and those who cannot or should not be selected as RPs (e.g., individuals convicted of a felony against SSA). That information is stored on the Master Representative Payee File (MRPF), which has three types of records. Those records contain data about:
1. applicants, both approved and denied;
 2. beneficiaries who have RPs; and
 3. the relationship between the two.

Information on the MRPF for individual RPs is entered and retrieved using the RP's own Social Security number (RPSSN).

Information about an organizational RP is stored and retrieved via a system that is unique to RPS. Since usually no identifying number exists, such as an SSN, the information is stored using the ZIP code of the business address of the organization. When a ZIP Code is entered instead of an SSN, RPS displays a list of all organizations within that ZIP Code that are on the MRPF. Choose the appropriate organization from the list.

Specific information about beneficiaries/recipients is retrieved using the person's own SSN. For the relationship between RPs and beneficiaries/recipients, RPS has the capability to link an RP with all beneficiaries/recipients being served, and to link the beneficiary/recipient with current and former RPs. This applies, however, only to those who have been entered into the MRPF.

Access is gained to the information by entering the SSN of either the beneficiary or the RP, and the type of requested response onto the RP Query Response Selection List (see *RQSL*, [Exhibit 6-39](#)) which is obtained by entering #19 on the MFQM (MSOM Section 238).

- n. **#20 – PCACS (Case Control Query)** – The Processing Center Action Control System (PCACS) was created for the Program Service Centers (PSC) to control the three things that make up their workloads: folders, paper, and diaries. PCACS also identifies the kind of folder, action, or diary; and tells *where the item is* and how long it has been there (MSOM Chapter 1601).

PCACS has two queries that give information in varying degrees of detail. They are:

1. **Standard Query** – The Standard Query screen (see *SQRY*, [Exhibit 6-40A](#)) is accessed by entering #20 into the MFQM, and then entering an SSN into the SRQY. A new screen with the requested response does not appear. Instead, the response is added in a segment to the original request screen (see [Exhibit 6-40B](#)). It lists all of the actions, folders and diaries for an SSN that are being controlled by PCACS.
2. **Full Queries** – Once on the Standard Query and response, the viewer has the option of selecting a Full Query for a folder or action if he/she decides that he/she needs more information. If an “X” is entered into the space on the left-hand side of the SSN in the response section of the query, the system will produce a more detailed explanation of the folder’s past and present location (see *FQY1*, [Exhibit 6-41](#)).

- o. **#21 IBIQ (Interstate Benefit Inquiry Query)** –The IBIA is an online link SSA developed to be used to obtain wage and unemployment information from participating state workforce agencies to SSA. The primary purpose of this online link is to establish a verification of eligibility and/or payment amounts under certain benefit programs administered by SSA.

The link is available through the SSA Main Menu, Option 9, Master File Query. Select function number 7, Data Exchange Query Menu (DXQM), include the SSN. From the DXQM, select Option 6 - IBIQ T-11 DIB (DOL ICON NETWORK) Unemployment Insurance or Option 7 - IBIQ T-XVI (DOL ICON NETWORK) Unemployment Insurance. The SSN is propagated from the DXQM screen.

After Option 6 or 7 is selected, the SSN is prefilled from the DXQM. You may enter the abbreviations of up to five states for which you would like to receive claim and/or wage data.

006.140 SS-5 Requests

A. A completed and signed Form SS-5 (Application for a Social Security Card) or system-generated application is required to obtain:

1. an original SSN;
2. a new (different) SSN;
3. a duplicate SSN card (same name and SSN); or
4. a corrected SSN card (new name but the same SSN).

A completed and signed SS-5 is also required to:

1. correct information on the electronic record even though a replacement card may not be issued;
2. correct and re-enter an Enumeration at Birth (EAB) exception;
3. issue a replacement card when the name on the card was misspelled, garbled, or incomplete due to an FO keying error or computer malfunction in the card printing process; or
4. issue a replacement card when the applicant alleges non-receipt.

B. The paper SS-5 is used when the applicant wants to apply for an SSN card through the mail, in person at an SSA FO, or an SSA card center. A paper copy of the SS-5 can also be obtained from the Internet. SSA processes the SS-5 via the Social Security Number Application Process (SSNAP). The applicant attests to the application as the MES Interview Mode is no longer utilized.

C. Photocopies of SS-5 forms can be obtained from the Security Records Center (SRC) in Boyers, Pennsylvania (Boyers) for those applications completed/processed prior to SSNAP. Those applications processed through SSNAP records can be found via SSNAP's link located under I-MAIN Production at the following link: <http://otsodiet.ssahost.ba.ssa.gov/ssawebapps.htm>

Boyers processes requests that are received via the SS-5 Reprints online application process and EARS as the SRC no longer accepts fax or email.

1. SS-5 Reprints Application Instructions (preferred method)

Prior to accessing the site, you should have the Numident available for the record(s) you are requesting.

The website address is: (b) (7)(E) This will take you directly to the SS-5 Reprints Homepage. The system automatically recognizes your pin and worksite address information. Authorized users are then able to submit requests. If you are not identified as an authorized user, you are instructed to contact the Office of Central Operations (OCO) Help Desk via the email link provided, to request user authorization.

Either a “certified” or a “non-certified” SS-5 can be requested. There is no limit to the number of requests that can be submitted, however, each SSN requires a separate submission. Certified copies are automatically sent by Federal Express Mail Service (FedEx) and should be received the following day. When requesting the non-certified copies, the user can choose their response method by selecting e-mail (which is sent directly to the requester with a scanned copy of the SS-5 attached), U.S. mail, or FedEx.

By default, the “Date Needed By” is two weeks from the current request date. By checking “Urgent,” the turnaround for requests is approximately one business day.

(Note: The SS-5 Reprints Homepage has a link for “User Manuals.” The second option under “User Manuals” contains the *OIG Users Instructions*. These instructions provide the systematic process for OIG.)

2. Submitting EARS requests through SSNAP

Submit requests for completed SSN applications and records via EARS (see the SSNAP User Guide for instructions). To access EARS, click the EARS link in the left navigation menu within SSNAP. Make a request using the SSN or reference number (RFN).

Once retrieved, you can view and print completed SSN applications and records for 30 days. Applications and records with a CYD of less than 45 days from the current date are available immediately. Those with a CYD of more than 45 days from the current date are available the next business day.

006.150 DECOR or EDCOR “No Match” Letters

- A.** As an integral part of SSA's verification process for notifying the employee and employer that discrepancies exist with name/SSN combinations submitted to the IRS in employer wage (W-2) reports, SSA issues two types of letters.
- 1.** DECOR (decentralized correspondence) - notifies the employee of the discrepancy and offers an opportunity to correct the problem by visiting a local SSA office.
 - 2.** EDCOR (educational correspondence) - notifies the employer of numerous discrepancies attributed to the reporting entity. SSA uses the employer address reported on the W-2 and the Employer Identification Number (EIN) to mail EDCOR letters. At present, SSA software limits the total number of SSNs listed in each EDCOR letter to 500, even if a company may be responsible for submitting thousands of discrepant wage reports.
- B.** DECOR and EDCOR letters, also known as “no match letters,” are considered tax return information, the disclosure of which is strictly limited by the Internal Revenue Code.
- 1.** No disclosure of such information may be made except as permitted under 26 U.S.C. § 6103.

2. Disclosure of these letters by OI personnel must comport with guidelines found in the Special Agent Handbook (SAH), Chapter 6, Section 006.015. According to this section, SSA OIG may disclose tax return information from its files only to the Department of Justice and only if the disclosure is for the purpose of administering the Social Security Act. In simpler terms, DECOR and EDCOR letters must be contained in a formal OIG investigative file, and should be disclosed to an AUSA only if the AUSA is considering Social Security-related charges (i.e., SSN misuse, SSA program fraud, etc) for prosecution.

3. (b) (7)(E)

4. Any questions regarding specific situations encountered in the field regarding disclosure of tax return information should be vetted through the field division chain of command to the appropriated CID desk officer, who will obtain an OCIG opinion.

C. Information on obtaining EDCOR or DECOR letters - previously EDCOR letters were obtained through requests to the appropriate SSA component, now special agents and criminal research specialists have direct access to the request screens. Step by step instructions on how to access the letters through the SSA Mainframe, as well as examples of DECOR and EDCOR letters is located in the Employee Resource Center - Investigative/Legal Tools-Viewing and Printing Educational Correspondence Letters. Contact your CID desk officer if don't have access.

1. Requests to SSA for EDCOR or DECOR letters will be referred back to the requestor.

2. In cases where the correspondence must be certified for presentation in court proceedings, SSA will provide certification and witnesses.

006.160 Policy for the Transportation of Personally Identifiable Information Outside of OIG Secure Space

A. The Office of the Chief Information Officer (OCIO) provided guidelines to be followed by all Social Security Administration (SSA) personnel regarding safeguarding Personally Identifiable Information (PII) while in transit or outside of secure SSA space.


B. The procedures require prior supervisory approval for the removal of PII from the workplace. The procedures also require that a log be established to record the removal of PII from the employee's duty station. Because of the nature of the Office of Investigations (OI) business, it would be a laborious process to maintain a log to record the removal of PII from OI secured space. However, in order to comply with SSA's procedures the following policy will be adopted immediately.

C. This policy serves as the approval for the removal and transportation from OI secured space of all PII deemed necessary for investigative or other purposes.

1. The National Investigative Case Management System (NICMS) will serve as the official log for all OI files that contain PII.

2. In the case of paper documents, only working copies of items containing PII may be transported from OI secured space. All original documents should remain in the official case file.
3. Claims folders and other relevant PII documents removed from SSA Offices will be governed by SSA policy. An OI employee may be required to complete the log file maintained at the SSA office. However, the OI employee is subject to the OI policy for reporting the loss of PII.
4. Supervisors are directed to provide a copy of SSA's *Annual Reminder on Safeguarding Personally Identifiable Information for SSA Employees* to each of their employees. Both the supervisor and the employee should sign the corresponding "Acknowledgment Statement" indicating that the employee has read the annual reminder. Once signed, the original "Acknowledgment Statement" will be filed in the employee's SF-7B Extension File and a copy of the signed form is provided to the employee. This is an annual certification requirement and is generally completed at the time appraisals and performance plans are distributed.
5. Should PII become lost or stolen, agents/personnel will contact the Assistant Inspector General for Investigations (AIGI) via telephone within one hour of discovering the loss. Failure to do so may result in disciplinary action.

D. Transporting files, documents or electronic devices containing PII

1. You must make every reasonable effort to secure PII and electronic devices (e.g., computers, laptops and flash drives) during transport and at your destination.
2. You must not leave PII or electronic devices out of your control while transporting them. (This requirement may be subject to Transportation Security Administration regulations when traveling by air.)
3. SSA's e-mail system is encrypted and the Agency has implemented a secure method to send e-mails to Centers for Medicare & Medicaid Services (CMS).
4. (b) (7)(E)

5. You must use approved SSA encrypted or password-protected electronic devices (e.g., computers, laptops and flash drives).

Chapter 6 — EXHIBITS

Exhibit 6-0	—	Payment Extracts
Exhibit 6-1	—	SSA Main Menu (VTAM)
Exhibit 6-2	—	SSA Production (Production)
Exhibit 6-3	—	SSA Menu (Main)
Exhibit 6-4	—	Master File Query Menu (MFQM)
Exhibit 6-5	—	Title II Menu (T2SM)
Exhibit 6-6	—	Photocopy Request (PEPH)
Exhibit 6-7	—	Detailed Office/Organization System (DOORS)
Exhibit 6-8	—	Field Office Address and Phone Numbers (FOADDRESS)
Exhibit 6-9	—	Representative Payee Main Menu (RPMM)
Exhibit 6-10	—	RP Query Response Selection List (RQSL)
Exhibit 6-11	—	CDR Selection Menu (MCDR)
Exhibit 6-12	—	CDR Query Screen (QCDR)
Exhibit 6-13	—	Prison Systems/Fugitive Felons (PFSM)
Exhibit 6-14	—	Prison Systems Menu (PSMU)
Exhibit 6-15	—	Master File Query Menu (MFQM)
Exhibit 6-16	—	Abbreviated Account Query (AACT)
Exhibit 6-17	—	SSA Claims Control System query (SSACCS)
Exhibit 6-18	—	Numident Query Sensitive Information (NUMI)
Exhibit 6-19	—	Numident (NUMI)
Exhibit 6-20	—	Alpha-Index Query (ALPH)
Exhibit 6-21	—	Data Exchange Query Menu (DXQM)
Exhibit 6-22	—	National Directory New Hire, Wage & Unemployment Menu (NDNH)

[Exhibit 6-23 — Systematic Alien Verification for Entitlement \(SAVE\)](#)

[Exhibit 6-24 — Non-Immigrant Information and Alien Status Verification Display \(NIIS\)](#)

[Exhibit 6-25 — Summary Earnings Query \(SEQY\)](#)

[Exhibit 6-26 — Summary Earnings Report \(SEQR\)](#)

[Exhibit 6-27 — Detail Earnings Query \(DEQY\)](#)

[Exhibit 6-28 — Detail Earnings report \(DEQR\)](#)

[Exhibit 6-29 — Supplemental Security Income Queries \(SSQM\)](#)

[Exhibit 6-30 — SSI Complete Record \(SSID\)](#)

[Exhibit 6-31 — Payment History Update System Queries \(PHUS\)](#)

[Exhibit 6-32 — Payment History by BIC \(PHU1\)](#)

[Exhibit 6-33 — Miscellaneous Menu \(MISM\)](#)

[Exhibit 6-34 — Routing Transit Number \(RTND\)](#)

[Exhibit 6-35 — Final Financial Institution Listing \(RTN1\)](#)

[Exhibit 6-36 — EIF Access by Name \(AEQY\)](#)

[Exhibit 6-36A — EIF Access by EIN \(AEQY\)](#)

[Exhibit 6-37 — EIF Response to Query \(AEQY\)](#)

[Exhibit 6-38 — Consolidated Query \(CNQY\)](#)

[Exhibit 6-39 — RP Query Response Selection List \(RQSL\)](#)

[Exhibit 6-40A — Standard Query \(SQRY\)](#)

[Exhibit 6-40B — Standard Query & Reply \(SQRY\)](#)

[Exhibit 6-41 — Folder Query \(FOY1\)](#)

[Exhibit 6-44 — SSA Consent for Release of Information](#)

[Exhibit 6-45 — Request for Testimony and/or Information/Records](#)

Exhibit 6-0

Office of the Inspector General
Office of Investigations
Social Security Administration

Date:

To: _____

From: _____

Subject: Request for:_____

Re: SSA OIG OI File Number (SSN)_____

Certified Extract – Scheduled court date (if known).

In conjunction with an official investigation being conducted by this office, this is a request for (if requesting payment extract, provide period of time covered):

Please forward the documents identified above to

at the following address:

no later than (date)

Requester phone number:

SOCIAL SECURITY
Office of the Inspector General

FOR PROBLEM ASSISTANCE CALL (b) (7)(E) TERMID: VC271100

SSA MAIN MENU

- | | |
|------------------------|-----------------------------|
| A. PRIMARY | K. TRAINING |
| B. ALTERNATE | M. SECURITY ADMINISTRATION |
| C. LAN ALTERNATE 3 | N. EVENT MANAGEMENT SYSTEM |
| D. LAN ALTERNATE 4 | O. PC NOTICE PROCESSING |
| F. FPPS | P. TSC NOTICE PROCESSING |
| I. EMERGENCY NETSTAT | T. TIME & ATTENDANCE SYSTEM |
| J. NETWORK STATUS MENU | 1. MANAGEMENT INFORMATION |
| | SERVICES FACILITY/PROD |
| | REGION MENU |

SELECT THE DESIRED FUNCTION : A

SOCIAL SECURITY
Office of the Inspector General

C
I
P
C
M
T
B

W E L C O M E T O T H E F U T U R E
CIGN

```

          SSSSSSSSSSSS      SSSSSSSSSSSS      AAAAAAAAAAAAAA
        SSSSSSSSSSSSSSSS    SSSSSSSSSSSSSSSS    AAAAAAAAAAAAAAAA
      SSSSS      SSSSSS    SSSSSS      SSSSSS    AAAAA      AAAAA
    SSSS      SSSSSSSSSSSS    SSSS      SSSSSS    AAAAA      AAAAA
  SSSSSSSSSSSSSSSS    SSSSSSSSSSSSSS    AAAAAAAAAAAAAAAA
        SSSS      SSSS      AAAAA      AAAAA
  SSSSS      SSSSSS    SSSSS      SSSSSS    AAAAA      AAAAA
SSSSSSSSSSSSSSSSS    SSSSSSSSSSSSSS    AAAAA      AAAAA
  \ \
  SSSSSSSSSSSS      SSSSSSSSSS      AAAAA      AAAAA
  \ \ \
  |||
  |||
  >>>>>

  \ \ \ \
  \ \

```

WELCOME TO THE PRODUCTION REGION CICS/TRANSACTION SERVER VER. 1.3.0
 PIN : XXXXXX *****W A R N I N G*****
 G***** USE OF THIS SYSTEM IS
 MONITORED AND RECORDED. UNAUTHORIZED USE OR DISCLOSURE OF
 PASSWORD : XXXXXX INFORMATION IS
 STRICTLY PROHIBITED. PENALTIES INCLUDE
 REPRIMAND,
 NEW PASSWORD: SUSPENSION/TERMINATION OF EMPLOYMENT AND/OR
 VERIFICATION : CRIMINAL PROSECUTION.

SOCIAL SECURITY
Office of the Inspector General

SSA MENU

MAIN

SELECT THE DESIRED FUNCTION: _____

- | | |
|---------------------------------|-----------------------------------|
| 1. TITLE II/INITIAL CLAIMS | 19. CPS DATA INPUTS/QUERIES |
| 2. TITLE II/PE | 20. DOORS |
| 3. TITLE XVI/IC CLAIMS AND PE | 21. RRB DATA INPUTS |
| 4. SHARED PROCESSES | 22. ALTERNATE MODE FACILITY |
| 5. ENUMERATION | 23. REPRESENTATIVE PAYEE |
| 6. DEBT MANAGEMENT | 24. MODERNIZED DEVELOPMENT |
| WORKSHEET | |
| 7. TITLE II/INTERACTIVE COMPS | 25. WMS LISTINGS |
| 8. TITLE XVI/INTERACTIVE COMPS | 26. PC ACTION CONTROL SYSTEM |
| 9. MASTER FILE QUERY | 27. PAYMENTS OUTSIDE TITLE II |
| SYSTEM | |
| 10. MACADE | 28. DRUG ADDICTION AND ALCOHOLISM |
| 11. APPOINTMENT/REFERRAL/LEADS | 29. ACC&SS |
| 12. EARNINGS MODERNIZATION | 30. COMMON TICKLE |
| 13. INTEGRITY REVIEW | 31. ONLINE NOTICE RETRIEVAL |
| 14. RSDHI DATA INPUTS | 32. CONTINUING DISABILITY REVIEW |
| FILE | |
| 15. SSI DATA INPUTS | 33. PRISON SYSTEM/FUGITIVE FELONS |
| 16. ADMINISTRATIVE APPLICATIONS | 34. NETWORK STATUS |
| 17. OHA DATA INPUTS/QUERIES | 35. UNVERIFIED PRISONER SYSTEM |
| 18. NDDSS MASTER FILE MENU | 99. RETURN |
-

Exhibit 6-5

SOCIAL SECURITY
Office of the Inspector General

DIP
T2SM

TITLE II MENU

FIELD OFFICE: T12

UNIT:

xxxxxx

SELECT THE DESIRED FUNCTION: 13

- | | |
|-----------------------------|----------------------|
| 1=**** (FUTURE USE) | 15=**** (FUTURE USE) |
| 2=**** (FUTURE USE) | 16=**** (FUTURE USE) |
| 3=**** (FUTURE USE) | 17=**** (FUTURE USE) |
| 4=**** (FUTURE USE) | 18=**** (FUTURE USE) |
| 5=**** (FUTURE USE) | 19=**** (FUTURE USE) |
| 6=**** (FUTURE USE) | 20=**** (FUTURE USE) |
| 7=**** (FUTURE USE) | 21=**** (FUTURE USE) |
| 8=**** (FUTURE USE) | 22=**** (FUTURE USE) |
| 9=**** (FUTURE USE) | 23=**** (FUTURE USE) |
| 10=**** (FUTURE USE) | 24=**** (FUTURE USE) |
| 11=**** (FUTURE USE) | 25=**** (FUTURE USE) |
| 12=**** (FUTURE USE) | 26=**** (FUTURE USE) |
| 13=PEPH (PHOTOCOPY REQUEST) | 27=**** (FUTURE USE) |
| 14=PESP (STOP PAYMENT) | 28=**** (FUTURE USE) |

FOR EDIT CORRECTION, ENTER SSN:
OPTIONAL ENTRY - MESSAGE NUMBER:

SOCIAL SECURITY
Office of the Inspector General

DIP
PEPH

PHOTOCOPY REQUEST

TRANSFER TO:
XXXXXX

UNIT:

CONTACT METHOD: 1=PHONE 2=VISIT 3=MAIL 4=SYSTEM

ROUTE RESPONSE TO: 1=SCREEN 2=PRINTER

CAN: _____ BIC: _____ BN: _____, OFFICE CODE: _____

PAYMENT TYPE: PAYMENT AMOUNT:

(1=RECURRING 2=PMA 3=CMA 5=A- 9=COURTESY DISBURSEMENT)

SPECIAL ACTION CODE: _____

(O=OVERRIDE B=BLACK LUNG R=REP PAYEE E=EXCESS F=FOREIGN)

REGIONAL FINANCE CENTER: _____

(P=PHILADELPHIA,S=SAN FRANCISCO,K=KANSAS CITY)

SPECIAL PAYMENT DATA: _____

MONTH OF PAYMENT: _____

PHOTOCOPY TYPE: _____

(K=REGULAR L=CERTIFIED M=STATUS)

LEGEND: _____

ADDRESS: _____, _____

_____, _____

ZIP: _____

REMARKS:

SOCIAL SECURITY
Office of the Inspector General

DOORS DETAILED OFFICE/ORGANIZATION RESOURCE SYSTEM
DOORSMAINMENU

- | | |
|---|-------------------|
| 1. FIELD OFFICE INFORMATION/LOCATOR | 6. ALL OFFICES |
| 2. PROCESSING CENTERS (PC) | 7. CLOSED OFFICES |
| 3. TELESERVICE CENTERS (TSC) | 8. HARDWARE |
| 4. REGIONAL OFC/AREA OFC/DDS/ODAR/OTHER | |
| 5. FOREIGN SERVICE POSTS (FSP) | |

SELECT DESIRED FUNCTION: 1

--AND/OR--

ENTER ONE OR MORE IDENTIFIERS (OPTIONAL)

FUNCTION NOT REQUIRED-- FUNCTION REQUIRED--

OFFICE CODE: 669 CITY:

(STATE

PC NUMBER: STATE:

REQUIRED)

SSN: ZIP CODE:

FSP CONSUL CODE: REGION:

FSP COUNTRY:

RING NUMBER:

NETNAME:

ROUTE RESPONSE TO: 1 (1. SCREEN 2. PRINTER) UNIT: XXX

PF1-HELP PF6-CLR

SOCIAL SECURITY
Office of the Inspector General

DOORS FIELD OFFICE ADDRESSES AND PHONE NUMBERS FOADDRESS

OFFICE CODE: 669 NAME: MIAMI NORTH FL LEVEL: 1
OPEN: 10/14/1936 CLOSE: / / REOPEN: / /

LOCATION-

SOCIAL SECURITY
BUILDING/SUITE: LINCOLN SQ OFC CTR
STREET ADDRESS: 18475 NW 2ND AVE
CITY: MIAMI
ST/ZIP: FL 33169 -

MAILING-

SOCIAL SECURITY
LINCOLN SQ OFC CTR
18475 NW 2ND AVE
CITY: MIAMI
ST/ZIP: FL 33169 -

EMAIL: |FL FO MIAMI NORTH

PHONE NUMBERS EXT

BUSINESS: 305 652 4339
ADMINISTRATIVE: 305 655 0835
TITLE 2: 305 652 4339
TITLE 16: 305 652 4339
TTY: 305 655 2987

FAX NUMBERS

305 652 4637
305 652 4637
305 652 4637
305 652 4637

RMRKS:

PF1-HELP PF3-MAIN MENU PF4-SUB MENU PF6-CLR PF8-HOURS

SOCIAL SECURITY
Office of the Inspector General

RPAY REPRESENTATIVE PAYEE MAIN MENU

RPMM

OFFICE CODE: XXX

UNIT:

XXX

SELECT THE DESIRED MODE: 1

1. ESTABLISH

2. UPDATE

3. QUERY

SELECT THE DESIRED PROCESS: 7

01. REP PAYEE APPLICATION

09. INSTITUTION

02. SELECT REP PAYEE

10. SSN CORRECTION

03. DEVELOPMENT WORKSHEET

11. GENERAL MESSAGE

04. CASE MOVEMENT

12. NOTICES

PRINT/REPRINT

05. WMS FUNCTION

13. UPDATE SELECTION

ADDRESS

06. ACCOUNTING

14. QUESTIONNAIRE

07. QUERY RESPONSE

15. RPS INFORMATION

08/23/99

08. PE EVENT

16. MANAGEMENT

APPROVAL

APPLICANT/REP PAYEE SSN: XXXXXXXXXX
XXXXXXXXXX

BENEFICIARY/RECIPIENT SSN:

OR UNKNOWN (Y/N): N

APPLICANT/REP PAYEE LOCATION ZIP: _____

SOCIAL SECURITY
Office of the Inspector General

RPAY
RQSL

RP QUERY RESPONSE SELECTION LIST

UNIT:XXXXXX

APPLICANT/REP PAYEE SSN: XXXXXXXXXX

APPLICANT/REP PAYEE LOCATION ZIP: _____

BENEFICIARY/RECIPIENT SSN: XXXXXXXXXX OR UNKNOWN (Y/N): Y

QUERY RESPONSE(S) SELECTION(S):

1. RP SCREENING QUERY RESPONSE
2. RP FULL QUERY RESPONSE
3. INDIVIDUAL BENEFICIARY/RECIPIENT QUERY RESPONSE

(SELECTIONS 1, 2, AND 3 WILL ALWAYS BE RETURNED TO THE SCREEN)

4. INDIVIDUAL RP BENEFICIARY/RECIPIENT LIST (RPBL)
5. ORGANIZATION/INSTITUTION RP BENEFICIARY/RECIPIENT LIST (OIBL)

Exhibit 6-11

SOCIAL SECURITY
Office of the Inspector General

CDRMS
MCDR

CDR SELECTION MENU

OFFICE: XXX

SELECT: XX

1=QUERY
2=FO UPDATE
3=PC UPDATE
4=DQB/DDS UPDATE
5=REMARKS UPDATE
6=ADR SELECTION
7=TWP ACTIVITY
8=ESTABLISH CDR

9=DEVELOPMENT WORKSHEET
10=OFFICE ACTIONS
11=TICKET TO WORK
12=QUERY EARNINGS
13=VERIFY EARNINGS
14=EMPLOYMENT NETWORK
15=FUTURE USE

SSN: XXXXXXXXXX

BIC:

EARNINGS BEGINNING (MMCCYY): XXXXXX
(MANDATORY FOR 12-13)

Exhibit 6-13

SOCIAL SECURITY
Office of the Inspector General

PRSN/FRATS

PRISON SYSTEMS/FUGITIVE FELONS
SUB-MENU

PFSM

SELECT FUNCTION: X

- 1.PRISON SYSTEMS(PUPS AND IRCS)
 - 2.FUGITIVE FELONS SYSTEM(FRATS)
-
-

SOCIAL SECURITY
Office of the Inspector General

PRSN PRISON SYSTEMS MENU
PSMU

FIELD OFFICE: XXX

SELECT MODE: ____ 1. ESTABLISH 2. UPDATE 3. QUERY 4. CO USE
ONLY

SELECT FUNCTION: XX

1. PRISONER - BENEFICIARY/RECIPIENT SSN: XXXXXXXXXX
2. REPORTER
3. FACILITY
4. REPORTER AND FACILITY
5. REPORTER ID BY STATE
6. FACILITY ID BY STATE
7. REPORTER AND FACILITY ID BY STATE

REPORTER ID CODE: ____ FACILITY ID NUMBER: _____ STATE: _____

—

ESTABLISH MODE - SELECTION 3 ENTER REPORTER ID CODE
SELECTION 4 ENTER STATE

UPDATE/QUERY MODE - SELECTION 2 ENTER REPORTER ID CODE
SELECTION 3 ENTER FACILITY ID NUMBER
SELECTION 4 ENTER REPORTER ID CODE AND FACILITY ID
NUMBER

QUERY MODE - SELECTION 5, 6, 7 ENTER STATE

SOCIAL SECURITY
Office of the Inspector General

QRY MASTER FILE QUERY MENU

MFQM

TRANSFER TO: _____
XXXXXX

FIELD OFFICE: XXX

UNIT:

SELECT ONE OF THE FOLLOWING: XX

- | | |
|-----------------------------------|--------------------------------|
| 1=AACT (ABBREVIATED MBR) | 13=1099 (BENEFIT STATEMENT) |
| 2=FACT (FULL MBR) | 14=TPQY (THIRD PARTY) |
| 3=SSACCS (CLAIMS CONTROL) | 15=DEQM (DELAYED QUERY MENU) |
| 4=THIS (TRANSACTION HISTORY) | 16=MISM (MISCELLANEOUS MENU) |
| 5=NUMI (NUMIDENT) | 17=QRSL (INQUIRY RESPONSE) |
| 6=ALPH (ALPHIDENT) | 18=CNQY (CONSOLIDATED) |
| 7=DXQM (DATA EXCHANGE QUERY MENU) | 19=RPQY (REPRESENTATIVE PAYEE) |
| 8=SEQY (SUMMARY EARNINGS) | 20=PCACS (CASE CONTROL QUERY) |
| 9=DEQY (DETAIL EARNINGS) | 21=HCFA (HI/SMI) |
| 10=SSQM (SSID,SSI2,SSI3,SSI4) | 22=PBRQ (PEBES ONLINE) |
| RECORD) | 23=ICERS (INFO/CERT EARNINGS |
| 11=PHUS (PHU1,PHU2,PHU3) | 24=PBHQ (STATEMENT HISTORY) |
| 12=PHU4 (TAXATION INQUIRY) | 25=WC/PDB OFFSET DATASHEET |

SOCIAL SECURITY NUMBER: XXXXXXXXX

(SSN OPTIONAL FOR 9, 20, 23)

ROUTE RESPONSE TO / RETURN TO (SELECT ONE): 1 (MANDATORY FOR 1-3)

1=SCREEN 2=PRINTER/MAIN 3=PRINTER

BENEFICIARY ID CODE (BIC): ____ (OPT FOR 1-2, 17, 21) REDIRECT (N): ____ (OPT 17)

SOCIAL SECURITY
Office of the Inspector General

AACT DTE:06/17/02 SSN: BIC: DOC: UNIT: PG: 001+
STATUS MBR YES LOU-06/17 DATA FILES YES LOU-06/17 SSACCS NO LOU-06/14
CPS NO
ACCOUNT PCOC-7 QCE-25 QCR-13 SP-F CIS-NS TAC-D RCC-5 ERC-95 CDY-0
PMT CYC CYI-1 PCEFD-06/15/1996 PCCOM-06/96 PCCR-S
PRIMARY DOB-11/09/1960 LSPA-\$0.00
PIA HIS 12/00 \$ 318.40 L K FMAX-\$ 318.40D
07/01 \$ 318.70 L K FMAX-\$ 318.70D
12/01 \$ 326.90 L K FMAX-\$ 326.90D
PAYMENT PIC-A MPA-\$326.00 DOC-C52 SCC-26290 RD-02/07/02 LAP-# PSC-C
TELE NO BTC1-N CPND-03/01
PAYEE
ADDRESS
BANK RTN-021031207 DAN- BDCD-09/14/00 SRCD-E
BENEFIT BIC-A SB-F DOB-11/09/1960 B DOEC-11/95 ABN-314C
LAF-C MBP-\$326.00 DRD-09/14/00 DOEI-11/95 DOF-10/96 SAC-D ENAC-C
LANG-E RDD-090
MED BILLING-3RD PTY

HI CONTS PRD-11/1997 SMI CONTS PRD-11/1997

HI-DIB START-11/1997 BASIS-DISABILITY TYPE-FREE FILING-10/1997

AACT DTE:06/17/02 SSN: BIC: DOC: UNIT: PG: 002+

SMI-DIB START-11/1997 BASIS-DISABILITY PERIOD-IEP FILING-10/1997

SMI PREM START-11/1997 PENALTY-000% CURRENT AMT-\$ 54.00
SMI 3PTY START-03/1998 STOP-12/1999 CODE-500 CATEGORY-STATE BILLING
PENALTY-000%
START-01/2000 CODE-260 CATEGORY-STATE BILLING PENALTY-000%
ST EXCH SEWC-260 SECAC-H SEAD-11/01 SEAC-X SEWN-01M444770411
DIB INV TWPE-0 DIG-3180 MRED-12/03 MDR-7 DDT-A DPM-P SDIG-2960
SID SIFT-D SIED-01/02 SISC-E SCCR-26290 SILAC-A
DIB DDO-09/23/92 LOD-1
DIB DDO-05/15/95 DOED-11/95
HISTORY 02/98 \$ 296.70 \$ 0.00 700 01 SR \$ 296.00
12/98 \$ 300.50 \$ 0.00 500 01 SR \$ 300.00
12/99 \$ 307.70 \$ 0.00 700 01 SR \$ 307.00
12/00 \$ 318.40 \$ 0.00 400 01 SR \$ 318.00
07/01 \$ 318.70 \$ 0.00 700 01 SR \$ 318.00
12/01 \$ 326.90 \$ 0.00 900 01 SR \$ 326.00
PAYMENT PIC-C1 MPA-\$0.00 DOC-190 SCC-50160 RD-03/08/99 LAP-U
TELE NO BTN- BTC1-H CPND-09/98
PAYEE

SOCIAL SECURITY
Office of the Inspector General

AACT DTE:06/17/02 SSN: BIC: DOC: UNIT: PG: 003+
ADDRESS

BENEFIT BIC-C1 SB-F DOB-07/11/1998 B DOEC-08/98 ABN-5BIJ
LAF-SD MBP-\$0.00 DRD-09/10/98 DOCA-09/98 DOEI-08/98 DOF-08/98
DOST-08/98 SAC-DC ENAC-C LMETY-98 RELATC-N

ST EXCH SEWC-260 SECAC-C SEAD-11/01 SEAC-X SEWN-003630294
R PAYEE DOS-09/1998 TOP-MTH CC-PYE GS-N CMC-Y RPN- RPNI-1
BENREF BOAN-
HISTORY 08/98 \$ 0.00 \$ 0.00 000 D00 R \$ 0.00

PRISONER

A RECORD IS PRESENT ON THE PRISONER UPDATE PROCESSING SYSTEM
DATABASE FOR BOAN: BIC-A .

+++ TRANS UPDATED THRU 06/17 +++

TRANS RD-2/05/02 LAP-#C BACOM-SSI UPDATE PIC-A
RD-2/07/02 LAP-#C BACOM-SSI UPDATE PIC-A

SOCIAL SECURITY
Office of the Inspector General

SSACCS DTE:06/20/02 SSN: DOC: UNIT: PG: 001+
STATUS MBR YES LOU-06/20 DATA FILES YES LOU-06/20 SSACCS NO LOU-06/19
CPS NO
ACCOUNT PCOC-7 QCE-25 QCR-13 SP-F CIS-NS TAC-D RCC-5 ERC-95 CDY-0
PMT CYC CYI-1 PCEFD-06/15/1996 PCCOM-06/96 PCCR-S
PRIMARY DOB-11/09/1960 LSPA-\$0.00
PIA HIS 12/00 \$ 318.40 L K FMAX-\$ 318.40D
07/01 \$ 318.70 L K FMAX-\$ 318.70D
12/01 \$ 326.90 L K FMAX-\$ 326.90D
PAYMENT PIC-A MPA-\$326.00 DOC-C52 SCC-26290 RD-02/07/02 LAP-# PSC-C
TELE NO BTC1-N CPND-03/01
PAYEE
ADDRESS
BANK RTN-021031207 DAN- BDCD-09/14/00 SRCD-E
BENEFIT BIC-A SB-F DOB-11/09/1960 B DOEC-11/95 ABN-314C
LAF-C MBP-\$326.00 DRD-09/14/00 DOEI-11/95 DOF-10/96 SAC-D ENAC-C
LANG-E RDD-090
MED BILLING-3RD PTY

HI CONTS PRD-11/1997 SMI CONTS PRD-11/1997

HI-DIB START-11/1997 BASIS-DISABILITY TYPE-FREE FILING-10/1997

SSACCS DTE:06/20/02 SSN: DOC: UNIT: PG: 002+
SMI-DIB START-11/1997 BASIS-DISABILITY PERIOD-IEP FILING-10/1997

SMI PREM START-11/1997 PENALTY-000% CURRENT AMT-\$ 54.00
SMI 3PTY START-03/1998 STOP-12/1999 CODE-500 CATEGORY-STATE BILLING
PENALTY-000%
START-01/2000 CODE-260 CATEGORY-STATE BILLING PENALTY-000%
ST EXCH SEWC-260 SECAC-H SEAD-11/01 SEAC-X SEWN-01M444770411
DIB INV TWPE-0 DIG-3180 MRED-12/03 MDR-7 DDT-A DPM-P SDIG-2960
SID SIFT-D SIED-01/02 SISC-E SCCR-26290 SILAC-A
DIB DDO-09/23/92 LOD-1
DIB DDO-05/15/95 DOED-11/95
HISTORY 02/98 \$ 296.70 \$ 0.00 700 01 SR \$ 296.00
12/98 \$ 300.50 \$ 0.00 500 01 SR \$ 300.00
12/99 \$ 307.70 \$ 0.00 700 01 SR \$ 307.00
12/00 \$ 318.40 \$ 0.00 400 01 SR \$ 318.00
07/01 \$ 318.70 \$ 0.00 700 01 SR \$ 318.00
12/01 \$ 326.90 \$ 0.00 900 01 SR \$ 326.00
PAYMENT PIC-C1 MPA-\$0.00 DOC-190 SCC-50160 RD-03/08/99 LAP-U
TELE NO BTN- BTC1-H CPND-09/98
PAYEE

Exhibit 6-17

SOCIAL SECURITY
Office of the Inspector General

SSACCS DTE:06/20/02 SSN: DOC: UNIT: PG: 003+
ADDRESS

BENEFIT BIC-C1 SB-F DOB-07/11/1998 B DOEC-08/98 ABN-5BIJ
LAF-SD MBP-\$0.00 DRD-09/10/98 DOCA-09/98 DOEI-08/98 DOF-08/98
DOST-08/98 SAC-DC ENAC-C LMETY-98 RELATC-N

ST EXCH SEWC-260 SECAC-C SEAD-11/01 SEAC-X SEWN-003630294
R PAYEE DOS-09/1998 TOP-MTH CC-PYE GS-N CMC-Y RPN-533725725 RPNI-1
BENREF BOAN-
HISTORY 08/98 \$ 0.00 \$ 0.00 000 D00 R \$ 0.00

+++ TRANS UPDATED THRU 06/20 +++

TRANS RD-2/05/02 LAP-#C BACOM-SSI UPDATE PIC-A
RD-2/07/02 LAP-#C BACOM-SSI UPDATE PIC-A

+++ YEAR 2000 COMPS +++

07/16/2001 - CPI COLA 2000 ADJUSTMENT OF \$12 PAID TO A.

CPI COLA ADJUSTMENT 2000 NOT PAID TO C1 BECAUSE NO BENEFITS WERE PAID

Exhibit 6-18

SOCIAL SECURITY
Office of the Inspector General

QRY
NUMI

NUMIDENT QUERY

TRANSFER TO:
XXXXXX

SENSITIVE INFORMATION

UNIT:

COMPLETE THE FOLLOWING

ROUTE RESPONSE TO / RETURN TO (SELECT ONE): 1

1=SCREEN 2=PRINTER/MAIN 3=PRINTER

SOCIAL SECURITY NUMBER: xxx xx xxxx

OPTIONAL FIELD

ADDITIONAL RECORD TYPES REQUESTED:

1 = CROSS REFERENCE RECORDS

2 = CORRESPONDENCE RECORDS

3 = BOTH OF THE ABOVE

SSN VERIFICATION PRINTOUT: N (Y/N)

SOCIAL SECURITY
Office of the Inspector General

NUMI DTE:06/07/02 SSN:----- XC:X UNIT:----- PG:001+

ACCOUNT SSN:----- ETC:0 RFN:70655032228 DOC:520 IDN:P

NAME NAA: -----

BIRTH (b) (6)

PARENT (b) (6)

FNA: (b) (6)

INTERNAL FMC:1 CYD:03/09/1987

ACCOUNT (b) (6) ETC:2 RFN:73512062718 DOC:491 IDN:D

NAME NAA: -----

BIRTH (b) (6)

PARENT MNA: -----

FNA: -----

INTERNAL FMC:1 CYD:12/18/1987

Exhibit 6-20

SOCIAL SECURITY
Office of the Inspector General

QRY ALPHA-INDEX QUERY ALPH
TRANSFER TO: SENSITIVE INFORMATION UNIT: OIG124

COMPLETE THE FOLLOWING

APPLICANT NAME:
XXXXXXXXXXXXX XXXXXXXXXXXXXXXX XXXXXXXXXXXXXXXX XXXXX
BIRTH DATE OR START DATE OF SEARCH RANGE (MMDDCCYY):
ROUTE RESPONSE TO / RETURN TO (SELECT ONE): 1
1=SCREEN 2=PRINTER/MAIN 3=PRINTER

ADDITIONAL OPTIONAL SEARCH FIELDS

FOR DATE OF BIRTH SEARCH RANGE
 NUMBER OF MONTHS TO BE SEARCHED (1 - 12): _____
 NUMBER OF YEARS TO BE SEARCHED (1 - 4): _____
 PLACE OF BIRTH STATE: _____ FOREIGN COUNTRY: _____
MOTHER'S NAME AT HER BIRTH:

FATHER'S NAME: _____

REQUEST RESPONSES EXCEEDING DESIGNATED MAXIMUM (Y/N): _____

SOCIAL SECURITY
Office of the Inspector General

DATA EXCHANGE QUERY MENU

DXQM

FIELD OFFICE: XXX UNIT: XXXXXX

SELECT ONE OF THE FOLLOWING: X

1= NDNH (NEW HIRE, QTR WAGE, UNEMPLOYMENT)

2= VBAQ (VETERANS BENEFIT ADMINISTRATION)

3= SAVE (NON-IMMIGRANT INFORMATION AND ALIEN STATUS VERIFICATION)

SOCIAL SECURITY NUMBER (NOT VALID FOR OPTION 3): **(b) (6)** _____

SOCIAL SECURITY
Office of the Inspector General

QRY NATIONAL DIRECTORY NEW HIRE, WAGE & UNEMPLOYMENT MENU
NDNH

SSN: ----- DATE: 06/18/2002 UNIT: -----

'Y' MEANS SSN IS ON THE REPORT. OVERKEY WITH 'X'S' FOR DETAILS.

'N' MEANS SSN IS NOT ON THE REPORT.

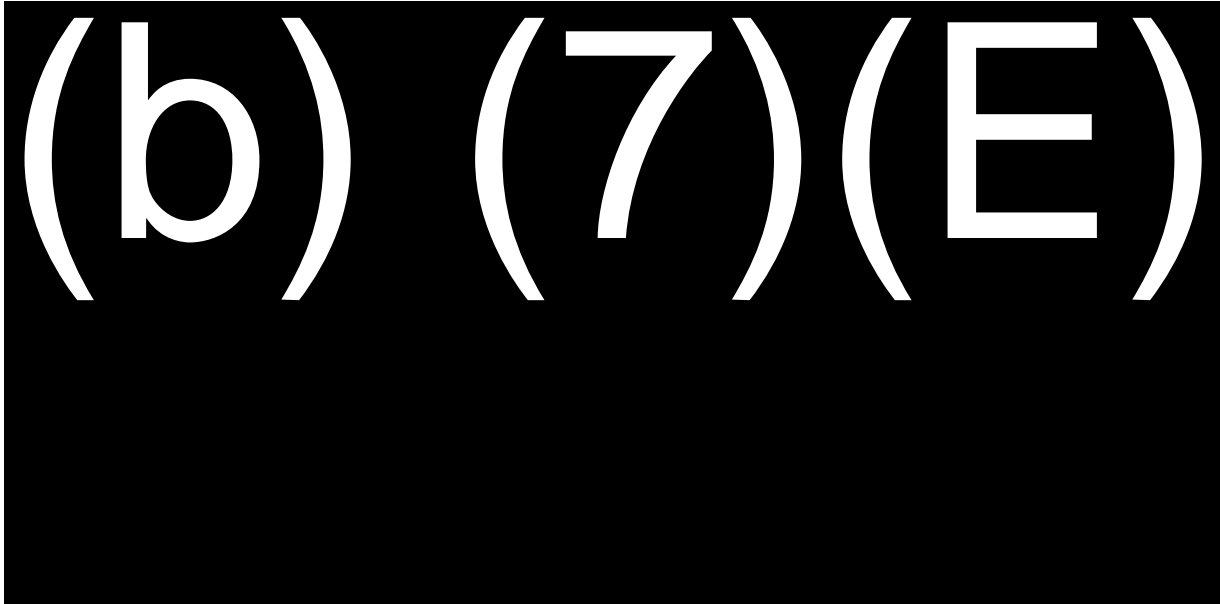
'QUARTER' MEANS WHEN THE REPORT WAS PROCESSED, NOT WHEN PAYMENTS WERE MADE.

NEW HIRE REPORT:	WAGE REPORT	UNEMPLOYMENT REPORT	
QUARTER			
4TH/2001	N	N	(INCOMPLETE
QUARTER)			
3RD/2001	N	N	
2ND/2001	N	N	
1ST/2001	N	N	
4TH/2000	N	N	
3RD/2000	N	N	
2ND/2000	N	N	
1ST/2000	N	N	
4TH/1999	N	N	

Exhibit 6-23

SOCIAL SECURITY
Office of the Inspector General

SAVE - SYSTEMATIC ALIEN VERIFICATION FOR ENTITLEMENT



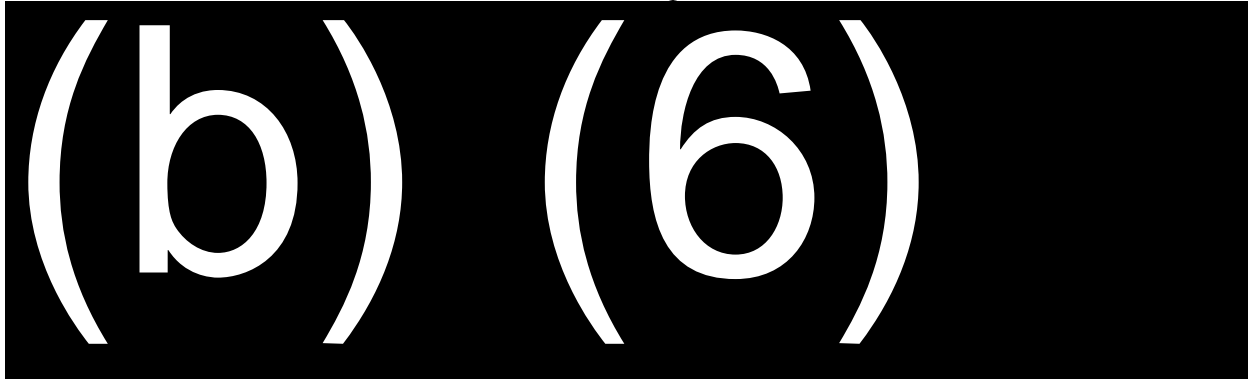
SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)

SOCIAL SECURITY
Office of the Inspector General

SEQY DTE:06/18/02 AN: ----- DOC: --- UNIT: ----- PG: 001
MEF: QN: ----- NA: ----- DB: (b) (6) SX: (AK: (b) (6) (

SUMMARY FICA EARNINGS FOR YEARS REQUESTED



REMARKS
CLAIMS ACTIVITY -- SEE MBR
W-2 PENSION EARNINGS PRESENT FOR: 1987
NON-COVERED EARNINGS PRESENT FOR: 1990-1999

SOCIAL SECURITY
Office of the Inspector General

QRY DETAIL EARNINGS QUERY DEQY
TRANSFER TO: UNIT: XXXXXX

ROUTE RESPONSE TO (SELECT ONE): 1
1=SCREEN 2=PRINTER/MAIN 3=PRINTER

ACCESS KEYS

SSN: XXXXXXXXXX EIN: PAYROLL RECORD UNIT:

REPORT PERIODS

INCLUSIVE YEARS: TO
SPECIFIC YEARS (ENTER UP TO 5 YEARS):

REQUESTED DETAILS (DEFAULT IS COVERED DETAILS ONLY): X

1=COVERED DETAILS	5=PENSION
2=SELF-EMPLOYMENT	6=RAILROAD
3=MQGE & HEALTH INSURANCE	7=SPECIAL WAGE PAYMENT
4=ALL NON-COVERED DETAILS	8=EMPLOYER ADDRESS
	9=LAST EMPLOYER ADDRESS

RELATED SSN:
MAXIMUM OVERRIDE REQUESTED(Y/N): N

SOCIAL SECURITY
Office of the Inspector General

QRY DATE:06/20/02 AN:----- DOC:--- UNIT:----- DEQR PG:001
INPUT: YRS REQ: 1998-2001; COVERED DETAILS
MEF: NA:----- DB: (b) (6) SX: (AK: (b) (6)



00 NONE

01 NONE

REMARKS

NON-COVERED EARNINGS PRESENT FOR 1998-1999

SOCIAL SECURITY
Office of the Inspector General

QRY SUPPLEMENTAL SECURITY INCOME QUERIES SSQM
TRANSFER TO: UNIT: XXXXXX

COMPLETE THE FOLLOWING FOR ALL SELECTIONS
ROUTE RESPONSE TO / RETURN TO (SELECT ONE): 1
1=SCREEN 2=PRINTER/MAIN 3=PRINTER
SOCIAL SECURITY NUMBER: XXXXXXXXXX

SELECT ONE OF THE FOLLOWING: X
1=SSID (COMPLETE RECORD REQUEST)
2=SSI2 (SELECTIVE REQUEST)
3=SSI3 (GENERAL SSI QUERY)
4=SSI4 (OVERPAYMENT/REDETERMINATION QUERY)

COMPLETE FOR SPECIFIED QUERY (AS NEEDED)
ANY= ACCOUNT HOLDER:
RECORD NUMBER:
SSID= LIMIT:
SSI2= SEGMENT REQUEST IDENTIFIERS:

SOCIAL SECURITY
Office of the Inspector General

MSG: DTE:06/19/02 SSID QN: ----- RN:04X04 UN: ----- PG: 001+
 CCTL FUN: ----- CFL:C52 MV:02/01/02-R FRC:L00 PFL:191
 ----- PSY:C01 TMR:DI ID:DI TDA:06/10/02 SEQ:4
 CMSC HUN: ----- RIC:G VER:3 CPD:06/10/02-P CPF:06/10/02 SD:03/02
 SBM:01/02 MSI:2-1-02/01/02
 RMKS 1:DD IS EBT ACCT
 CRZD RZ: S RZP T RZD RZI RZC RTD EE
 3 02/01/02 02/02 02/02
 PRSN RE: C:B AP:11/17/97 DB:(b) (6) -B SX:(b) (6) - - - LPS:ENGLISH
 LPW:ENGLISH DOE:11/97 AK:(b) (6) (b) :1 MCI:C
 RCRD EST:02/01/02 XDO:C52 IDD:**88888C SNV:3 CNV:5 LAF:C PCO:7 FS:Y-N-02/02
 DRDP BCR:----- BCA:----- DDC:02/01/02
 ADDR CTY: STN:----- DIS:C52
 ST:26290A ACD:02/01/02
 RADR ----- CTY:----- STN:-----
 DIAR MR-06/30/01
 DISB DPC:F SAC:S82 DSA:11/17/97 DDO:05/15/95 MQ:E MDR:3 DIG:3180-2960 DPM:N
 NOTC C/O:Y 06/10/02-8100 2013 2002 2016 1904 1295 1905 2525 RVW001 1926
 1438 1487 2750 2570 1720 SSAS12 -- 02/23/02-8166 2013 2002 1905 1018
 1016 1931 2400 RVW001 1926 1487 1650 1727 1720 SSAS12 ENC008 1654 --
 02/01/02-0002 0000
 MULT ----- X-02/01/02

 MSG: DTE:06/19/02 SSID QN: ----- RN:04X04 UN: ----- PG: 002+
 TRAN UN:PAM OL-06/10/02-C52, OL-06/10/02-C52, DA-06/06/02-C52,
 PR-04/13/02-D98, OL-03/22/02-C52, OL-03/22/02-C52, OL-03/11/02-C52,
 NU-02/06/02, MB-02/05/02, OL-02/01/02-C52
 UMIH
 TUMP UMS UMA FUMI PV TUMP UMS UMA FUMI PV
 A 0102 0000 326.00 C 533725725A 71
 CMPH FAM SAM SUP UMC ENC PCI PS BELGPF FO MHSWADCMICT
 0102 .00 .00 26290 306.00 .00 306.00 C01 0ENN AZ 3NN SW4
 0202 .00 .00 26290 .00 .00 .00 N25 0NNN AZ 3NN SW4
 0302 TOP:239.00 SQN:03
 0302 .00 .00 26290 .00 .00 .00 N25 0NNN AZ 3NN SW4
 0602 239.00 .00 26290 306.00 .00 306.00 C01 0ENN AZ 3NN SW4
 0702 239.00 .00 26290 306.00 .00 306.00 C01 1ENN AZ 3NN SW4
 PMTH 1 2 3 5 CKA FMA SMA U
 03/01/02 1 N D 239.00 239.00 .00
 04/01/02 5 N 54.50 54.50 .00
 04/01/02 1 N D 184.50 184.50 .00
 07/01/02 5 N 54.50 54.50 .00
 07/01/02 1 N D 184.50 184.50 .00
 PUPS PRISONER DATA EXISTS FOR -----
 MPMT OPD:2414.20 TNP:Y OPR:54.50 OPC:218.00

 MSG: DTE:06/19/02 SSID QN: RN:04X04 UN: ----- PG: 003
 OPSQ C OPB OPE OPA AX TS SQD NTD SQR SBL BAL
 01 0000 0000 2061.80 PX 020102 M-010202 .00 1843.80

Exhibit 6-30

SOCIAL SECURITY

Office of the Inspector General

02	0000 0000	352.40	PX 020102 M-010202	.00	352.40						
03	0302 0502	717.00	MN 061002 M-061002	.01	717.00						
04	0000 0000	239.00	PN 061002 M-061002	.01	239.00						
OPDD	DTE	AMT	USD	SCD	DOC	TR1	OSN	FIL	L	DEC	R
	02/01/02	2061.80	.00	533	P	99	01				
	02/01/02	352.40	.00	533	P	99	02				
	02/01/02	352.40	.00	533	D		02				
	03/22/02	2061.80	.00	C52	WX	01	02/15/02	03/22/02	F		
	03/22/02	2061.80	.00	C52	D		01				
	06/10/02	239.00	.00	C52	P	99	04				
	06/10/02	717.00	.00	533	DA		03				
	06/10/02	239.00	.00	533	DA		04				

SOCIAL SECURITY
Office of the Inspector General

PHU1 DTE:06/19/02 SSN: ----- DOC: -- UNIT: ----- PG: 001+
STATUS MBR YES PHUS YES LOU-06/19 DATA FILES YES LOU-06/19
SSACCS NO LOU-06/18

ACCOUNT PCOC-7 NOB-01 BICS-A

PERSON BIC-A NAME- ----- (b) (6) -----
MBR FDS DOC-C52 CAD-03/16/01 RTN- ----- BDCD-09/14/00
PAYEE- -----
ADDRESS- -----
LAF-C NAME- ----- DOB: (b) (6) DOEC-11/95 ABN-314C
DOEI-11/95 SMI START-11/97 MBC-\$326.00 PCI-1
INDCTR RETURN TO MBR-11/00 RT-Y
PNAD -----

+++BIC-A TY-01+++
TRANS RPD-07/13/01 COM-07/01 SSC-Z3 OCO A- PAYMENT SYSTEM
EVNT-042 PMA CHK AMT-\$ 12.00 OCO CPS RPD-07/16/01 ETD-07/01
EVNT-199 CPICOLA PY AMT-\$ 12.00 ETD-07/01 **INFORMATIONAL**
MBR PMT EVNT-014 RECUR PMT AMT-\$ 318.00 ETD-01/01 THRU 07/01 (07)
EVNT-014 RECUR PMT AMT-\$ 318.00 ETD-08/01 THRU 12/01 (05)
STM TOT BENEFITS FOR 2001-\$ 3828.00 (BOX 3)

PHU1 DTE:06/19/02 SSN: ----- DOC: -- UNIT: ----- PG: 002
INCLUDES:00-\$ 12.00
ADD: DIRECT PAY-----\$ 3828.00

BENEFITS REPAID TO SSA IN 2001-\$ 0.00 (BOX 4)

+++NET BENEFITS FOR 2001-\$ 3828.00
+++ (BOX 5=BOX 3 MINUS BOX 4)

SOCIAL SECURITY
Office of the Inspector General

QRY

MISCELLANEOUS MENU

MISM

TRANSFER TO:

UNIT: XXXXXX

SELECT ONE OF THE FOLLOWING: XX

- | | |
|--|----------------------------------|
| 1=DRMQ (DRAMS QUERY) | 9=DTMA (ADD DEATH RECORD) |
| 2=CRC1 (CORC OFFLINE/CASE QUERY RECORD) | 10=DTMC (CORRECT DEATH RECORD) |
| 3=CRC2 (CORC ONLINE COUNTS QUERY RECORD) | 11=DTMD (DELETE DEATH RECORD) |
| 4=CRC3 (CORC ONLINE SSN QUERY NUMBER) | 12=RTND (ROUTING TRANSIT NUMBER) |
| 5=FUTURE USE | 13=AEQY (ALPHA ACCESS TO EIF) |
| 6=FUTURE USE | 14=ERQY (EMPLOYER REPORT QUERY) |
| 7=FUTURE USE | |
| 15=SEID(SSAEMPLOYEEIDENTIFICATION) | |
| 8=FUTURE USE | |

COMPLETE THE FOLLOWING FOR SELECTION 1 ONLY - DRMQ (DRAMS QUERY)

SOCIAL SECURITY NUMBER: XXXXXXXXX

ROUTE RESPONSE TO / RETURN TO (SELECT ONE): 1

1=SCREEN 2=PRINTER/MAIN 3=PRINTER

SOCIAL SECURITY
Office of the Inspector General

PAGE 1 OF 1 FINAL FINANCIAL INSTITUTION LISTING RTN1

NAME: COMMERCIAL FEDERAL BANK UNIT: XXXXXX

ADDRESS: 2120 SOUTH 72 ST RTN: 3011-7108-1

OMAHA NE DD RTN:

XREF RTN:

ZIP: 68124-0000 TELEPHONE: (402) 390-5132

REMARKS:

DAN MUST BE 10 DIGITS--IF 13 SHOW, DROP LAST 3 DIGITS.

SOCIAL SECURITY
Office of the Inspector General

EM 1.4 EIF ACCESS AEQY
TRANSFER TO: UNIT: XXXXXX
ROUTE RESPONSE TO / RETURN TO (SELECT ONE): 1
1=SCREEN 2=PRINTER/MAIN 3=PRINTER

EIN:

BUSINESS OR U.S. GOVERNMENT NAME:
(b) (6) STATE: (b) (OPTIONAL)

INDIVIDUAL EMPLOYER NAME: STATE:
FIRST MIDDLE LAST

STATE/LOCAL GOVERNMENT NAME:
STATE:

OPTIONAL SEARCH CRITERIA:
CITY: OR ZIP CODE:

SHOW ALL POSSIBLE MATCHES: N (Y OR N)
FOREIGN COUNTRY: N (Y OR N)

SOCIAL SECURITY
Office of the Inspector General

EM 1.4 EIF ACCESS AEQY
TRANSFER TO: UNIT: XXXXXX
ROUTE RESPONSE TO / RETURN TO (SELECT ONE): 1
1=SCREEN 2=PRINTER/MAIN 3=PRINTER

EIN: 43 1890723

BUSINESS OR U.S. GOVERNMENT NAME:
STATE: (OPTIONAL)

INDIVIDUAL EMPLOYER NAME:
STATE:
FIRST MIDDLE LAST

STATE/LOCAL GOVERNMENT NAME:
STATE:

OPTIONAL SEARCH CRITERIA:
CITY: OR ZIP CODE:

SHOW ALL POSSIBLE MATCHES: (Y OR N)
FOREIGN COUNTRY: (Y OR N)

SOCIAL SECURITY
Office of the Inspector General

AEQY DTE: 06/19/02 DOC: --- UNIT: ----- PG: 01 OF 01

EIN: (b) (6) EMPLOYER NAME: (b) (6)

(b) (6)

YEAR:2002 WEEK:19

SOCIAL SECURITY
Office of the Inspector General

QRY CONSOLIDATED QUERY CNQY
TRANSFER TO: UNIT: XXXXXX

SOCIAL SECURITY NUMBER: XXXXXXXXX

SELECT ANY OF THE FOLLOWING:

- | | |
|----------------------------------|--------------------------|
| 0=AACT (ABBREVIATED MBR) | 5=**** |
| 1=SSID (COMPLETE RECORD REQUEST) | 6=DEQY (DETAIL EARNINGS) |
| 2=NUMI (NUMIDENT) | 7=SSI2 (FOLDER LOCATION) |
| 3=SEQY (SUMMARY EARNINGS) | 8=**** |
| 4=ALL OF THE ABOVE (0-3) | 9=FACT (FULL MBR) |

ONLINE (Y/N):

SOCIAL SECURITY
Office of the Inspector General

RPAY RP QUERY RESPONSE SELECTION LIST RQSL
UNIT: (b) (6)

APPLICANT/REP PAYEE SSN:
APPLICANT/REP PAYEE LOCATION ZIP:
BENEFICIARY/RECIPIENT SSN: OR UNKNOWN (Y/N):

QUERY RESPONSE(S) SELECTION(S):

1. RP SCREENING QUERY RESPONSE
2. RP FULL QUERY RESPONSE
3. INDIVIDUAL BENEFICIARY/RECIPIENT QUERY RESPONSE

(SELECTIONS 1, 2, AND 3 WILL ALWAYS BE RETURNED TO THE SCREEN)

4. INDIVIDUAL RP BENEFICIARY/RECIPIENT LIST (RPBL)
5. ORGANIZATION/INSTITUTION RP BENEFICIARY/RECIPIENT LIST (OIBL)

Exhibit 6-40A

SOCIAL SECURITY
Office of the Inspector General

PCACS 06/19/02 STANDARD QUERY SQRY
TRANSFER-TO: ENTERING COMPONENT: MODXX UNIT: XXXXXX

ROUTE RESPONSE TO: 1 1. SCREEN 2. PRINTER

ENTER SSN/SSNX OR SELECT RECORD(S) FOR FULL QUERY:
SSN: XXXXXXXXXX SSNX:

Exhibit 6-40B

SOCIAL SECURITY
Office of the Inspector General

PCACS 06/19/02 STANDARD QUERY SQRY
TRANSFER-TO: ENTERING COMPONENT: MODXX UNIT: -----

ROUTE RESPONSE TO: 1 1. SCREEN 2. PRINTER

ENTER SSN/SSNX OR SELECT RECORD(S) FOR FULL QUERY:
SSN: ----- SSNX:

SSN	SSNX	AD I H C TOEL1/2/LIST	LOCATION	LOCDT	SITEDT
<u>_X_</u> -----	70111		PC7 FRCS STG S01	090100	021397

SOCIAL SECURITY
Office of the Inspector General

PCACS 06/19/02

FOLDER QUERY

FQY1

ENTERING COMPONENT: MODXX

UNIT: XXXXXX

SSN: XXXXXXXX SSNX: 70111 ASSOCIATION DESCRIPTOR (AD): HOLD DT:

TYPE OF RECORD:

CURRENT LOCATION: PC7 FRCS STG S01

02/13/97 09/01/00 09/01/00 09/01/00

PREVIOUS LOCATION: PC7 AUXRH FIN FIN

02/13/97 02/13/97 02/13/97 02/13/97

TO LOCATION:

FRC CODE: 07 ACCESSION: 047-00-2198 CONTAINER: 0000063 ASSIGN:

FRC DT: 09/01/00 PENDING INACTIVATION: FOLDER REQUEST DT:

SPECIAL EVENT:

LISTING CODES:

RELATED RECORDS:

SSN: SSNX: AD: SSN: SSNX: AD:

SSN: SSNX: AD: SSN: SSNX: AD:

CONVERTED RECORD: PAGE 1

Social Security Administration
Consent for Release of Information

TO: Social Security Administration

Name _____

Date of Birth _____ Social Security Number _____

I authorize the Social Security Administration to release information or records about me to:

NAME

ADDRESS

_____	_____
_____	_____
_____	_____

I want this information released because:

(There may be a charge for releasing information.)

Please release the following information:

- ___ Social Security Number
- ___ Identifying information (includes date and place of birth, parents' names)
- ___ Monthly Social Security benefit amount
- ___ Monthly Supplemental Security Income payment amount
- ___ Information about benefits/payments I received from _____ to _____
- ___ Information about my Medicare claim/coverage from _____ to _____
(specify) _____
- ___ Medical records
- ___ Record(s) from my file (specify) _____
- ___ Other (specify) _____

I am the individual to whom the information/record applies or that person's parent (if a minor) or legal guardian. I know that if I make any representation which I know is false to obtain information from Social Security records, I could be punished by a fine or imprisonment or both.

Signature: _____
(Show signatures, names, and addresses of two people if signed by mark.)

Date: _____ Relationship: _____

Social Security Administration
Consent for Release of Information

Please read these instructions carefully before completing this form.

**When To Use
This Form**

Complete this form only if you want the Social Security Administration to give information or records about you to an individual or group (for example, a doctor, or an insurance company).

Natural or adoptive parents or a legal guardian, **acting on behalf of a minor**, who want us to release the minor's:

- o nonmedical records, should use this form,
- o medical records, should not use this form, but should contact us.

Note: Do not use this form to request information about your earnings or employment history. To do this, complete Form SSA-7050-F3. You can get this form at any Social Security office.

**How To
Complete
This Form**

This consent form must be completed and signed only by:

- o the person to whom the information or record applies, or
- o the parent or legal guardian of a minor to whom the **nonmedical** information applies, or
- o the legal guardian of a legally incompetent adult to whom the information applies.

To complete this form:

- o Fill in the name, date of birth, and Social Security Number of the person to whom the information applies.
- o Fill in the name and address of the individual or group to which we will send the information.
- o Fill in the reason you are requesting the information.
- o Check the type(s) of information you want us to release.
- o Sign and date the form. If you are not the person whose record we will release, please state your relationship to that person.

The Paperwork Reduction Act of 1995 requires us to notify you that this information collection is in accordance with the clearance requirements of section 3507 of the Paperwork Reduction Act of 1995. We may not conduct or sponsor, and you are not required to respond to, a collection of information unless it displays a valid OMB control number.

TIME IT TAKES TO COMPLETE THIS FORM--We estimate that it will take you about 3 minutes to complete this form. This includes the time it will take to read the instructions, gather the necessary facts and fill out the form. If you have comments or suggestions on this estimate, write to the Social Security Administration, ATTN: Reports Clearance Officer, 1-A-21 Operations Bldg., Baltimore, MD 21235-0001. Send only comments relating to our "time it takes" estimate to the office listed above. All requests for Social Security cards and other claims-related information should be sent to your local Social Security office, whose address is listed under Social Security Administration in the U.S. Government section of your telephone directory.



Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

Request for Testimony and/or Information/Records

Case Caption: _____

Criminal Matter: (Check if Yes)

Civil Matter: (Check if Yes)

Name of the prosecutorial authority: _____

Name, phone number and email address of lead prosecutor: _____

Brief explanation of testimony and/or information being requested, date testimony or information is needed, name of employee requested to testify (if applicable) and sufficient information to identify the individual about whom testimony or information is requested, such as name, Social Security number, and date of birth, etc. _____

If the request is for testimony from a specific employee, include a brief explanation of why the testimony of that particular employee is required.

If a specific SSA employee is not needed to testify, describe the testimony needed, and SSA, in consultation with OIG, will identify the employee who possesses the necessary expertise and information.

Certified records are required: Yes No

SSA or an SSA employee is a party in the matter: Yes No

If SSA or an SSA employee is not a party, provide sufficient information to explain why providing the records or testimony is in SSA's interest (i.e., potential SSN fraud or benefit fraud is involved, needed for an open OIG investigation, etc.)

OIG has an open investigation: Yes No

Name, phone number and email address of OIG agent assigned to the investigation:

INVESTIGATIVE OPERATIONS AND SUPPORT

007.000 **Investigative Operations**

- A.** An Investigative Operation is a planned event, or series of events, involving one or more special agents (SAs) and, at times, other law enforcement officers, participating in one or more specialized and/or high risk law enforcement activities/techniques.
- B.** Investigative Operations are further classified as:
- 1. Field Operations**, which are planned actions that are **independent of undercover operations**, and which are designed to investigate a criminal operation that involves sensitive activities or techniques, or the activity, places investigators, SSA employees, and the public in high-risk situations.
 - a.** Examples of *sensitive activities* include:
 - 1.** Covert investigations conducted at Social Security Administration (SSA) facilities.
 - 2.** Executing arrest warrants at SSA facilities.
 - a.** (b) (7)(E) [REDACTED]
 - b.** (b) (7)(E) [REDACTED]
 - 3.** (b) (7)(E) [REDACTED]
 - 4.** (b) (7)(E) [REDACTED]
 - b.** Examples of *sensitive techniques* include:
 - 1.** Surveillance measures used to intercept wire, oral, and /or electronic communications, conduct mobile tracking, or obtain video imaging (e.g. “pole camera”), to include those measures that require judicial authorization.
 - 2.** Executing search and/or arrest warrants.

Questions concerning whether a particular activity or technique is a Field Operation within the meaning of this section should be directed to the Criminal Investigations Division (CID) through the appropriate Assistant Special Agent-in-Charge (ASAC), Resident Agent-in-Charge (RAC), or Special Agent-in-Charge (SAC).

c. Examples of *high-risk situations* include:

1. The execution of arrest and/or search warrants in high crime areas.
2. When known or suspected organized criminal groups are targeted.

2. **Undercover Activities** are any investigative activities involving the use of an assumed name or cover identity by an employee of the Office of the Inspector General (OIG); another Federal, State, or local law enforcement organization; or individual (e.g. SSA employee purporting to be a corrupt employee, confidential informant, etc.); working with, or under the direction and control of the Office of Investigations (OI). Therefore, if the employee or individual is not acting under an assumed name or cover identity, the activity is not deemed an Undercover Activity, but rather a Field Operation.

3. **Undercover Operations** involve a series of related undercover activities over a period-of-time by an undercover employee or individual, as designated above. For the purpose of this policy, “employee” refers to any OIG employee, SSA employee, or employee of a Federal, State, or local law enforcement agency, or confidential informant working under the direction and control of OI in a particular investigation, whose relationship with OI is concealed from third parties in the course of an investigative operation by the maintenance of a cover or alias identity. Additionally, for the purpose of this policy, a “series of undercover activities” generally consists of more than three separate substantive contacts by an undercover employee with the individual(s) under investigation. However, undercover activity involving sensitive or fiscal circumstances constitutes an undercover operation regardless of the number of contacts involved. A contact is “substantive” if it is a communication with another person, whether by oral, written, wire, or electronic means, which includes information of investigative interest. Mere incidental contact, e.g., a conversation that establishes an agreed time and location for another meeting, is not a substantive contact within the meaning of this policy. Undercover activity includes using a fictitious identity or cover in an on-line or virtual environment. Undercover Operations are designed to:

- a. determine if a crime is being planned or has been committed;
- b. identify persons involved;
- c. obtain evidence; and,
- d. establish the most opportune time and place for making arrests and seizing contraband.

C. The following investigative procedures are **not** considered as Field or Undercover Activities/Operations for purposes of this section:

1. Use of temporary covers by OI employees on surveillance or conducting routine investigative activities, (b) (7)(E)
2. (b) (7)(E).

3. Contacting informants.
4. Operations in which the SSA Office of the Inspector General (OIG) is not the lead investigative agency, **and** when no OIG employee is participating as an undercover operative. This does **not** include cases involving SSA employees or SSA facilities.

007.010 Policy

- A. All Field Operations will be approved by the Field Division (FD) SAC or his/her designee. Instructions contained in Chapter 8 of this Handbook apply if electronic monitoring of communications will incur during the field operation.
- B. All Undercover Activities and Operations will be approved, in advance, by the Operations Review Committee (ORC), OI Headquarters (HO). Prior to requesting approval for an undercover activity or operation, the agent and supervisor must consult the *Council of the Inspectors General on Integrity and Efficiency (CIGIE) GUIDELINES ON UNDERCOVER OPERATIONS* to determine the level of approval required for the operation (See [Guidelines on Undercover Operation \(CIGIE\)](#)). The Guidelines include instructions when working joint operations with the Federal Bureau of Investigation or other law enforcement agencies.
- C. Arrest Policy: When arrests are to be made as part of any operation or activity:
 1. Special agents (SA) must be aware of the sensitivities and the safety concerns inherent in executing arrests.
 2. SAs must exercise good judgment and use appropriate tactics to promote their safety and the safety of others.
- D. All Investigative Operations require the preparation and approval of a tactical plan prior to initiation (refer to Chapter 13 for specific information regarding search warrants). Tactical Plan: Surveillance, Undercover, Arrests (*Form OI-17, Exhibit 7-1*) and Tactical Plan for Search Warrants (*Form OI-18, Exhibit 7-2*) are written guidelines that outline the law enforcement activity in terms of purpose, personnel assignments, and targets of the investigative activity, equipment, identification, and emergency procedures. Additional information should be provided as appropriate. The *original* approved plan is always kept in the case file.
- E. Undercover Activities and Undercover Operations may involve danger to the operatives. Accordingly:
 1. Undercover Activities and Undercover Operations should not be used if other equally effective means of securing the desired information are available.
 2. All available physical protection should be afforded operatives. (b) (7)(E) [REDACTED] who have full law enforcement authority, unless unusual circumstances dictate otherwise.
 3. Volunteers should be sought to function as undercover operatives.

4. SACs/ASACs/RACs shall ensure, to the maximum extent practical, that the backgrounds of employees used in undercover operations are free of information that could be used to discredit their testimony.
- F. Before conducting an undercover operation lasting longer than six months, or involving any of the sensitive circumstances set forth in the Undercover Guidelines, the Office of the Inspector General must first notify the Federal Bureau of Investigation (FBI). The FBI may choose to join the investigation, in which case the undercover operation would be subject to review by the Criminal Undercover Operations Review Committee of the FBI. If the FBI opts not to join the case, the undercover operation will be reviewed by CIGIE's IG Undercover Review Committee (URC). No undercover operation involving sensitive circumstances may be conducted without the approval of one of these committees. For purposes of these Guidelines, sensitive circumstances are involved if there is a reasonable expectation that the undercover operation will involve one or more of the following circumstances:
1. An investigation of possible criminal conduct by any elected or appointed official, or political candidate for a judicial, legislative, management, or executive-level position of trust in a Federal, State, or local government entity or political subdivision thereof;
 2. An investigation of any public official at the Federal, State, or local level in any matter involving systemic corruption of any governmental function;
 3. An investigation of possible criminal conduct by any foreign official or government, religious organization, political organization, or the news media;
 4. Engaging in activity having a significant effect on or constituting a significant intrusion into the legitimate operation of a Federal, State, or local government entity;
 5. Establishing, acquiring, or operating a proprietary in accordance with all applicable laws and regulations;
 6. Providing goods or services that are essential to the commission of a crime, which goods and services are reasonably unavailable to a subject of the investigation except from the Government;
 7. Activity by an undercover employee that is proscribed by Federal, State, and local law as a felony or that is otherwise a serious crime, but not including the purchase of stolen or contraband goods; delivery or sale by the Government of stolen property whose ownership cannot be determined; controlled delivery of drugs that will not enter commerce; conduct of no more than five money laundering transactions, not to exceed a maximum aggregate amount of \$1 million; payment of bribes that are not included in the other sensitive circumstances; or the making of false representations to third parties in concealment of personal identity or the true ownership of a proprietary (this exemption does not include any statement under oath or penalties of perjury);
 8. A significant risk that a person participating in an undercover operation will be arrested or will supply falsely sworn testimony or false documentation in any legal or administrative proceeding;

9. Attendance at a meeting or participation in communications between any individual and his or her lawyer;
 10. A significant risk that a third party will enter into a professional or confidential relationship with a person participating in an undercover operation who is acting as an attorney, physician, clergyman, or member of the news media;
 11. A request to an attorney, physician, member of the clergy, or other person for information that would ordinarily be privileged, or to a member of the news media concerning an individual with whom the news person is known to have a professional or confidential relationship;
 12. Participation in the activities of a group under investigation as part of a terrorism enterprise investigation or recruiting a person from within such a group as an informant;
 13. A significant risk of violence or physical injury to individual(s) or a significant risk of financial loss;
 14. Activities that create a realistic potential for significant claims against the United States arising in tort, contract, or for compensation for the “taking” of property, or a realistic potential for significant claims against individual government employees alleging constitutional torts; or
 15. Untrue representations by a person participating in the undercover operation concerning the activities or involvement of any third person without that individual’s knowledge or consent.
- G.** The application process for undercover operations subject to CIGIE URC approval is found in Section IV.F. of the [*Guidelines on Undercover Operations \(CIGIE\)*](#).
- H.** Undercover operatives shall not participate in illegal activities to further the objective of the operation unless failure to do so might:
1. lead to the loss of evidence or information vital for prosecutive purposes;
 2. cause loss of operatives’ cover or credibility; or
 3. result in serious injury or death to anyone involved.
- I.** The restriction above governing the participation of operatives in illegal activities *does not apply* to the purchase or possession of contraband, stolen documents, or claims when the activity is an integral part of the evidence collection scheme or undercover operation.
- J.** If an undercover purchase is made using confidential funds to include an undercover credit/debit card, a request for an undercover activity/operation and use of confidential funds must be submitted.
- K.** Prior to initiating an undercover activity/operation in an on-line or virtual environment the SAC or ASAC of the Digital Forensics Team (DFT) will be notified. DFT will consult with the OI field division in reference to the best practices and investigative methodologies to conduct an on-line undercover operation, and obtain digital evidence in a forensically sound manner.

Initiating Undercover Activities/Operations

A. All SAC requests for authorization to initiate an undercover activity/operation must be made in writing and sent to the Deputy Assistant Inspector General for Investigations (DAIGI), through the CID desk officer for approval in advance of the operation. The desk officer will review the memorandum to ensure that all elements of the required information are addressed. The memorandum must contain the following information:

1. **Reason for Activity** – The request must include a reasonably detailed statement of the background of the case, and relate the circumstances to the need for the operation. A description of proposed methods should also be included.
2. **Offense(s)** – Include the *citations* of all alleged offenses.
3. **Danger/Contingency Plans** – Potential/anticipated danger and actions to protect any participant in an undercover or special operation must be noted in this section. (b) (7)(E) *this section must state the results of both state and Federal criminal history checks of the target of the interception, e.g. “Subject has three prior arrests for assault.” Any history of violent behavior on the part of the target(s) must be addressed specifically in this section. If the target is unknown, an inherent risk (b) (7)(E) should be assumed, and special precautions must be addressed.)*

The request must also state the intended contingency plans, that an OI-17 has been prepared and is on file, or that a tactical plan will be prepared by the lead agency and will be on file prior to the initiation of the operation. An OI-17 will not be required when the undercover activity is restricted to an on-line or virtual environment.

4. **Description and Location of Devices/Equipment** – The request must specify what special equipment, such as monitoring or recording devices, will be used. The request must state where the device(s) will be concealed; i.e., on the person, in personal effects, or in a fixed location. When the monitoring and/or recording device is to be worn by a civilian, this section should contain a statement that a Consensual Non-Telephone Monitoring Request (*Form OI-25AL, Exhibit 7-3*) is being requested.
5. **Location of Operation** – The request must specify the location and primary judicial district where the operation will take place. If the location changes, notice should be given promptly to the approving DOJ and OI HQ officials.
6. **Duration and Dates** – The request must state the length of time needed for the operation. Initially, an authorization may be granted for up to (b) (7)(E) beginning with the day the operation is scheduled to begin. If there is a need to continue the operation beyond the approved date, extensions for periods of up to (b) (7)(E) may be granted. The request must show the anticipated starting and ending dates of the activity.
7. **Names** – The names of the expected targeted individuals and/or enterprises in special or undercover operations must be provided, as well as the names of all operatives and their roles and responsibilities. If the operation involves a consensual telephonic monitoring, state the name of the person whose conversation will be recorded. Include the name of the case agent and the agent recording the conversation(s). If the operation involves a consensual non-telephonic monitoring, the request must give the names of persons, if known, whose communications the agency expects to intercept, and the relation of such persons to the case

under investigation or to the need for the interception. (b) (7)(E)

8. **Trial Attorney Approval** – The request must state that the facts of the investigation have been discussed with the United States Attorney, Assistant United States Attorney (AUSA), Organized Crime Strike Force Attorney, DOJ Computer Crimes and Intellectual Property Section, DOJ Child Exploitation and Obscenity Section, or other authorized prosecuting attorney for the judicial district where the activity will occur. Identify the attorney by name, and state that the attorney has specifically approved the activity (include the date of the approval). The request must also state that the attorney has expressed an opinion that the operation is not likely to cause entrapment. In the case of extension requests, the case agent must re-contact the trial attorney and verify the attorney’s continued approval. The date of this contact must be reflected in the extension request memorandum.
9. **Potential for Criminal Activity by Cooperating Individual** – The request must include a discussion of anticipated activity during the operation which would constitute a crime under Federal, state, and/or local law if engaged in by a private person without approval of an appropriate Government official, and a proposal that addresses the potential criminal activity.
10. **Potential for Law Enforcement Officer (LEO) Criminal Activity** – The request must state the nature of any criminal activity that the LEO may become engaged in as part of the operation. This section must include a statement that the AUSA is aware of this potential criminal activity and has approved its use within this operation. (b) (7)(E)
11. **Unusual Expenses** - If it is anticipated that the operation will incur expenses that are above normal costs of business, the request must show the projected costs in detail; include travel, per diem, supplies, and equipment necessary for the operation.

B. Emergency Requests

1. In emergency situations, SACs may seek authorization from the Assistant Inspector General for Investigations (AIGI), the DAIGI by telephone. The SAC is responsible for ensuring that the appropriate written request is submitted to HQ within two working days after the emergency request is authorized.
2. “Emergency situations” are those where there is a potential threat to life or of bodily injury, or where failure to act could mean the destruction of essential evidence or the escape of a fleeing offender.
3. If the undercover operation for which the emergency request is made involves one of the “sensitive circumstances” described in the CIGIE Guidelines on Undercover Operations, the AIGI or DAIGI shall attempt consultation with the Chairperson of the URC, as well as with any appropriate prosecutor and FBI manager prior to authorizing the undercover operation.
4. Except in emergency situations, no Undercover Operation will be undertaken without the prior approval of the HQ ORC.

- A. The HQ desk officer responsible for the FD will prepare a Form OI-42, Action Memorandum (see [Exhibit 7-4](#)), when requests for approval of Undercover Activities or Operations are received. If the operation will extend beyond six months or involves sensitive circumstances (see [007.010 F](#)), the SAC CID will discuss the forwarding of the application to the CIGIE URC with the DAIGI.
- B. The ORC, which consists of four members (AIGI or DAIGI, SAC or ASAC of CID, SAC or ASAC of the Intelligence and Analysis Division (IAD), and one desk officer), will review the request. For requests involving on-line or cyber undercover operations, the SAC or ASAC of the Digital Forensics Team will replace the SAC or ASAC of IAD on the ORC. The AIGI or DAIGI always serve as the senior member of the ORC. The ORC shall weigh the risks and benefits of the operation, giving careful consideration to the following factors:
1. the risk of personal injury to individuals, property damage, financial loss to persons or businesses, damage to reputation, or other harm to persons;
 2. the risk of civil liability or other loss to the Government;
 3. the risk of invasion of privacy or interference with privileged or confidential relationships; and
 4. the risk that individuals engaged in undercover operations may become involved in illegal conduct, such as participation in any act of violence except in self-defense or initiation, or instigation of any plan to commit criminal acts where entrapment could be raised as a legal issue.
 5. The suitability of Government participation in the type of activity that is expected to occur during the operation, and, when applicable:

(b) (7)(E)

(b) (7)(E)

- C. The desk officer will convey a decision on the matter to the requesting SAC. The original approved OI-42 and supporting memorandum will be retained by the SAC CID.

007.040 Use of SSA Employees in Field or Undercover Operations

- A. Special considerations when using SSA employees in Field or Undercover Activities/Operations:
1. Use of SSA employees in Field or Undercover Activities/Operations should not be considered if other effective means of securing the desired information/evidence are available.
 2. All available physical protection must be afforded SSA employees involved in special operations. (b) (7)(E)
 3. The participation of SSA employees in Field or Undercover Activities/Operations shall be strictly voluntary. Prior to any operation, the SSA employee is required to execute a Consent

to Monitor Telephone Conversations (*Form OI-25L*, [Exhibit 7-5](#)) and/or a Consent to Monitor Non-Telephone Conversations (*Form OI-25AL*, [Exhibit 7-4](#)), as appropriate.

4. To the extent possible, SACs/ASACs/RACs shall ensure that the background of an employee used in a special operation is free of information that could later be used to discredit the employee's testimony.
- B.** When an SSA employee consents to the interception of his/her verbal communications, the recording device may be hidden on his/her person, within personal effects, or in a fixed location.
- C.** The Special Agent (SA) engaging in such consensual interceptions must ensure that the consenting employee will be present at all times when the device is operating. In addition, the SA must ensure:

(b) (7)(E)

007.050 Monitoring Field or Undercover Operations

- A.** An ASAC/RAC or Resident Agent (RA) will monitor each approved Field or Undercover Operation.
- B.** The duties of the ASAC/RAC/RA monitoring the operation will include:
1. supervising the operative(s), as approved by the SAC;
 2. reviewing activity reports;
 3. transmitting instructions and information to the operative(s);
 4. consulting with the U.S. Attorney's Office throughout the operation;
 5. ensuring that the processes leading to successful conclusion of the operation are followed;
 6. ensuring that the security of the operation is maintained; and
 7. expeditious handling of any problem situations that may arise.
- C.** The AIGI or other designated official shall consult with the Chairperson of the URC whenever a serious legal, ethical, prosecutive or departmental/agency policy question arises in any undercover operation, or if sensitive circumstances occur that were not anticipated. The Chairperson and AIGI shall consult with the appropriate prosecutor, or DOJ representative on whether to modify, suspend, or terminate the investigation related to such issues.

- D. When unforeseen sensitive circumstances arise, the AIGI shall submit a written application to the URC for authorization to continue the undercover operation previously approved, or amend the existing application.
- E. As soon as the proceeds from any undercover operation are no longer necessary, the ASAC/RAC must contact HQ/CID for the appropriate disposition of funds.

007.060 Reporting the Results of Undercover Operations

The SAC will provide an OI-24A, Report of Intercept, for the DAIGI (see Chapter 8, *Exhibit 8-1*), within 10 working days of completion of the operation, including the following details for each conversation monitored:

1. the degree to which the objectives of the operation were met;
2. the performance of the operatives and investigators involved;
3. the value of the information developed; and
4. the cost of the operation.

007.070 (b) (7)(E)

(b) (7)

[Redacted text block containing multiple paragraphs of information obscured by black bars.]

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

E. (b) (7)(E) [Redacted]

F. (b) (7)(E) [Redacted]

G. (b) (7)(E) [Redacted]

H. (b) (7)(E) [Redacted]

I. (b) (7)(E) [Redacted]

J. (b) (7)(E) [Redacted]

(b) (7)(E)

K. (b) (7)(E)

1. (b) (7)(E)

(b) (7)(E)

2. (b) (7)(E)

L. (b) (7)(E)

1. (b) (7)(E)

2. (b) (7)(E)

3. (b) (7)(E)

007.080 Mail Covers

A. A mail cover is used to record information on the outside container, envelope, or wrapper of mail, including the name and address of the sender and the place and date of postmarking. Obtaining information from the cover of a piece of mail from a Postal Inspector or any other postal employee, without an authorized mail cover, is illegal and can jeopardize a case that goes to court.

B. Mail covers may be authorized (b) (7)(E)


- F.** A mail cover request must be sent in writing to the Postal Inspection Service's Inspection Service Operations Support Group (ISOSG). The entire United States Postal Inspection Service (USPIS) Mail Cover Program (see [Exhibit 7-6A](#) for USPS Procedures-Mail Cover Requests) for the United States is managed by the Criminal Investigations Service Center located in Chicago, Illinois. All Mail Cover Requests should be sent to the following address using a standard transmittal letter (see [Exhibit 7-6B](#)), irrespective of geographic location:

CISC Manager
Attn: MC Specialist
433 W. Harrison St., Room 3255
Chicago, IL 60699-3255
(312) 669-5673

- D.** Where an emergency exists, the Postal Inspector in Charge of the area or designee may grant a mail cover based on an oral request. While the mail cover data will be released immediately, the requesting agency must submit a written request for the mail cover within three business days to the ISOSG.

- E.** A mail cover request (see [Exhibit 7-6C](#)) must contain the following:

1. the reason the mail cover is needed to locate a fugitive or to obtain information regarding the commission of or the attempted commission of a felony;
2. full name and complete address of the subject;
3. classes of mail to be covered, including reasons for any class other than First-Class;
4. how long the mail cover is to be in effect (mail covers are usually authorized for (b) (7)(E), and extensions are available);
5. laws suspected of being violated, including legal citations and penalties;
6. whether the subject has been indicted and whether the subject has an attorney (if so, the attorney's name and address must be included);
7. how often the mail cover data is needed (daily, weekly, or less frequently); and
8. any additional circumstances relevant to the investigation.

- F.** Information from a mail cover often provides valuable investigative leads. (b) (7)(E)
- 

007.090 Witness Identification of Subjects

- A. In-Person Lineups**

1. For the purpose of this chapter, a “lineup” is defined as a controlled environment in which a witness can be given an unencumbered opportunity to establish positive identity of a subject in a crime.
2. SAs are authorized to conduct and actively participate in lineups after consulting with, and receiving guidance from the prosecuting attorney’s office.

B. Photo Lineups

1. Photo lineups (photo spreads) offer an alternate means for establishing witness identification.
2. In the investigative stage, subjects have no constitutional right to counsel when their photos are included in a photo lineup. However, before showing a photo lineup at the custodial stage or “defendant” stage, SAs should contact the appropriate prosecuting attorney for an opinion. Some judicial districts have ruled that an individual at this stage may be entitled to have counsel present at the showing of a photo lineup. Other judicial districts have ruled that if the suspect is in custody and accessible, a physical lineup should be employed rather than a photo lineup.
3. SAs should adhere to the Photo Lineup Guidelines (see [Exhibit 7-7](#)) when presenting a photo lineup.
4. Written statements should be taken when a witness makes a positive identification.

007.100 Polygraph

- A. OI has the capability to support criminal investigations through the use of polygraph examinations provided by certified Federal polygraph examiners. The polygraph is intended as a tool to assist SAs in their criminal investigations; it is not intended to replace a thorough field investigation, nor will it be used as a psychological prop for an interrogation. See [Exhibit 7-8](#) for the standard operating procedures for polygraph examinations.
- B. OI personnel will not engage in the use of polygraphs without the specific authorization from the CID SAC.
- C. Any request for such authorization will be directed, in writing, to the CID SAC by the FD SAC/ASAC/RAC. The OI Polygraph Examination Request Worksheet is the document used to make the request (see [Exhibit 7-9](#)).
- D. Travel and per diem costs incurred by the examiner assigned to conduct the polygraph examination in support of OI investigations are the responsibility of OI HQ, not the FD.
- E. It is the responsibility of the case SA who initiates the polygraph examination request to:
 1. secure the examinee’s permission to undergo the examination;
 2. arrange for a suitable location for the examination;
 3. arrange for logistical support of the examiner; and
 4. make every effort to have the examinee available at the scheduled time.

- F. No requests should be made for mass screenings of subjects or for an examiner to travel to a location to be on “stand-by” awaiting investigative developments that may lead to an examination.

007.110 Electronic Sources of Information

- A. The following list of information sources is not meant to be all-inclusive. It is a basic guide for SAs to utilize in conducting inquiries. A comprehensive document entitled, “Investigators Guide to Sources of Information” published by the Government Accountability Office (GAO), may be accessed through the GAO website <http://www.gao.gov/>.
- B. The Federal Bureau of Investigation (FBI) operates an information sharing network known as Law Enforcement Online (LEO). LEO is a virtual private network provided by the FBI to all levels of the law enforcement, criminal justice, and public safety communities. In addition to information sharing, LEO is a system for secure electronic communications and online training. The LEO Special Topics Index allows members to share information regarding new investigative programs and sources of information. The LEO Multimedia Library provides a large repository of publications, documents, and technical bulletins of interest to law enforcement personnel. In order to gain access to this system, users must contact: FBI, Attn: LEO Program Office, 935 Pennsylvania Ave., NW, Washington, DC 20535 (phone 202-324-8833 or email leoprogramoffice@leo.gov).
- C. **National Crime Information Center (NCIC)/National Law Enforcement Telecommunications System (NLETS)**
 - 1. NCIC is a restricted nationwide computerized information system that primarily provides criminal history information on individuals convicted of State and Federal felony offenses. (See [Exhibit 7-20](#) for detailed information on the NCIC.)
 - a. Negative responses do not necessarily indicate the absence of a criminal record. Participating agencies are strongly encouraged, but not compelled, to enter arrest and/or judicial information into NCIC. As such, not all relevant information is entered into NCIC.
 - b. Arrests for misdemeanor charges are very rarely included on the record of a requested individual.
 - 2. NCIC also contains information regarding stolen property, including vehicles, boats, license plates, securities, guns, and other stolen articles with unique identifiers and valued over \$500.
 - 3. Warrants issued in SSA OIG cases can be entered into NCIC by the local U.S. Marshals Service office. Agents should complete [Exhibit 7-18](#), “NCIC Data for USMS,” and present it to their local U.S. Marshals Service office.
 - 4. All personnel who conduct criminal history inquiries through NCIC are responsible for ensuring that the recipient is authorized to receive the data.

- a. Criminal history information that is not known to be public information **may not** be disseminated to non-criminal justice agencies or to sections within the OIG that are non-criminal justice in nature; for example, the OIG Office of Budget.
 - b. Criminal history information **may** be disseminated to:
 - 1. Criminal justice agencies, such as courts, other IG offices, State and Federal law enforcement agencies, United States Attorney's Offices; or
 - 2. agencies or subunits thereof that perform the administration of criminal justice, such as judges, the SSA Office of Disability Adjudication and Review (ODAR), and Disability Determination Services (DDS) units.
 - c. All secondary dissemination must be recorded in the log maintained by the office. The requestor's name should be placed in the attention field of the inquiry. The name of the agency should also be included if the inquiry is conducted for someone outside of the OIG.
 - d. For specific dissemination concerns, consult with the Office of Counsel to the Inspector General (OCIG).
5. Instructions on destroying criminal history queries when a case is closed can be found in Chapter 11 Section [011.030 C.3](#).
6. NLETS is a restricted national computerized system that provides law enforcement agencies the capability to exchange narrative criminal justice-related information interstate on a 24-hour basis through an administrative message format. NLETS also provides such information as (b) (7)(E)
-
7. **Routine Request Procedures** – All requests for NCIC/NLETS information must be documented on Form OI-43, "Request for NCIC/NLETS Records Checks" (see [Exhibit 7-10](#)).
- a. The original OI-43 completed by the computer operator must be filed in a standard ring binder at the computer workstation where the information was accessed.
 - b. A copy of the completed OI-43 and the results of the request must be maintained in the case file.
8. **Urgent Request Procedures** - In the event that an SA requires an immediate NCIC/NLETS inquiry during off-duty hours, or in emergencies, assistance can be requested from U.S. Customs' Sector, utilizing the protocol outlined in the instructions relating to radio communications.

D. TECS Database

1. TECS is a database of enforcement data that contains border security and law enforcement related information supplied by the Department of Homeland Security (DHS) and other Federal agencies. The DHS' U.S. Customs and Border Protection (CBP), serves as the system manager for TECS. OI is a user agency that has been granted access to TECS through a TECS Memorandum of Understanding (MOU). For practical information on TECS, see the [TECS HUB SharePoint](#).
2. OI must comply with the current TECS Data Standards for the transmission of data to TECS, including any subsequent revisions of those standards. OI must also comply with the appropriate administrative security provisions and any other relevant directives and regulations for the access, use, and handling of applicable TECS information. OI TECS users must abide by the standards set forth in the [TECS MOU](#).
3. OI's Intelligence and Analysis Division (IAD) will designate a National System Control Officer (NSCO) to serve as the single point of contact within OI for TECS access and use.
 - a. The NSCO will be responsible for developing and implementing SSAOIG policy for TECS use and coordinating the designation and assignment of TECS access for all employees in SSAOIG. Further, the NSCO will be responsible for assigning and maintaining profiles for OI users, and will serve as the authorized contact with CBP to add, revise, and archive OI TECS users in accordance with established OI and CBP policies and procedures.
 - b. Each OI field division will designate Local SCOs (LSCOs) who will serve as authorized contacts with CBP and will be responsible for adding, revising, and archiving OI TECS users within their field division in accordance with policies and procedures established by the NSCO.
 - c. The OI NSCO/LSCOs will be responsible for keeping their accounts in active status by completing the TECS Security and Privacy Awareness (TSPA) course yearly and logging into the TECS system regularly (at least every 30 days).
4. Requests for access to TECS will be completed on a [Request for TECS Access](#) form, available on the [TECS Hub SharePoint](#). The requestor must have a valid need for access to TECS (i.e., investigative duties), as certified by supervisor's approval, and a current background investigation, in accordance with the TECS MOU. After obtaining supervisory approval, the requestor will send the request form to their LSCO (The NSCO and LSCOs are identified on the [TECS HUB SharePoint](#)). The LSCO will ensure that the requestor has a current Level 3 Background Investigation, as verified by the list provided by the NSCO. If the requestor meets all requirements, the LSCO will set up a new TECS User account and will forward the completed TECS Access Request form to the NSCO.

NOTE: Student interns, state employees, contract employees, and seasonal/temporary employees WILL NOT have access to TECS. TECS access is limited to OI criminal investigators (supervisors/agents), criminal research specialists, and investigations/intelligence analysts.

5. All TECS users must abide by the provisions outlined in CBP's TECS Privacy Awareness course (TPA course). Compliance will be verified through the completion of the online CBP TPA course and passing of the TECS certification test. After successful completion of the

automated test, OI's National SCO will create a User Profile Record (UPR), establishing the user's account providing access to TECS. In addition, all TECS users must complete SSA's annual IT security awareness training.

- a. Based on their role as custodian of both the data and the processes in TECS, CBP is required to document all security infractions. OI's National SCO will notify the TECS application owner, who will report it to CBP's Internal Affairs. If a violation occurs, the National SCO must be notified immediately by sending an email to the ^OIG PAD mailbox, detailing the security violation. **NOTE: All TECS violations will be reported to OI's National SCO using the ^OIG PAD mailbox. The National SCO will notify CBP, who will refer the violation to CBP Internal Affairs.**

6. OI TECS users will be authorized access to the following categories of records:

(b) [REDACTED]

7. OI TECS users will be authorized access to the following functions:

(b) [REDACTED]

(b) [REDACTED]

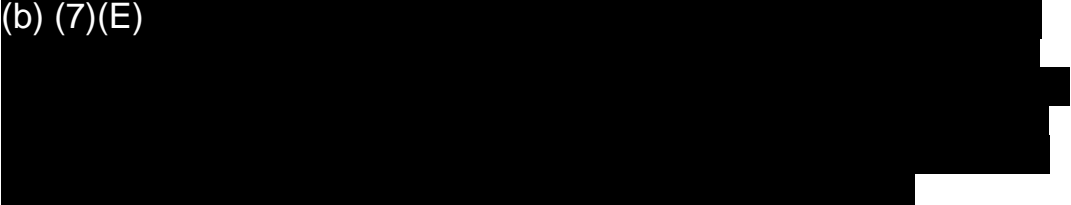
E. Financial Crimes Enforcement Network (FinCEN)

1. FinCEN provides intelligence and analytical support to law enforcement. The Agency's information sources fall into three broad categories:
 - a. **Financial** - This database contains reports that are required to be filed under the Bank Secrecy Act and include Currency Transaction Reports (CTR), Report of International Transportation of Currency or Monetary Instruments (CMIR), Currency Transaction Report by Casinos (CTRC), and Reports of Foreign Bank and Financial Accounts (FBAR). FinCEN also has access to data from IRS Form 8300 (Reports of Cash Over \$10,000 Received in a Trade or Business). Furthermore, FinCEN has access to Suspicious Activity Reports (SAR) filed by banks and other depository institutions upon suspicion that one or more of various financial crimes may have been perpetrated in or against the financial institution.
 - b. **Law Enforcement** - Through a series of written agreements outlining details of database access and dissemination authority, FinCEN is able to access individual law enforcement databases maintained by agencies such as the U.S. Treasury Bureaus and the Drug Enforcement Administration (DEA).
 - c. **Commercial Databases** - FinCEN procures access to numerous commercially maintained databases which are valuable in locating individuals, determining ownership and establishing links between individuals, businesses, and assets, including CDB-Infotek (public filings) and Equifax (credit information).
2. **Procedures** – The SSA OIG may request assistance from FinCEN by submitting a FinCEN Request for Information Form (see [Exhibit 7-11](#)). FinCEN's facsimile number is (703) 905-3526.
 - a. FinCEN requires supervisory approval prior to submission of the application for information.
 - b. (b) (7)(E) [REDACTED]
3. Additional information regarding FinCEN and the services it provides may be found on its website, (b) (7)(E) [REDACTED]

F. U.S. Treasury Financial Management Service (FMS) PACER Program

1. The U.S. Treasury Financial Management Service reconciles all government checks paid by the U.S. Treasury, and maintains photocopies of the cancelled U.S. government checks. FMS can provide electronic copies of the checks to law enforcement for investigative purposes.
2. Various SSA OIG offices can access PACER and obtain front and back copies of cancelled U.S. Treasury checks. SAs should contact their ASAC/RAC for information concerning how to obtain check copies through PACER.

G. Commercial Databases

1. (b) (7)(E) 
2. SAs must obtain a user name and password from their ASAC/RAC prior to being allowed to access the commercial database system used by OI.
3. Commercial databases available to OI agents through SSA or the OIG are for official use only. Anyone who uses these systems for non-work related matters is subject to disciplinary action up to and including removal.
4. Each employee who has obtained a user name and password for access to a commercial database based on his or her employment with the OIG is required annually to complete form OI-88 Law Enforcement Systems and Commercial Database Security Acknowledgement (see [Exhibit 19](#)) acknowledging that he or she understands that the use of the database is for official use only.
5. Supervisors are required to review the transaction history for the commercial database semiannually to ensure that employees have used a database only for official purposes. The usage reviews should be conducted randomly throughout the review period so that employees do not know when they will occur.
6. Any unauthorized use of a commercial database shall be reported through the chain of command to the appropriate DAIGI within five working days following the discovery of the unauthorized use.
7. All personnel must be able to memorialize their use of commercial databases to demonstrate that access was made in the course of official business. If subjects cannot be linked to an allegation or case, they must be listed in a log maintained in the office.

H. Unauthorized Access and Disclosure of Information from Law Enforcement Information Systems and Commercial Databases


1. All unauthorized access into, and/or releases of information from, State and Federal Criminal Justice Information Systems (e.g. NCIC) and commercial databases available to employees through SSA or the OIG are serious violations. The final determination as to whether a *particular* access and/or release rises to the level of criminal misconduct only

speaks to the seriousness of the violation. Anyone who misuses a criminal justice information system is subject to discipline up to and including removal.

2. The Inspector General supports disciplinary penalties for system security violations, in addition to any criminal penalties prescribed by Federal and State laws regarding privacy of records and personal information.

I. Non-SSA Internet Lines (Stand Alone Computers in OI Offices)

The following guidance must be followed by OI personnel when using non-SSA internet lines available in OI offices equipped with stand alone workstations with commercial internet access.

1. Stand alone work stations shall be used for official business only. Due to the lack of security on those computers, OIG personnel should never access personal e-mail, their own social networking profiles, or personal accounts at financial institutions.
2. Each office with access to non-SSA internet lines shall maintain a log ([Exhibit 7-21](#)) to account for use of the internet. The log must contain the user's name, date, case or allegation number, and purpose/comments.
3. (b) (7)(E) 
4. OI field divisions are encouraged to utilize anti-virus and anti-malware software and ensure that the software is updated based on the manufacture's recommendations.
5. If any material of a probative nature is found, request assistance from the Digital Forensics Team via NICMS so the material can be forensically captured, and preserved as evidence. A print out or screen capture is not forensically sound and may not be admissible in court.

007.120 Electronic Device Forensic Examinations

- A. The Office of Investigations' Criminal Investigations Division's Digital Forensics Team (DFT) provides technical assistance, on-site support, and laboratory analysis for investigations involving electronic devices and media. Examples of electronic devices and media include computers, flash drives, CDs/DVDs, cell phones, iPads, and iPods.
- B. To obtain DFT support, an FD agent must submit a request by clicking on the "Request DFT Assistance" button on the Case Data screen in the National Investigative Case Management System (NICMS). Once completed, the request for DFT assistance will be routed to the FD ASAC/RAC for review and approval. Once the request is approved by the ASAC/RAC, the case will be forwarded to the SAC/ASAC of IAD for approval and assignment to a Forensic Analyst/Specialist. The request must contain the following: case number, name of case agent, and a description of the services requested.

- C. Agents requesting DFT support for examinations of mobile devices (cell phones, iPads, etc.) must complete a Mobile Device Inventory Worksheet, Form OI-94 (see [Exhibit 7-22](#)), and submit the worksheet to DFT along with the device to be examined. In a situation where multiple mobile devices are to be examined, a separate worksheet should be prepared for each device.
- D. DFT also provides support for employee investigations. (See *Chapter 4, Section 004.075.*)
- E. DFT has provided guidelines to the Social Security Administration (SSA) regarding the identification of child pornography on the SSA network. These guidelines provide a process for the Agency to follow once child pornography is identified and the method to follow for reporting the information to OIG. (See [Exhibit 7-12.](#))
- F. Contact information for DFT members, as well as information on how to submit evidence is contained on the OIG SharePoint under Directories>Office Directory>Digital Forensics Team.
- G. If an individual voluntarily consents to a search of a computer or electronic device in his or her lawful possession, the agent shall attempt to obtain a completed Consent to Search Computers/Electronic Media, Form OI-91 ([Exhibit 4-19](#)), from the person whose computer or device is to be searched.

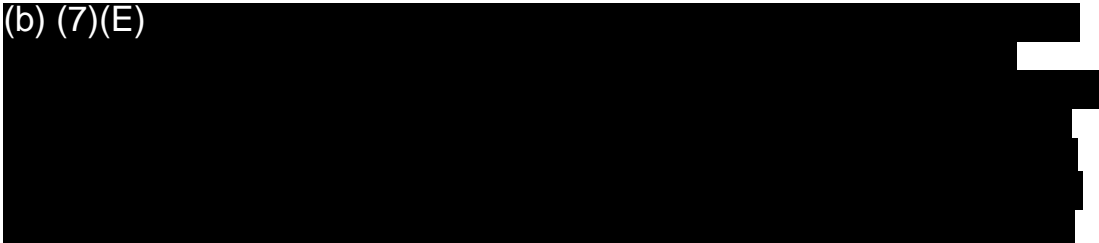
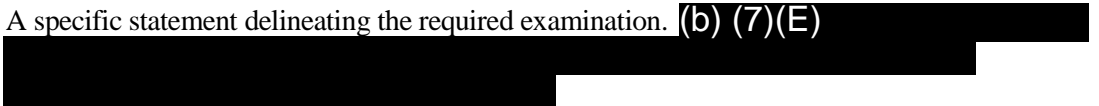
007.130 Other Forensic Examinations

- A. Investigations involving a document may require various forensic examinations. The document can be examined to determine if the signature on the document is genuine or a forgery, develop latent fingerprints, determine the approximate age of the document, and other forensic tests.
- B. SSA OIG has entered into a Memorandum of Understanding with the United States Secret Service (USSS) to provide forensic examinations and subsequent expert testimony. OI FDs requiring such forensic assistance should submit their request, along with the required documents, to CID for forwarding to the USSS.
- C. In submitting a request, OI FDs must provide the following items to CID via their assigned Desk Officer:
 1. Request for Forensic Examination memorandum to the SAC of CID, from the OI FD SAC/ASAC/RAC. The memorandum must include the date, OI case number, and reason for activity, while specifying whether the request is for handwriting or latent print examination.
 2. Letter of Request for Forensic Examination from the FD SAC/ASAC/RAC, addressed to the USSS, Special Agent-in-Charge (SAIC) of the Forensic Services Division (*Note: Contact CID for current SAIC information.*):

- U.S. Secret Service
Forensic Services Division
Attn: SAIC _____
245 Murray Lane, S.W., Bdg. T-5
Washington, D.C. 20223

3. Cover letter referencing the MOU between the USSS and the SSA/OIG, detailing forensic assistance being available to the OIG in support of criminal investigations. This letter is composed by the FD, addressed to the same USSS contact and location as above, from the SAC of CID. *(The letter must indicate what documents are enclosed for examination, the OI case agent's name and contact information, and the OI case number).*
4. Writing samples/latent prints for the USSS examiner to review. In order to issue an expert opinion, the handwriting examiner must have writing samples similar to those in question. SAs are responsible for obtaining sufficient handwriting specimens to be used for comparison purposes. Forms OI-29A and OI-29B are available for use in obtaining these specimens (see Exhibits [7-13](#) and [7-14](#)).
5. Evidence Property Report ([Form OI-21](#)), listing the description of the evidence sent. *(The OI-21 must have the "chain of custody" section completed, to show custody from the OI FD, to CID; then, CID will complete originals from CID to USSS/Forensic Services Division. After the forensic analysis is completed, the OI-21 and results of the examination will be forwarded directly from the USSS, to the address on the request for the OI FD).*

D. Requests for forensic examination should contain the following basic elements:

1. Subject and case number of the investigation.
2. (b) (7)(E) 
3. A specific statement delineating the required examination. (b) (7)(E) 
4. Procedures for obtaining proper exemplars and standards

A subject's apparent cooperation in providing exemplars should not negate the SA's effort to obtain standards as well. Both are extremely helpful to the document analyst during the examination. The following are fundamental requirements for obtaining proper exemplars and standards:

- a. (b) (7)(E) [Redacted]
- b. (b) (7)(E) [Redacted]
- c. (b) (7)(E) [Redacted]
- d. (b) (7)(E) [Redacted]
- e. (b) (7)(E) [Redacted]

007.140 Technical Investigative Equipment and Support

- A. Each field division is required to have at least one SA trained in the use of technical investigative equipment to serve as the coordinator for technical investigative equipment within the division.
- B. The ATSAC PAD at OI HQ should be contacted in the event that additional technical investigative equipment is needed on a permanent or temporary basis.
- C. Refer to Chapter 8, “Interception of Communications,” for detailed policy and procedural information regarding the use, care and storage of technical investigative equipment.

007.150 Radio Communications

- A. **Purpose** - This directive sets forth the policies and general procedures for the use of SSA OIG radios on SSA and other allocated law enforcement frequencies.
- B. **Policy** - Customs and Border Protection (CBP) operates the National Law Enforcement Communications Center (NLECC). SSA OIG has entered into a Memorandum of Understanding (MOU) with the CBP, authorizing SSA OIG access to the NLECC’s national radio communications network. SAs are permitted to use the communications network through the radio communications equipment provided by SSA OIG. The use of the communications equipment and network shall be in accordance with the procedures provided in this directive.

C. Background

1. During criminal investigative operations, SAs are involved in various activities, including arrests, surveillance, court ordered searches, consensual monitoring, etc. It is often necessary to obtain motor vehicle or computer system wants/warrant information on subjects. Emergencies may arise during the course of an investigation where SAs need to request immediate assistance. For each of these reasons, it is necessary for SAs to have access to a radio communications system.

2. (b) (7)(E) [Redacted]

3. (b) (7)(E) [Redacted]

D. Definitions

1. **Simplex/Direct Operation (Radio to Radio)** - Communicating from one radio to another radio utilizing one frequency. Both radios transmit and receive on the same frequency (e.g., car-to-car communications).
2. **Talk Around** - This is a simplex operation with the transmission and reception of a signal on the repeater's output frequency. This allows for localized tactical operations of limited geographic scope (e.g., surveillance). This enables users to receive strategic communications without interfering with the repeater.
3. **Duplex Operation** - Describes a radio transmission on one frequency to a repeater. The repeater receives the transmission and immediately re-transmits it on a second frequency. The use of a repeater allows for a much broader geographic coverage (approximately a 30-mile radius) due to its increased power output and the location of the antenna.
4. **"In the Clear" Communication** - Describes a non-encrypted communication.
5. **Microprocessor Radio Telephone Interconnect (MRTI)** - This device allows SECTOR to connect a radio transmission from a repeater in one geographical area to a repeater in another geographical area.

6. **Regional Communications Officer (RCO)** - Each Field Division will have at least one RCO. The RCO is responsible for coordinating all radio communications activities within the field office's area of responsibility.
7. **National Communications Officer (NCO)** - The NCO is responsible for coordinating all radio communications activities for SSA OIG, including coordination with outside agencies.
8. **Radio Network User Registration** – A mandatory form (see [Exhibit 7-15](#)) that updates radio and SA identification information. CBP requires that the form be completed quarterly and forwarded to them CBP as part of their continuing radio security measures.

E. Regional Communications Officers (RCO)

1. The RCOs are responsible for:
 - a. Ensuring that each SA in his/her respective field division completes an **updated** Radio Network User Registration (RNUR) form each quarter.
 - b. Completing a RNUR form for each spare radio (serial number and UID) with its location (field division, field office, etc.).
 - c. Providing a list of any spare radio parts, including vehicle adapters, on hand in their field divisions.

F. Observations

1. The maximum effective range of a radio is limited. The range is based on placement of the antenna coupled with the power output of the radio. A radio installed in a vehicle has a significantly greater range (approximately a 25-mile radius) than a handheld radio (approximately a 6-mile radius). At times, transmissions may be garbled, or difficult to understand. SAs may enhance communications by considering the following:
 - a. move to a higher position (e.g., hilltop, higher building floor, etc.);
 - b. move away from obstructions (e.g., tall buildings);
 - c. avoid valleys, power lines, large steel structures, underpasses and leafy trees;
 - d. move toward moist ground or a body of water; or
 - e. with handheld radios, move from the interior of a building to a window.
2. When using radio equipment, SAs should use plain language to get the message across with the minimum amount of time. Some standard radio responses have been incorporated into a numerical code, commonly referred to as the 10-Code. When utilizing the 10 Code on SSA OIG or CBP frequencies, SAs will use the CBP 10 Code (see [Exhibit 7-16](#)).
3. The clarity of words transmitted over the radio is often garbled and difficult to understand. This is especially true when transmitting letters (e.g., license plates). Radio operators have developed phonetic alphabets consisting of one word beginning with each letter of the alphabet. (b) (7)(E)

(b) (7)(E)

G. Care and Use of Radios

1. All communications are **for official use only**.
2. All SAs issued a radio will also be assigned a radio call sign. SAs must use their designated call signs during all radio communications.
3. SAs must exercise proper radio protocol at all times. Failure to do so could lead to adverse action against SSA OIG, the SA, or both.
4. SAs are responsible for the security of the radios at all times, and must prevent unauthorized use.
5. SAs are prohibited from adding or removing frequencies, or attempting to make radio repairs. All repairs must be coordinated through the RCO.
6. SAs must report the loss of a radio to SECTOR **immediately** upon discovering that the radio is unaccounted for to ensure the radio is disabled without delay. Subsequently, SAs must report, as soon as possible, the loss of a radio to their immediate supervisor, who must then notify the appropriate Special Agent-in-Charge. At first opportunity, the SAC must submit a written account of the circumstances surrounding the loss to the NCO, and make certain the appropriate survey report is completed.
7. Under the agreements with CBP and other agencies, SSA OIG cannot grant radio communication access to non-law enforcement personnel.
8. (b) (7)(E)
9. Radios and radio equipment should not be transferred from office to office. They are to remain in the office to which they were originally assigned, unless the radio and all of its associated equipment, including the Vehicle Adapter, are also transferred. The FD RCO must be notified when a pending transfer of radio equipment is being considered. The RCO must then notify the NCO at HQ of the circumstances regarding this transfer of radio equipment. The NCO is the sole authority for the transfer of radio equipment.

H. Radio Etiquette and Emergency Procedures

1. If an emergency is declared on a radio frequency, SSA OIG SAs not involved in the situation should discontinue using that particular radio frequency until the situation has been resolved. Accessing that frequency will only interfere with those assisting in the emergency response.
2. When accessing a radio frequency, listen for a broadcast and look for the red transmission light. This quick survey will allow SAs to determine if the frequency is clear. If so, the microphone can be actuated to begin a transmission.

3. SAs will use their assigned call signs for identification.
4. Offensive language or slang is prohibited.
5. If SAs need emergency assistance, the following should be stated clearly: **“I have an emergency situation!”** This statement alerts all parties that an emergency exists, and serves to clear the frequency for specific requests for assistance.
6. SAs should identify themselves in plain language, state their location, and describe the nature of the emergency.
7. When using the CBP and SSA OIG frequencies in an emergency, SECTOR assumes control of the frequency. SECTOR will notify the appropriate emergency services (e.g., local police, ambulance, fire, etc.) to render assistance.
8. Once the situation is under control, SAs should immediately declare the emergency over. SECTOR will continue to treat the situation as an emergency until told otherwise.

I. Customs and Border Protection Support

CBP provides the following communication services to SSA OIG:

1. Continuous monitoring of the NLECC VHF radio network for officer safety purposes.
2. Emergency service requests, including emergency medical, rescue coordination, law enforcement back-up and/or message relays when emergency communications or telephones are not available (e.g., contacting a supervisor at home).
3. Pursuit coordination for vehicle, vessel, and/or aircraft chase support.
4. Support services for transporting prisoners or a member of the opposite sex. SAs may ask SECTOR to document time and mileage at the beginning and end of a transport. SECTOR will also conduct safety checks during the course of the transport.
5. Communications and coordination support for surveillance, convoy, or tracking activities.
6. Support services for high-risk situations, including vehicle stops, vessel boarding, aircraft searches, warrant services, high-risk interviews, etc. This includes radio network monitoring of the situation for officer safety, officer call back status checks, and law enforcement database inquiries.
7. Law enforcement database inquiries include on-air queries of NCIC, NLETS, TLETS, Street Atlas and PhoneDisk.
8. Provide system historical transaction data (a printout of SECTOR’s tapes and logs). The system will automatically record and maintain a record of all transmissions for seven days. This request must be directed through the NCO.
9. Radio and telephone paging and patching service is available on a critical need basis (e.g., contacting a supervisor at home). SECTOR will not conduct calls of a personal nature.

J. Communications Security

1. (b) (7)(E) [Redacted]
2. (b) (7)(E) [Redacted]
3. (b) (7)(E) [Redacted]
4. (b) (7)(E) [Redacted]
5. (b) (7)(E) [Redacted] :
 - a. (b) (7)(E) [Redacted]
 - b. (b) (7)(E) [Redacted]
 - c. (b) (7)(E) [Redacted]
 - d. (b) (7)(E) [Redacted]

K. Frequencies

1. (b) (7)(E) [Redacted]
 - a. (b) (7)(E) [Redacted]
 - b. (b) (7)(E) [Redacted]

- c. (b) (7)(E) [redacted]
 - d. (b) (7)(E) [redacted]
2. (b) (7)(E) [redacted] :
- a. (b) (7)(E) [redacted]
 - b. (b) (7)(E) [redacted]
 - c. (b) (7)(E) [redacted]
 - d. (b) (7)(E) [redacted]
3. (b) (7)(E) [redacted]

EXHIBITS

- [7-1 — Tactical Plan: Surveillance, Undercover, Arrest \(OI-17\)](#)
- [7-2 — Tactical Plan for Search Warrants \(OI-18\)](#)
- [7-3 — Consent to Monitor Non-Telephone Conversations \(OI-25AL\)](#)
- [7-4 — Action Memorandum \(OI-42\)](#)
- [7-5 — Consent to Monitor Telephone Conversations \(OI-25L\)](#)
- [7-6 — Federal Agency Agreement](#)
- [7-6A — USPS Procedures–Mail Cover Requests](#)
- [7-6B — Mail Cover Transmittal Letter \(IO-71\)](#)
- [7-6C — Request for Mail Cover \(official USPS version\)](#)
- [7-7 — Photo Lineup Guidelines](#)
- [7-8 — OI Standard Operating Procedures for Psychophysiological Detection of Deception](#)
- [7-9 — OI Polygraph Examination Request Worksheet](#)
- [7-10 — Request for NCIC/NLETS Records Checks \(OI-43A\)](#)
- [7-11 — FinCEN Request for Information](#)
- [7-12 — Guidelines for Suspected Child Pornography on Agency Networks](#)
- [7-13 — Handwriting Sample \(OI-29A\)](#)
- [7-14 — Handwriting Specimen \(OI-29B\)](#)
- [7-15 — Radio Network User Registration Form](#)
- [7-16 — \(b\) \(7\)\(E\)](#)
- [7-17 — \(b\) \(7\)\(E\)](#)
- [7-18 — NCIC Data for USMS](#)
- [7-19 — Policy for Law Enforcement Information Systems and Commercial Database Access](#)

and Law Enforcement Systems and Commercial Database Security Acknowledgement

7-20 — National Crime Information Center Information

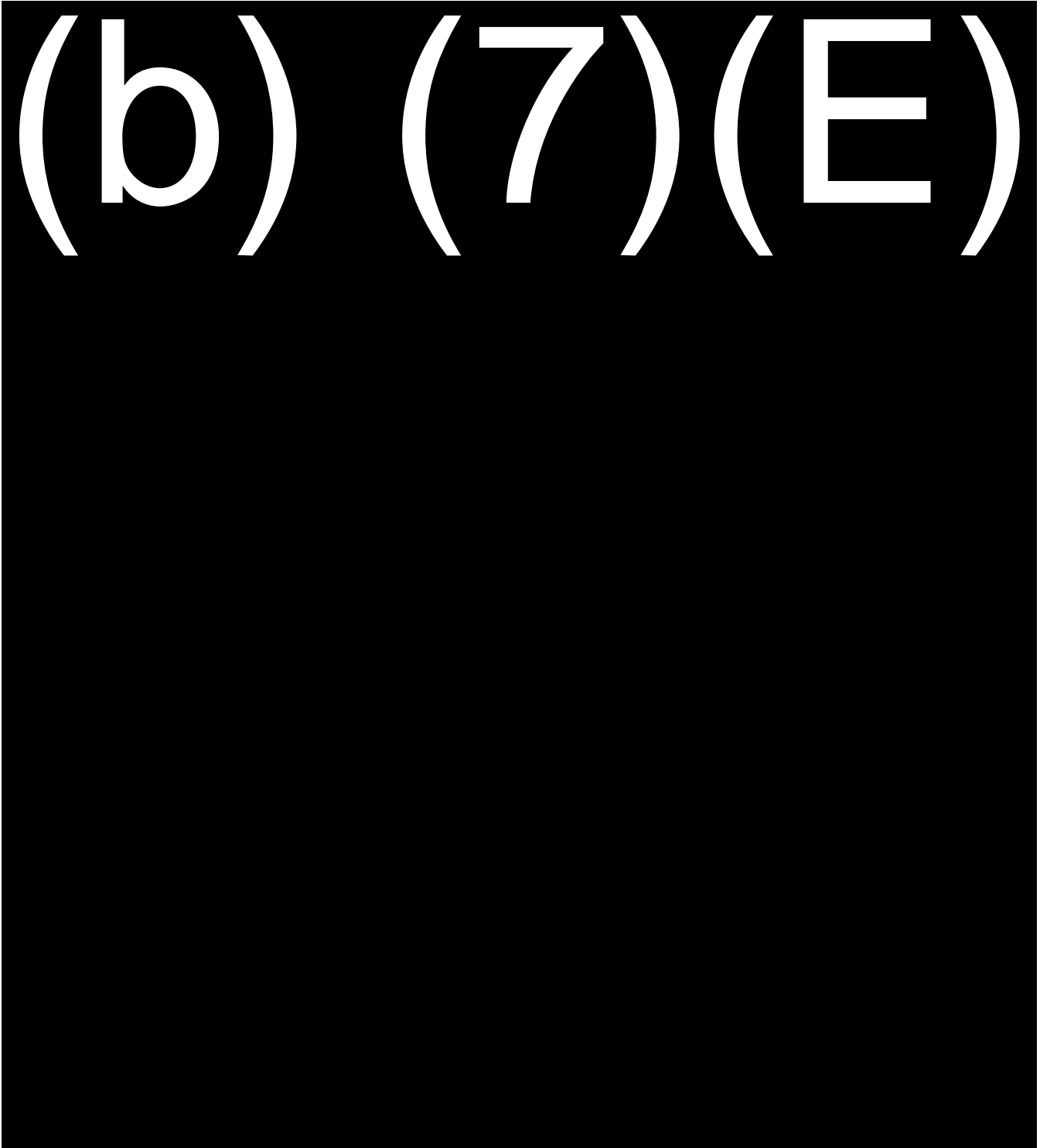
7-21 — Non-SSA Internet Access Log

7-22 — Mobile Device Inventory Worksheet (Form OI-94)

SOCIAL SECURITY

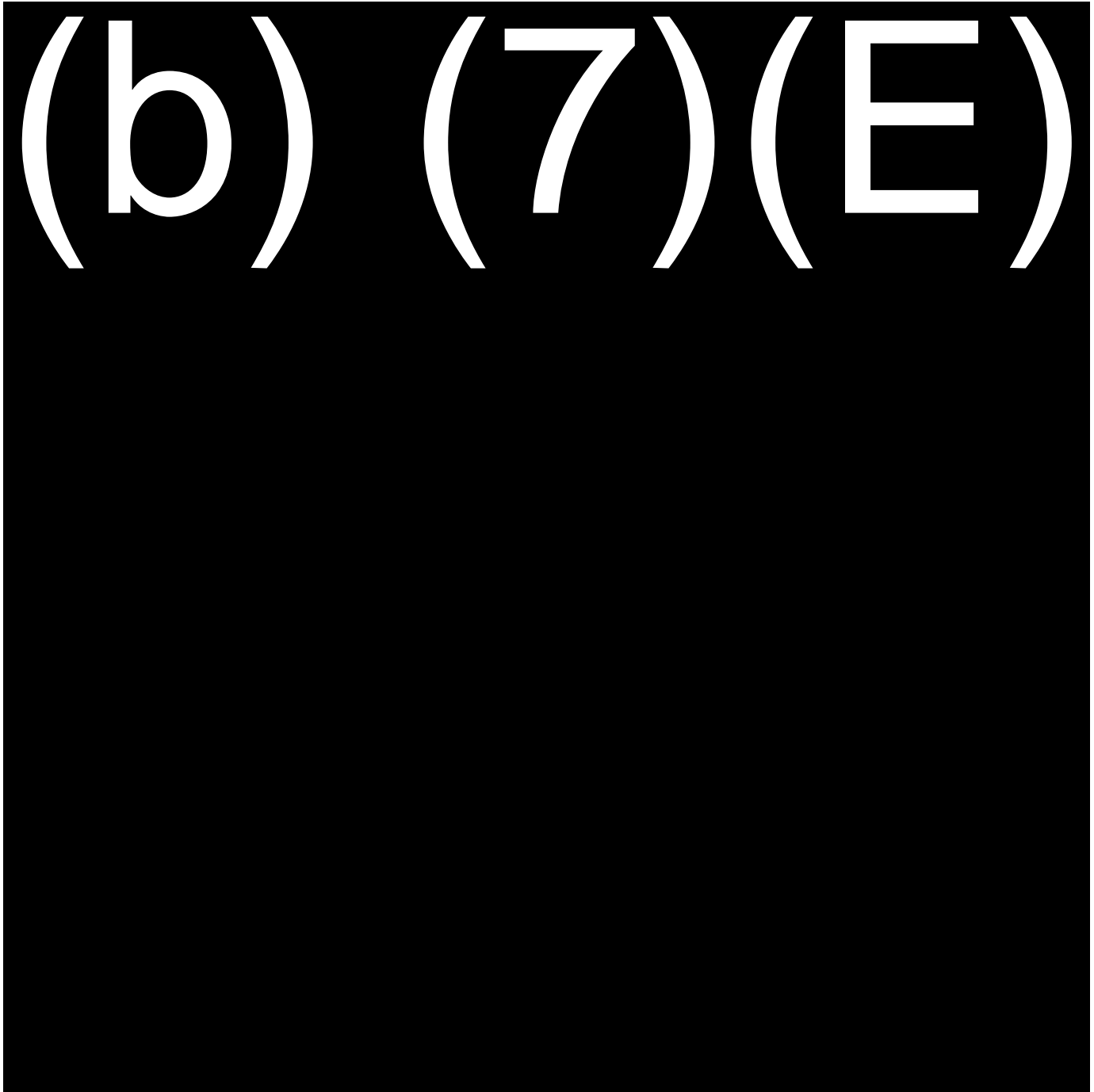
Office of the Inspector General

TACTICAL PLAN: SURVEILLANCE, UNDERCOVER, ARREST



This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General



This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY

Office of the Inspector General

INSTRUCTIONS FOR COMPLETING FORM OI-17

(TACTICAL PLAN: SURVEILLANCE, UNDERCOVER, ARREST)

MANDATORY FORM

(b) (7) (E)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

Tactical Plan for Search Warrants

(b) (7) (E)

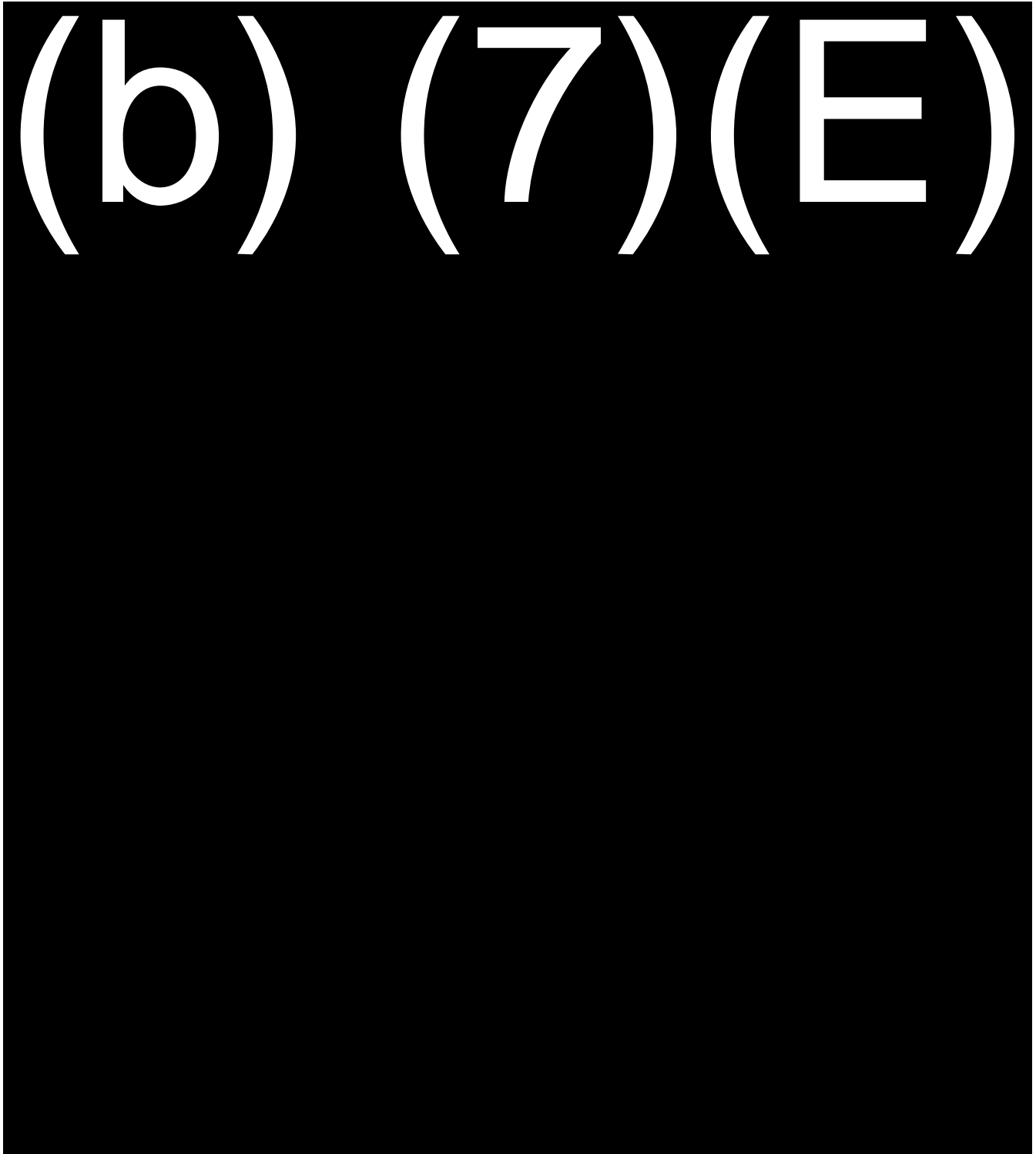
This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General



This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

ACTION MEMORANDUM					
To:	Office of Origin:	Date:			
	From:				
Subject:					
Attachments:					
Copies To:					
	Prepared by:	Cleared by:	Cleared by:	Cleared by:	
Surname Title					
Initials Date					File Number

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

Consent to Monitor Telephone Conversations

Date: _____

Location: _____

I, _____, _____ hereby (Name)
(Address)
authorize _____ and _____, Special Agents
(Name) (Name)
of the Office of Investigations, Office of the Inspector General, Social Security Administration,
to install a recording device on a telephone number

_____ located at _____
(Telephone #) (Location)

for the purpose of recording any conversation I may have on that telephone with

_____ on _____
(Name) (Date)

at/about _____.
(Time)

I have given this permission to the Special Agents named above voluntarily and without threats, pressure, or promises of any kind.

(Print Name)

(Signature)

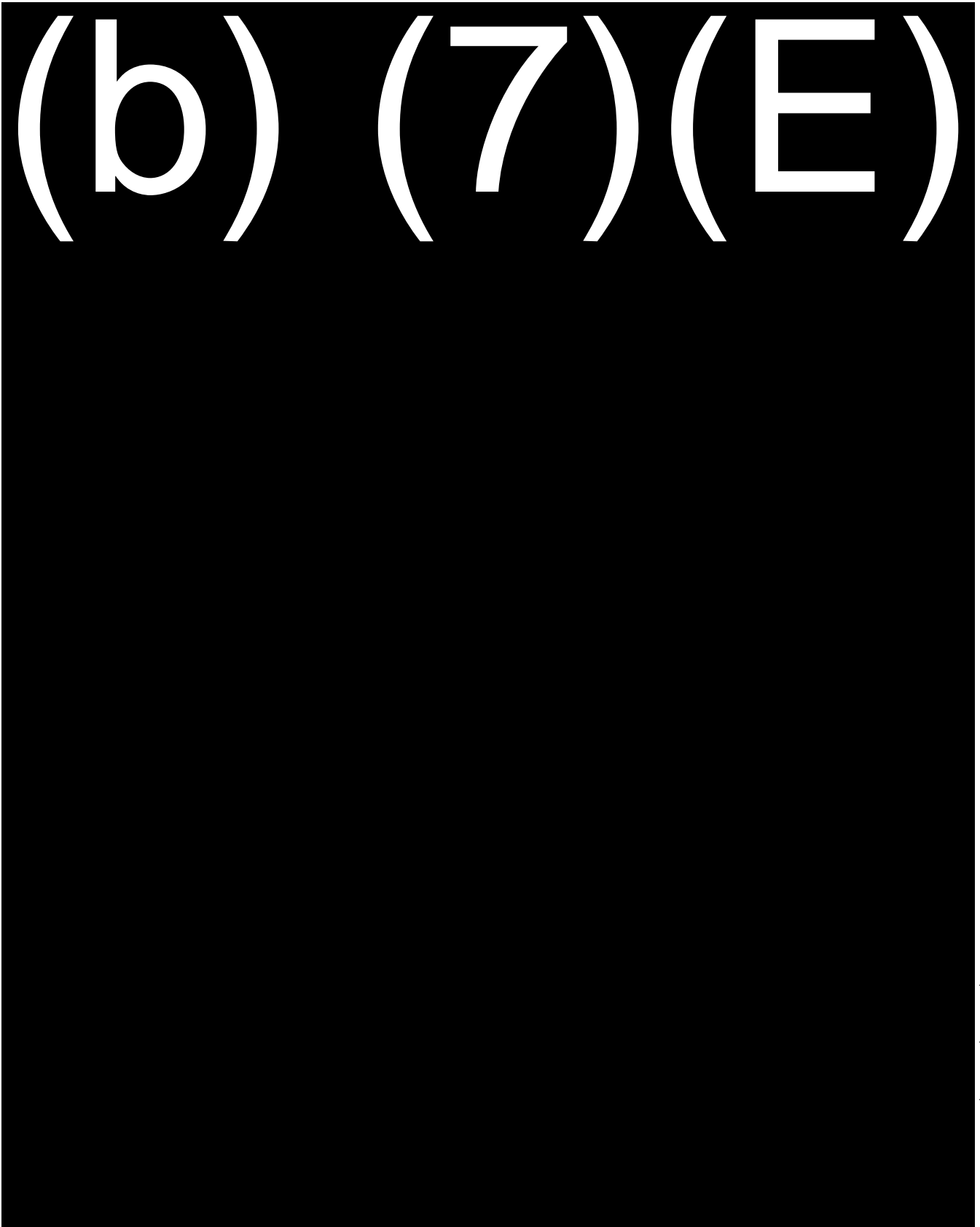
Witnesses:

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

FEDERAL AGENCY

AGREEMENT

(b) (7) (E)



FEDERAL AGENCY

ENDORSEMENT

(b) (7) (E)

NOTHING FURTHER FOLLOWS ON THIS PAGE
ON THE REVERSE OF THIS PAGE IS THE AGREEMENT WITH THE APPLICANT



(b) (7) (E)

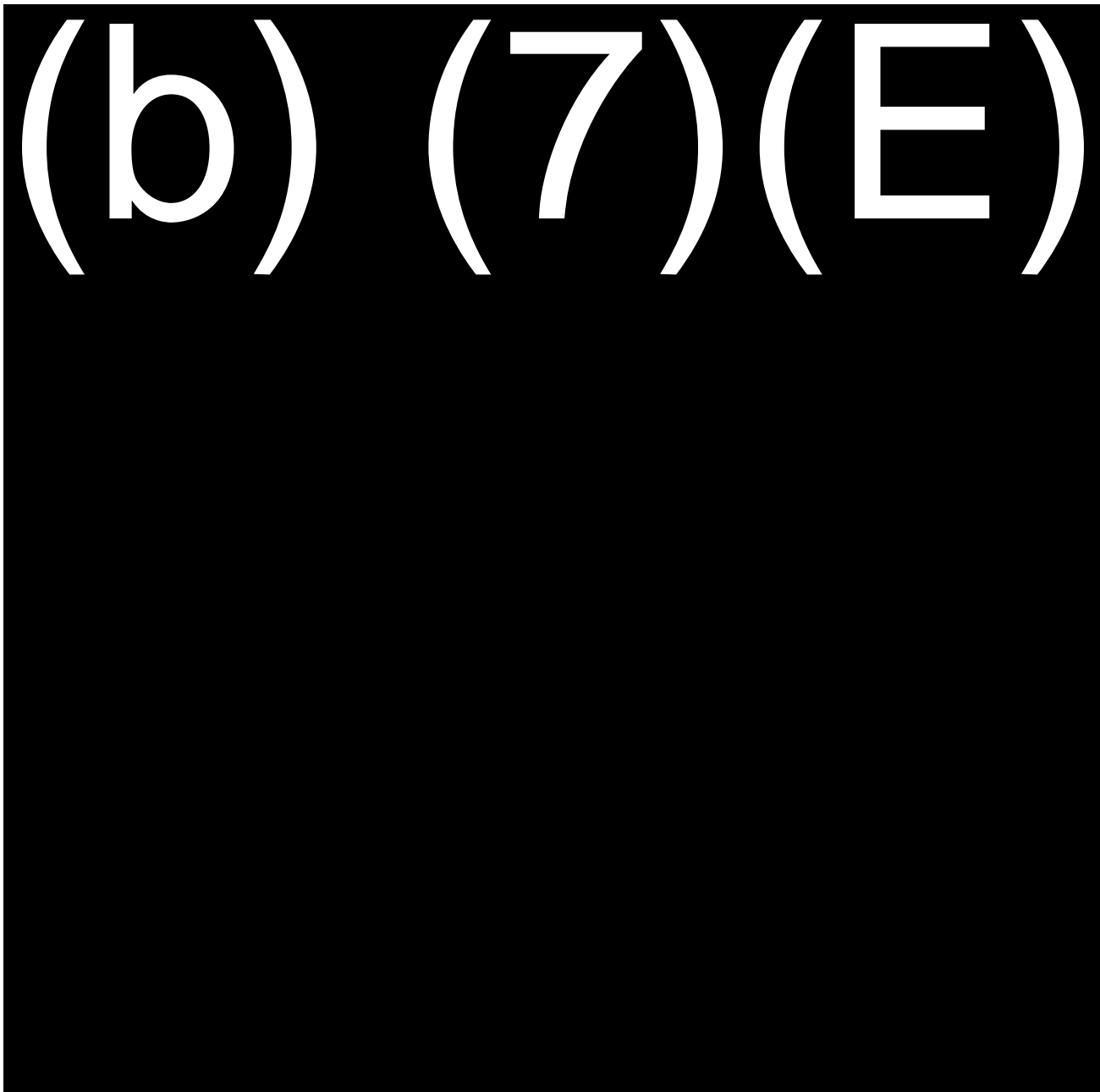
(b) (7) (E)

(b) (7) (E)



(b) (7) (E)

(b) (7) (E)



(b) (7) (E)

(b) (7) (E)



(b) (7) (E)



(b) (7) (E)



(b) (7) (E)



(b) (7) (E)

(b) (7) (E)



(b) (7) (E)



(b) (7) (E)



(b) (7) (E)



(b) (7) (E)



SOCIAL SECURITY

(b) (7) (E)

(b) (7) (E)



(b) (7) (E)



(b) (7) (E)



(b) (7) (E)



SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)



SOCIAL SECURITY
Office of the Inspector General

Standard Operating Procedures for Polygraph Examinations
(Psycho-Physiological Detection of Deception)

(b) (7) (E)



SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)



SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)



SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)

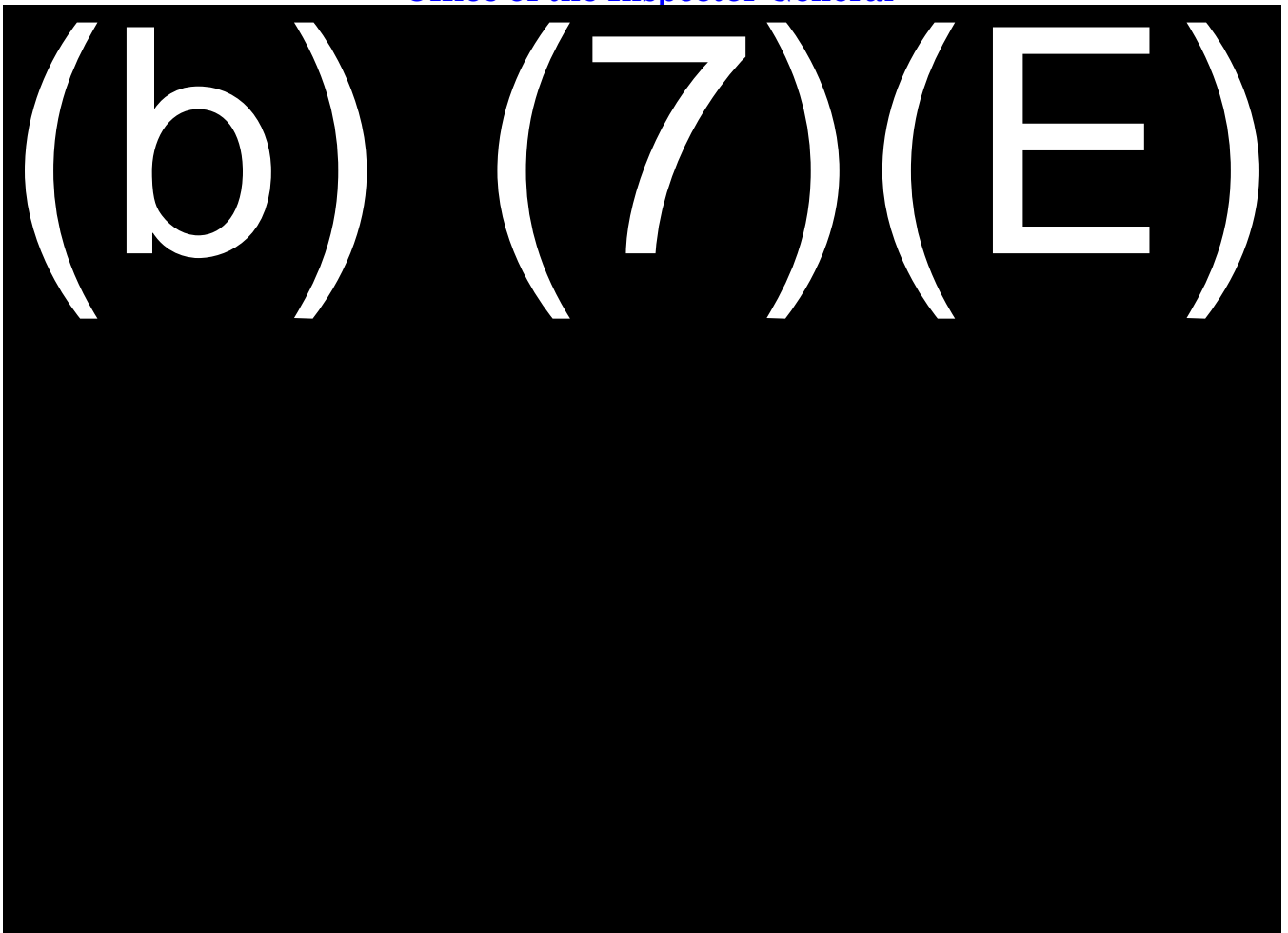


SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)

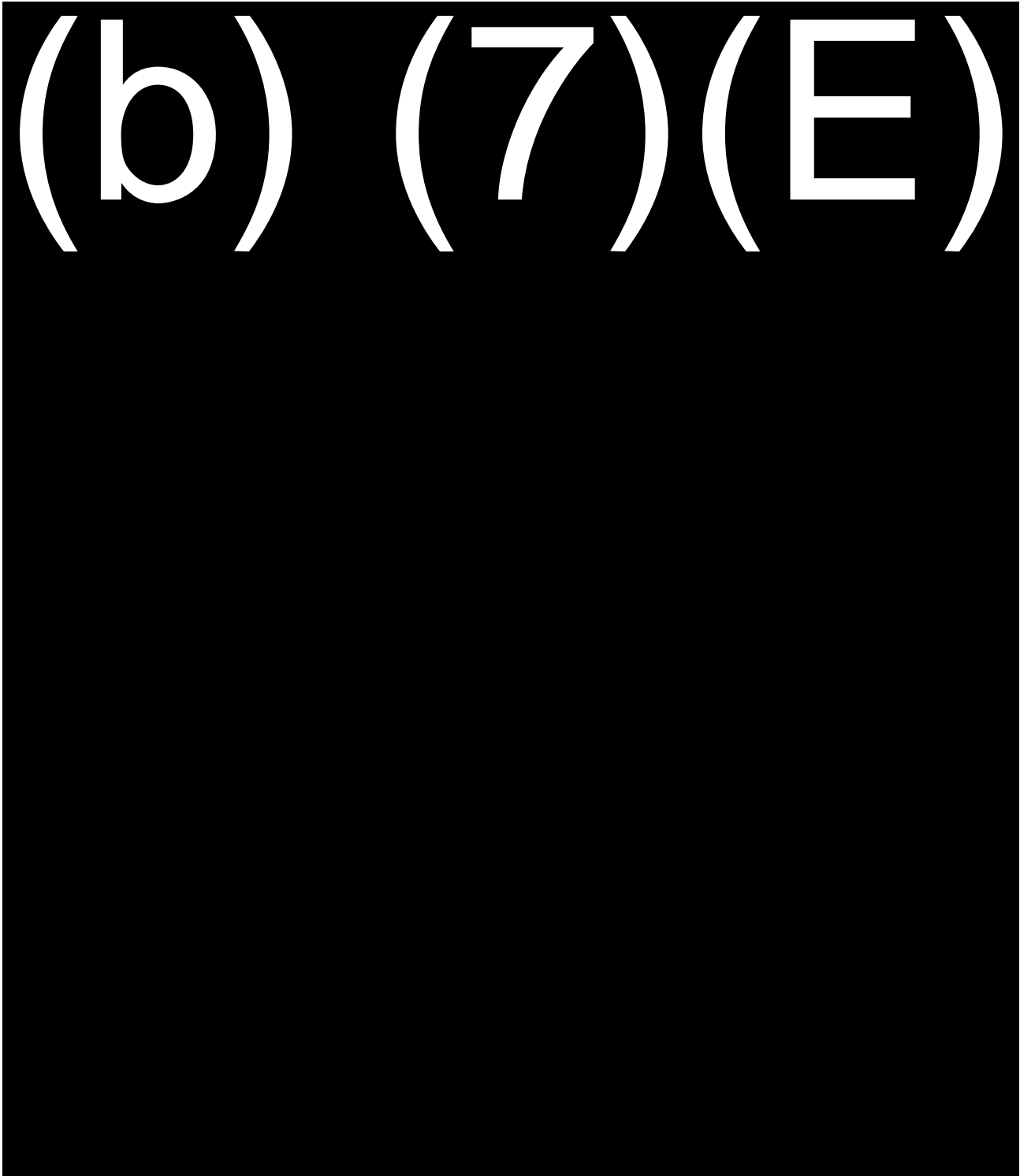


SOCIAL SECURITY
Office of the Inspector General



SOCIAL SECURITY
Office of the Inspector General

OI Polygraph Examination Request Worksheet



This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

REQUEST FOR NCIC/NLETS RECORDS CHECKS

(b) (7) (E)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

Form OI-43



OFFICIAL USE ONLY

**FINANCIAL CRIMES
ENFORCEMENT NETWORK**

P.O. Box 39, Vienna, VA 22183-0039



(b) (7) (E)

(b) (7) (E)



(b) (7) (E)

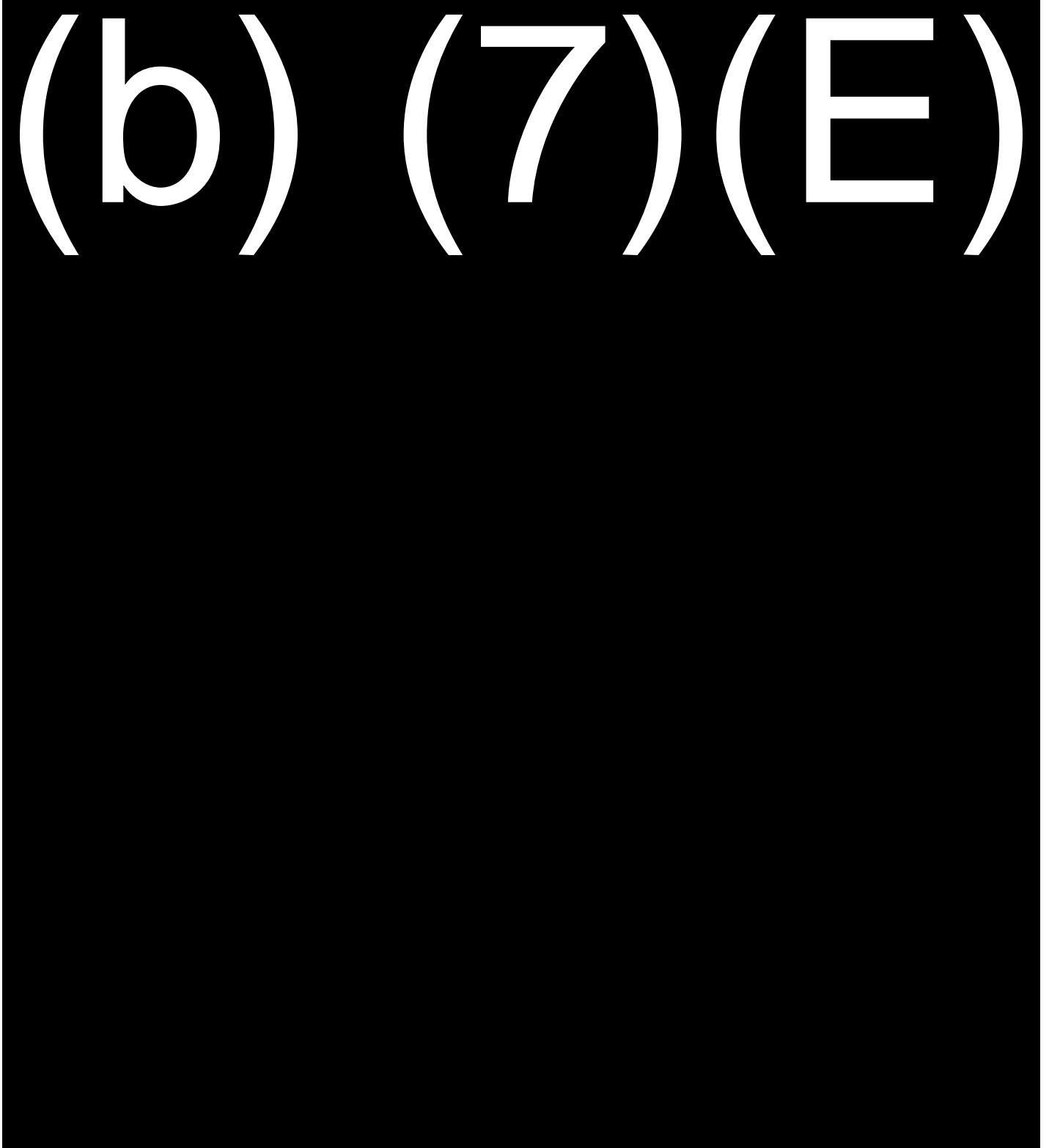


(b) (7) (E)



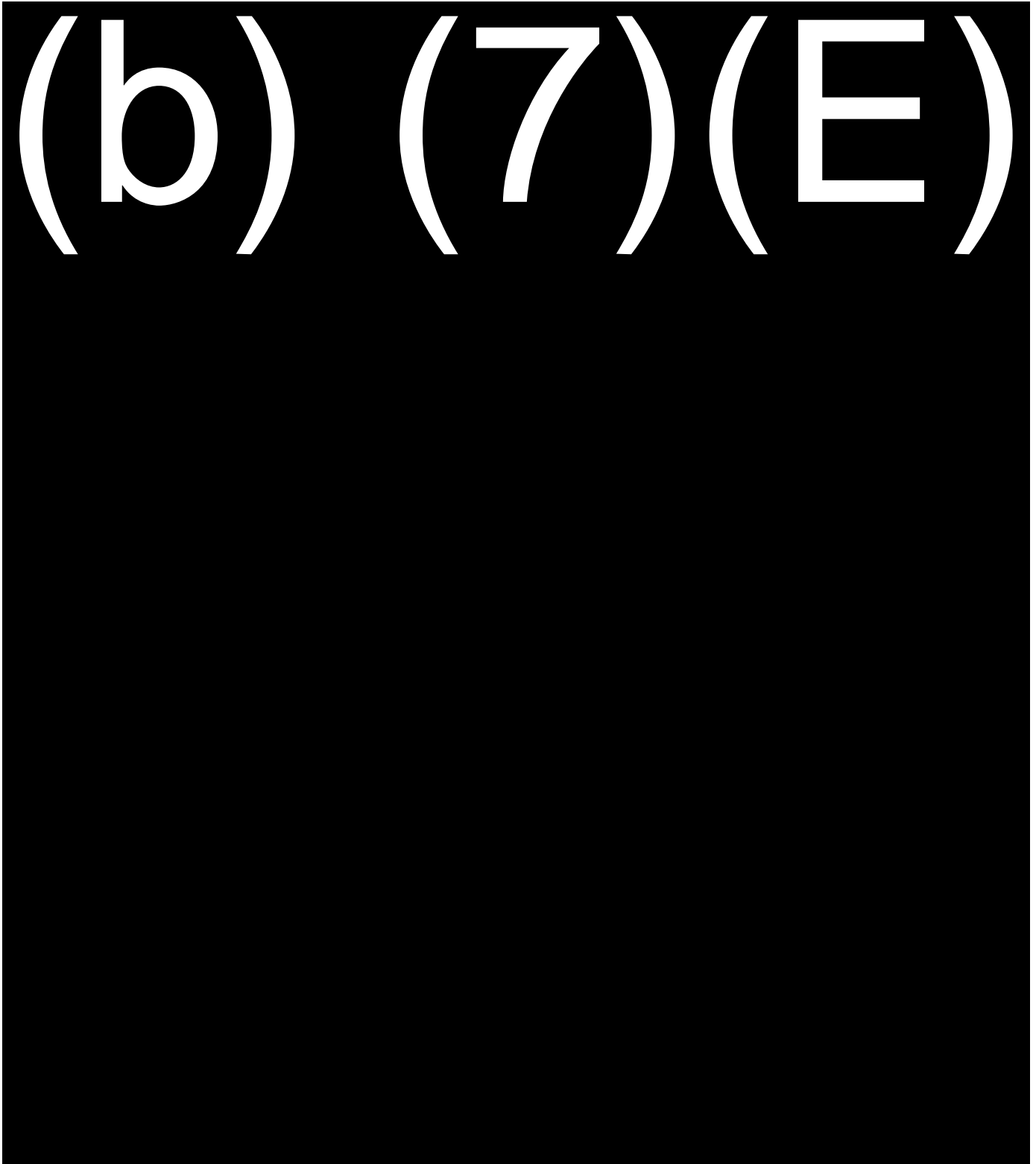
SOCIAL SECURITY
Office of the Inspector General

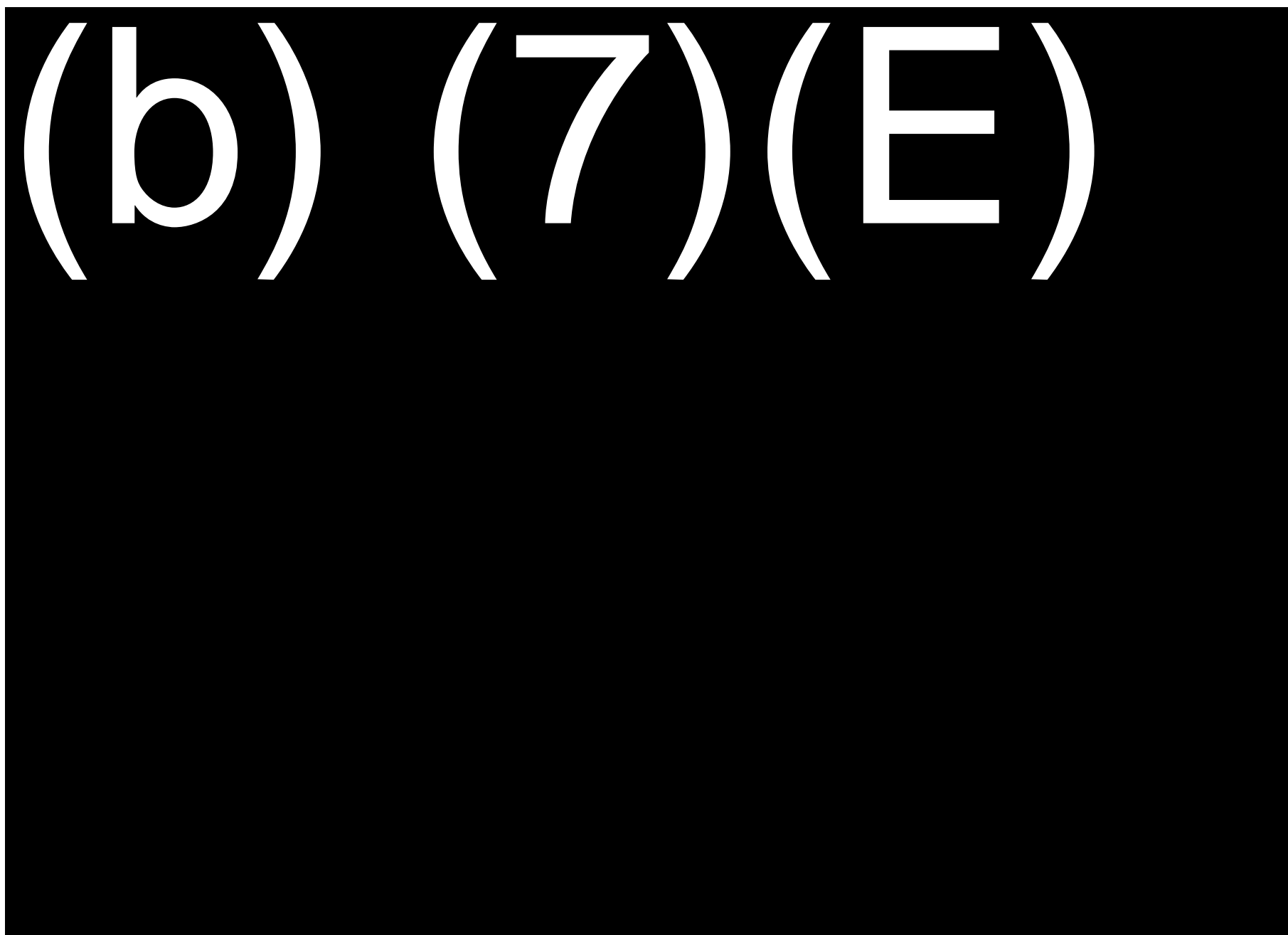
HANDWRITING SAMPLE



SOCIAL SECURITY
Office of the Inspector General

HANDWRITING SPECIMEN





(b) (7) (E)

(b) (7) (E)

(b) (7) (E)

Exhibit 7-18

NCIC Data for USMS

Special Agent: _____ Supervisor: _____

Office Telephone: _____ 24 Hr. Telephone: _____

Pager: _____ Fax Number: _____

Agency Case #: _____

The following information is provided for NCIC entry:
(* = Mandatory field; + = One numeric identifier must be included.)

1. Full Name*: Last _____ First _____ Middle _____

2. Alias(es): _____

3. Race*: _____ 4. Sex*: _____ 5. Height*: _____ 6. Weight*: _____ 7. Hair color*: _____

8. Eye color*: _____ 9. Scars, etc. _____ 10. Date of Birth*: _____

11. Place of Birth: _____

12. Social Security Number+: _____ 13. Passport Number: _____

14. Last Known Address – Street, City, & State: _____

15. Nationality: _____ 16. U.S. Naturalization Information: _____

17. Occupation: _____ 18. Driver's License Information+: _____

19. License Numbers: _____ 20. FBI Number: _____

21. Violation*: _____

22. Date of Warrant*: _____ 23. Warrant Number: _____ 24. Type of Warrant: _____

25. Agency Holding Warrant: _____

26. Info. on Dangerous Subjects: _____

27. Vehicle Description: _____

28. Associates: _____

Policy for Law Enforcement Information Systems and Commercial Database Access

The privacy of personal information obtained from law enforcement information systems (NCIC, NLETS, FinCEN, and State systems) and commercial databases made available to employees by either SSA or the OIG must be protected to the same extent as information contained in SSA systems. The Inspector General's position on systems security access violations is one of "zero tolerance."

No employee should access or attempt to access a government contracted database for purposes other than official business.

Penalties for Unauthorized Access

Anyone who misuses a criminal justice information system is subject to discipline up to and including removal.

Crimes and Criminal Procedures

This statute [18 U.S.C.1030] prohibits seven types of fraudulent activity in connection with computers, including, but not limited to:

- Intentionally accessing a computer without authorization or in excess of authorized access and thereby obtaining information from any department or agency of the United States.
- Without authority, accessing a computer of an agency or department of the United States.

A violation of this statute may result in a fine and/or imprisonment of up to 20 years, in accordance with Title 18 of the United States Code.

Internal Revenue Code

The Internal Revenue Code [26 U.S.C. 7213(a)] makes willful unauthorized disclosure by a Federal employee of information from a Federal tax return (which includes data in SSA's earnings datasets) a crime punishable by a \$5,000 fine, 5 years imprisonment, or both. Any officer or employee convicted of this crime will be dismissed from Federal office or employment.

Exhibit 7-19

Alcohol and Drug Abuse Patient Records

Any person who violates the Drug Abuse and Treatment Act or the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment, and Rehabilitation Act may be fined in accordance with Title 18 of the United States Code (above).

Exhibit 7-19

Law Enforcement Systems and Commercial Database
Security Acknowledgement

Employee Name _____

Employee Position _____

This is to acknowledge that I have read and understand the *Policy for Law Enforcement Information Systems and Commercial Database Access*. I understand that sanctions, up to and including dismissal, will be imposed for violations.

Year	Employee Signature	Date	Manager Signature	Date

National Crime Information Center (NCIC)

(b) (7) (E)



(b) (7) (E)



(b) (7) (E)



(b) (7) (E)



Non-SSA Internet Access Log

Name	Date	Case or Allegation Number	Purpose/Comments



**Social Security Administration
Office of the Inspector General
Office of Investigations**

***Mobile Device
Inventory
Worksheet***

Case Number: _____ Case Name: _____

Case Agent: _____ Office & Phone: _____

Warrant or Consent Date: _____ Date Acquired: _____

Mobile Device Information

	Evidence #	Manufacturer	Model	Size (GB)	Serial No./IMEI#	Type of Device
Cell Phone						
SIM Card						
Memory Card						
Other						

STATUS WHEN SEIZED	ITEMS RECOVERED
<input type="checkbox"/> Power off	<input type="checkbox"/> Charger
<input type="checkbox"/> Power on (Approx Battery Life = ____)	<input type="checkbox"/> Data Cables

(b) (7)(E)

Exhibit 7-22 (continued)

CHECKLIST

	Procedure	Date Completed:	Completed By:
1.	Before arriving on scene, review the search warrant to gain an understanding of the case.		
2.	Upon arrival at the scene, survey the site and identify media to be acquired.		
3.	Photograph cell phone and peripherals “as is” when arriving on the scene.		
4.	Initiate paperwork (Evidence Inventory).		
5.	Make note of Known Good Local Time (KGLT), particularly time zone information, and the source (such as cellular phone service provider) when starting on-scene activities.		
6.	Make note of condition of cell phone, and obtain any passwords, if applicable.		
7.	Place mobile device in a faraday bag or wrap in aluminum foil.		
8.	Complete paperwork.		
9.	Restore the scene to original configuration.		

INVENTORY NOTES
Cell Phone No.:
Service Provider:
PIN Number:
Passwords:
OTHER NOTES:

DATE	INITIALS	PAGE NO. 2 of 2
------	----------	--------------------

INTERCEPTION OF COMMUNICATIONS

008.000 Nonconsensual Monitoring

- A. The interception of verbal, non-wire communications when no party to the communications has consented and when all parties have a justifiable expectation of privacy must be conducted under tightly controlled circumstances.
- B. Each Special Agent (SA) must ensure that no communication of any party who has a justifiable expectation of privacy is intercepted, unless in accordance with the law.

008.010 Accounting for Interception Devices

- A. The Office of Investigations (OI) follows requirements established by the Attorney General (AG) concerning the use of interception devices (and devices used or intended for the surreptitious interception of non-wire verbal communications).
- B. The requirements generally provide for:
 - 1. Limiting the number of such devices to that reasonably required to accomplish an agency's lawful purposes.
 - 2. Storage of such devices in a minimum number of locations, to make them reasonably available.
- C. Each OI storage location will maintain an inventory of all such devices. When a device is withdrawn from storage, the user shall record the date and time of withdrawal. When the device is returned, the user must record the date and time of return.
- D. The user must account for the use of an interception device by completing a Report of Intercept, form OI-24A ([Exhibit 8-1](#)).
- E. Each OI storage location shall maintain copies of inventories, accounts, and reports concerning the interception devices for 10 years.
- F. The recording of internet based communications, (b) (7)(E) will be conducted with hardware and/or software approved by the SAC of the Criminal Investigations Division's Digital Forensics Team (DFT).

Electronic Tracking Devices

(b) (7)(E)

- (b) (7)(E)

- (b) (7)(E)

Use of an electronic tracking device requires appropriate legal approvals, administrative authorizations, and assistance from a Field Division Technical Agent (FDTA).

- A. Electronic Tracking Device Authorizations. In most instances, when SSA does not have the consent of the person who is the owner of the property or vehicle, a court order authorizing installation and use of a tracking device is required. SAs must discuss the specific legal requirements of the proposed installation with a local Assistant U.S. Attorney (AUSA) prior to utilizing this technique. The installation and use of tracking devices is covered under [Rule 41](#) of the Federal Rules of Criminal Procedure and specifically pursuant to [18 U.S.C. § 3117](#), Mobile Tracking Devices.

In most instances, no court order is required if the following conditions are met:

- No trespass is required to install the device;
- No power is taken from the vehicle; and,
- The tracking data recorded is *historical*, not *real-time*.

(b) (7)(E)

See SAH 008.040 for additional information related to Title III intercepts.

The use of electronic tracking devices must be approved by the Field Division SAC. To obtain such approval, the SA will prepare a memorandum ([see Exhibit 8-5](#)) to the SAC outlining the proposed use of an electronic tracking device, costs associated with operation of the device, and other resources required to track the target package or vehicle. The memorandum must include the following information:

- Case name and number;
- Complete description of target package or vehicle;
- Proposed duration of tracking;
- Results of initial conference with AUSA;
- Justification for use of electronic tracking device; and,
- Proposed surveillance plan.

The SA will retain the original request in the case file and forward copies to the SAC-Criminal Investigation Division (via their assigned desk officer) and the FDTA.

In urgent cases, approval to use an electronic tracking device may be made by telephone. This must be followed as soon as possible by written documentation as previously described.

SAs should begin the process of requesting the use of an electronic tracking device by consulting with the FDTA assigned to their division. The FDTA will assist the SA in gathering certain technical information, planning the installation of equipment, projecting costs, and formulating a proposed surveillance plan.

B. Court Approval of Electronic Tracking Device Procedures. The SA must contact the local AUSA to obtain advice concerning the legal authorization required to utilize this technique. If a court order is required, the SA must prepare an affidavit in support of the court order containing the following three critical elements:

- A recitation of the probable cause leading the affiant to believe the property or vehicle will be used in furtherance of a crime in violation of Federal laws investigated by SSA/OIG/OI;
- An explanation of how the success of the surveillance depends upon the tracking device; and,
- Authorization to access the property or vehicle to install and remove the tracking device.

The duration of a court order authorizing installation of a tracking device is 45 days and requests for extension may be made. It is recommended that such court orders be “sealed,” when possible, to preserve the integrity of the investigation.

C. Electronic Tracking Device Installation and Operation. Upon notification that a tracking request has been approved by the SAC (and the court, if required), the FDTA assigned will:

(b) [REDACTED]

The SA requesting use of a (b) (7)(E) tracking device:

(b) [REDACTED]

D. Consensual Use of Electronic Tracking Devices. In cases where the owner of property has given permission for the installation of an electronic tracking device, follow all the requirements for requesting approval, with the exception of obtaining a court order. Document the owner’s consent in writing ([see Exhibit 8-6, Form OI-25](#)) and ensure that the consenting party is lawfully authorized to give consent.

Note: Tracking of a government owned vehicle (GOV) may involve issues related to “reasonable expectation of privacy.” SAs must consult with a local AUSA prior to such installation. (b) (7) (E) [REDACTED]

008.030 Dialed Number Recorder

- A. It is the policy of the United States Department of Justice (DOJ) to require all Federal law enforcement officers to obtain a court order authorizing the installation and use of any dialed number recorder (DNR) or other similar device.
- B. Law enforcement officers who fail to obtain a court authorization may be exposed to civil or criminal liability (a potential felony) under 50 U.S.C. §§ [1809](#) and [1810](#).
- C. Use of a DNR also requires the consent of an OIG HQ approving official, as shown in Section 008.070.
- D. In an emergency situation, a SAC may seek a court order authorizing a DNR without the prior approval of OIG HQ. However, the DAIGI must be notified of the request at the earliest practical time.
- E. After the completion of each monitoring period, the investigator will complete a Report of Intercept, Form OI-24A (see [Exhibit 8-1](#)). The “other” box should be marked and “dialed number recorder” noted.

008.040 Interception of Wire or Oral Communications

The Omnibus Crime Control and Safe Streets Act of 1968, as amended (18 U.S.C. § 2510, et seq.) sets forth the requirements for obtaining court approval to intercept wire or oral communications. While these provisions are commonly referred to as the “wiretap” restrictions, they apply to any type of listening device employed surreptitiously. Devices not covered by these provisions are those which do not involve interception of communications; e.g., “beepers.” Neither do they cover situations where communications are monitored with the consent of one of the parties involved in the communication (consensual monitoring).

If the investigation appears to require interception of wire and/or oral communications as in 18 U.S.C. § 2510 et seq., the SA should first discuss the matter in detail with the Assistant United States Attorney (AUSA) who has jurisdiction. If the AUSA is satisfied that the offense being investigated falls within the scope of the governing statute (see [18 U.S.C. § 2516](#)) and that interception is required, the SAC should then discuss the matter with the Criminal Investigations Division (CID).

CID will decide the next action to be taken by OI in the matter, will seek any necessary approvals from the appropriate authorities, and will communicate all decisions in the matter to the SAC.

008.050 Consensual Telephone Monitoring

- A. The monitoring of a telephone conversation with the consent of one of the parties to the conversation constitutes “consensual telephone monitoring.”
- B. The express consent of an approving OI official is required prior to engaging in consensual

telephone monitoring. It is the policy of the OIG to obtain local approval from the United States Attorney, an AUSA, or the previously designated DOJ attorney responsible for a particular investigation.

- C. The term “approving official” as used in this section means the SAC of the field division. In the absence of the SAC, the Assistant Special Agent-in-Charge (ASAC) or Resident Agent-in-Charge (RAC) may act as the approving official. Approval will generally be obtained by memorandum from the SA to the approving official. Section 008.060 relates the information that should be included in the request. Once approved, a copy of the memorandum shall be provided to CID via the field division’s assigned desk officer.
- D. In urgent situations, the SA may request approval from the approving official by telephone. The SA shall prepare a memorandum to document the request as soon as practical. The memorandum must include the items listed in Section [008.060B](#).
- E. An affidavit showing consent will also be obtained from the consenting party prior to engaging in consensual telephone monitoring (*see [Exhibit 8-2](#), Form OI-25L.*)
- F. Records generated by consensual telephone monitoring must be incorporated into the relevant OI file. Such records may be released only in accordance with statutory disclosure restrictions applicable to that file.
- G. After the completion of each monitoring period, the SA will complete a Report of Intercept, Form OI-24A (*see [Exhibit 8-1](#)*).

008.060 Request for Approval of Consensual Telephone Monitoring

- A. The “Request of Consensual Telephone Monitoring” memorandum, Form OI-24 (*see [Exhibit 8-3](#)*), will be submitted through the appropriate ASAC to the field division SAC.
- B. In addition to the case number and title, the request will include:
 - 1. Reason for the Activity – The request must include a reasonably detailed statement of the background of the case and relate circumstances for the need to monitor.
 - 2. Offense – Include a citation of the primary alleged offense.
 - 3. Danger/Contingency Plans – Mention the measures taken to prevent non-consenting party from identifying the caller, any safety concerns during the monitoring, and any plan to protect both the identity and physical safety of the person making the call.
 - 4. Description and Location of Devices/Equipment – The request must specify what special equipment will be used. The location(s) at which the monitoring will be conducted, for both the calling and receiving telephones, must be identified. When the monitoring and/or recording device is to be used by a civilian, this section should contain a statement that a Consensual Telephone Monitoring Request ([Form OI-25L, Exhibit 8-2](#)) is being requested.

5. Location of Operation – The request must specify the location and primary judicial district where the monitoring will take place. If the location of the monitoring location changes, notice should be given promptly to the approving DOJ and OIG officials.
 6. Duration and Dates – Requests should be made for (b) (7)(E) periods unless special circumstances exist and are described in the request. The (b) (7)(E) period must be stated in specific terms; i.e., “from (date) to (date)” rather than simply stating (b) (7)(E).”
 7. Names – State the name of the person whose conversation will be recorded. Include the name of the case agent and the agent recording the conversation(s).
 8. Trial Attorney Approval – The request must state that the facts of the case were discussed with a DOJ attorney (e.g., AUSA or Organized Crime Strike Force Attorney) or other authorized prosecuting attorney for the judicial district where the activity will occur. The name of the attorney who approved the monitoring must be included in this section (also include the date of the approval). The request must also state that the attorney has expressed an opinion that the operation is not likely to cause entrapment.
 9. Potential for Criminal Activity by Cooperating Individual – As appropriate, mention if any anticipated activity during the monitoring may constitute a crime if engaged in by a private citizen without approval of an appropriate Government official.
 10. Potential for Law Enforcement Officer (LEO) Criminal Activity – The request must state the nature of any criminal activity which the LEO may become engaged in as part of the operation. This section must include a statement that the AUSA is aware of this potential criminal activity and has approved its use within this operation. The request must include a statement that there is no anticipation of criminal activity on behalf of SSA OIG Agents that would fall outside the scope of the undercover operation.
 11. Unusual Expenses – The request must show the projected costs of any expense above normal costs of business.
- C. The SAC shall notify the ASAC or SA via electronic mail or fax as soon as the request is approved. Written approval of the request will be returned to the SA. The SAC will retain a copy of the approved request. In addition, a copy of the approved memorandum will be provided to CID via the field division’s assigned desk officer.
- D. Requests for extensions or renewals should be submitted in the same manner as the original request. The renewal request must also refer to all previous authorizations and explain why an additional authorization is needed, as well as provide an updated statement as to the concurrence of the responsible trial attorney.

008.070 Consensual Non-Telephone Monitoring

DOJ’s and OI HQ’s approval (*via OI HQ’s Operations Review Committee-ORC*) is required for any monitoring or recording of non-telephone conversations where less than all of the parties to the conversation have consented to the monitoring or recording. This shall include (b) (7)(E)

These requests are generally combined with an undercover request. ***If the monitoring is conducted as***

part of an undercover activity/operation, follow the procedures for a request, as set forth in Chapter 7 of this Handbook.

The term “approving official” as used in this section means the DAIGI. In the absence of DAIGI, the AIGI or the IG may act as the approving official.

A. Authorization in Non-Sensitive Cases

1. Where monitoring appears to be necessary, the case agent or authorized designee must first obtain the approval of the appropriate DOJ official or prosecuting attorney in the district where it is to occur.
2. The SAC will then request HQ approval by sending a memorandum to the DAIGI, through the CID desk officer, for ORC-approval in advance of the operation. In urgent situations, the SAC or, in his/her absence, the ASAC or RAC may request DAIGI approval by telephone. In these situations, a memorandum must be forwarded to the DAIGI immediately after verbal approval is obtained.

B. Requests for approval of non-telephone monitoring are in the form of a memorandum to the DAIGI, Form OI-24 ([Exhibit 8-3](#)). In addition to the case number and title, the memorandum must contain the following information:

1. **Reasons for the Activity** – The request must include a reasonably detailed statement of the background of the case and relate the circumstances to the need for the interception.
2. **Offense** – Include a citation of the primary alleged offense.
3. **Danger/Contingency Plans** – If the interception is intended to provide protection to the consenting party, the request must explain the danger to the consenting party. If there is no particular danger, the request must state that no danger to the consenting party is known as of the time of the request. (**Note:** (b) (7)(E) is participating in the activity/operation, this section must state the results of both State and Federal criminal history checks of the target of the interception, e.g. “Subject has three prior arrests for assault.” **Any** history of violent behavior on the part of the target(s) must be addressed specifically in this section. If the target is unknown, an inherent risk to (b) (7)(E) should be assumed, and special precautions must be addressed.)

The request must also state the intended contingency plans, that an OI-17 has been prepared and is on file, or that a tactical plan will be prepared by the lead agency and will be on file prior to the initiation of the operation.

4. **Description and Location of Devices** – The request must describe the device(s) and state where the interception device(s) will be concealed: on the person, in personal effects, or in a fixed location. When the monitoring and/or recording device is to be used by a civilian, this section should contain a statement that a Consensual Non-Telephone Monitoring Request (Form OI-25L, Exhibit 8-4) is being requested.
5. **Location of Operation** – The request must specify the location and primary judicial district where the interception will take place. If the location of an interception changes, notice

should be given promptly to the approving DOJ and OIG officials. The record maintained on the request should reflect the location change.

6. Duration and Dates – The request must state the length of time needed for the interception. Initially, an authorization may be granted for up to (b) (7)(E) beginning with the day the interception is scheduled to begin. If there is need for continued interception, extensions for periods of up to (b) (7)(E) may be granted. In special cases (e.g., “fencing” operations run by law enforcement agents), initial authorization for up to (b) (7)(E) may be granted with similar extensions.
 7. Names – The request must give the names of persons, if known, whose communications the agency expects to intercept, and the relation of such persons to the case under investigation or to the need for the interception. If the interception will be conducted (b) (7)(E) the agency expects to intercept.
 8. Trial Attorney Approval – The request must state that the facts of the case have been discussed with the United States Attorney, AUSA, the previously designated DOJ attorney responsible for a particular investigation, or other such authorized prosecuting attorney for the judicial district where the activity will occur; and such attorney concurs that the use of consensual monitoring is appropriate (include the date of such concurrence). The attorney must also concur that the use of consensual monitoring under the facts of the investigation does not raise the issue of entrapment. Such statements may be made orally.
 9. Potential for Criminal Activity by Cooperating Individual – As appropriate, mention if any anticipated activity during the monitoring may constitute a crime if engaged in by a private citizen without approval of an appropriate Government official.
 10. Potential for Law Enforcement Officer (LEO) Criminal Activity – The request must state the nature of any criminal activity that the LEO may become engaged in as part of the operation. This section must include a statement that the AUSA is aware of this potential criminal activity and has approved its use within this operation. The request must include a statement that there is no anticipation of criminal activity on behalf of SSA OIG Agents that would fall outside the scope of the undercover operation.
 11. Unusual Expenses – The request must show the projected costs of any expense above normal costs of business.
- C. A request for renewal authority to monitor oral communications must contain all the information required for an initial request. The renewal request must also refer to all previous authorizations and explain why an additional authorization is needed, as well as provide an updated statement as to the concurrence of the responsible trial attorney.
- D. An affidavit expressing consent will be obtained from each consenting party to the monitoring. ([Exhibit 8-4](#), Form OI-25AL)
1. The OI SAs and other Federal law enforcement personnel who are consenting parties and whose conversations will be monitored are exempt from submitting an affidavit.

- E.** Records generated by consensual non-telephone monitoring must be incorporated into the relevant OI file. Such records may be released only in accordance with statutory disclosure restrictions applicable to that file.
- F.** After the completion of each monitoring period, the SA will complete a Report of Intercept, Form OI-24A (see [Exhibit 8-1](#)).
- G.** Authorization in Sensitive Cases

Prior formal written approval is required from the DOJ Office of Enforcement Operations, and will be requested by OIG HQ in the following six sensitive case categories:

1. (b) (7)(E) [Redacted]
2. (b) (7)(E) [Redacted]
3. (b) (7)(E) [Redacted]
4. (b) (7)(E) [Redacted]
5. (b) (7)(E) [Redacted]
6. (b) (7)(E) [Redacted]

H. Where monitoring is required in a case in one of the above categories, the SAC will request that OIG HQ obtain DOJ approval. The SAC's request should be in the form of a memorandum containing the information required above.

I. Emergency Authorizations

The OIG HQ approving officials listed above may authorize monitoring in sensitive or non-sensitive cases where the need for monitoring arises during non-working hours of the DOJ. In such cases, the SAC must provide all of the information required in a non-emergency situation. Where authorization is granted in a sensitive investigation (see Section 008.070G), OIG HQ must notify the DOJ Office of Enforcement Operations not later than the next working day.

J. Monitoring Equipment

1. When a communicating party consents to the interception of his/her verbal communications, the device may be hidden on his/her person, in personal effects, or in a fixed location.
2. The SA engaging in such consensual interceptions must ensure that the consenting party will be present at all times when the device is operating.
3. In addition, the SA must ensure:
 - a. That no SA or person cooperating with him/her trespasses while installing a device in a fixed location and
 - b. That as long as the device is installed in the fixed location, the premises remain under the control of the Government or consenting party.

K. Reporting of Results

1. When the monitoring period is completed, the SA will complete a Report of Intercept, Form OI-24A ([Exhibit 8-1](#)). *(If an extension is requested and granted, an OI-24A will be required for the initial period, as well as any subsequent extension periods.)*
 - a. After approval by the SAC, the Report of Intercept will be sent to the DAIGI via the CID desk officer.
 - b. The completed and approved Report of Intercept is due in OI HQ no more than 10 working days after the end of the monitoring period..
2. A copy of a surveillance log may be used to supplement the Report of Intercept.
3. CID keeps a record of all approved intercepts and provides this data for OI's annual report to DOJ.

Chapter 8 — **EXHIBITS**

[8-1 — Report of Intercept \(OI-24A\)](#)

[8-2 — Consent to Monitor Telephone Conversations \(OI-25L\)](#)

[8-3 — Sample Request Memorandum \(OI-24\)](#)

[8-4 — Consent to Monitor Non-Telephone Conversations \(OI-25AL\)](#)

[8-5 — Memo to SAC - Authorization for Installation of Electronic Tracking Device](#)

[8-6 — Consent to Use Electronic Tracking Device \(OI-25\)](#)



REPORT OF INTERCEPT

(b) (7) (E)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

Exhibit 8-1

INVESTIGATIVE BENEFITS DERIVED FROM INTERCEPT:

If the monitoring was attempted, did the efforts provide information which corroborated, or assisted in corroborating, the allegations or suspicions:

Prepared by Special Agent: _____
Approved by ASAC/RAC _____
Approved by SAC _____

Date _____
Date _____
Date _____

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.



Consent to Monitor Telephone Conversations

Date: _____

Location: _____

I, _____, _____ hereby (Name)
(Address)
authorize _____ and _____, Special Agents
(Name) (Name)
of the Office of Investigations, Office of the Inspector General, Social Security Administration,
to install a recording device on a telephone number
_____ located at _____
(Telephone #) (Location)
for the purpose of recording any conversation I may have on that telephone with
_____ on _____
(Name) (Date)
at/about _____.
(Time)

I have given this permission to the Special Agents named above voluntarily and without threats, pressure, or promises of any kind.

(Print Name)

(Signature)

Witnesses:

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.**



MEMORANDUM

Date:

Refer To:

To:

From:

Subject:

1. Reason for Activity:

2. Offense:

3. Danger / Contingency Plans:

4. Description and Location of Devices / Equipment:

5. Location of Interception:

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

6. Duration and Dates:

7. Names:

8. Trial Attorney Approval:

9. Potential for Criminal Activity by Cooperating Individual:

10. Potential for Law Enforcement Officer (LEO) Criminal Activity:

11. Unusual Expenses:

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.



Consent to Monitor Non-Telephone Conversations

Date: _____

Location: _____

I, _____, _____ hereby (Name)
 (Address)
 authorize _____ and _____, Special Agents
 (Name) (Name)
 of the Office of Investigations, Office of the Inspector General, Social Security
 Administration, to place a _____ on my person, property,
 (Type of Non-Telephone Monitor)
 or premises for the purpose of recording any conversation with
 _____ on or about _____.
 (Name) (Date)

I have given this permission to the Special Agents named above voluntarily and without threats, pressure, or promises of any kind.

(Print Name)

(Signature)

Witnesses:

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.



MEMORANDUM

Date: Enter Date **Refer To:** OI Case Number

To: Name of Special Agent in-Charge, XXXXXX Field Division

From: Name of Assistant Special Agent-in-Charge, XXXXXX Group

Subject: Authorization for Installation of Electronic Tracking Device

SUBJECT is an SSA Claims Representative assigned to XXX, located in XXXX. SUBJECT is the lead suspect in a case in which sensitive SSA documents have been stolen from the division building and were recovered from the apartment of an individual involved with identity theft. SUBJECT is known to associate with convicted felons and possible gang members. This case is being worked jointly with XXXXX. SUBJECT resides at XXXX.

(b) (7)(E)



On date, XXXX, Assistant United States Attorney, XXX Judicial District of XXXXX concurred with the (b) (7)(E). AUSA XXXX stated a court order is not required provided (b) (7)(E) in a public place.

Cc: SAC Criminal Investigation Division
Field Div. Tech Agent

APPROVED: Electronic Signature

Date

Special Agent in Charge, XXXX Field Division



Consent to Use an Electronic Tracking Device

Date: _____

Location: _____

I, _____, _____ hereby
(Name) (Address)
authorize _____ and _____, Special Agents
(Name) (Name)
of the Office of Investigations, Office of the Inspector General, Social Security
Administration, to place a _____ on my vehicle or property,
(Type of Electronic Tracking Device/Serial #)
described as: _____; for the
(Description i.e.: property, vehicle make, color, year, and license plate)
purpose of: _____.

I have given this permission to the Special Agents named above voluntarily and without threats, pressure, or promises of any kind.

(Print Name)

(Signature)

Witnesses:

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

CONFIDENTIAL EXPENDITURES

009.000 Purpose

Section 6, Part (a) (9) of the Inspector General Act of 1978 authorizes the Office of the Inspector General (OIG) to make confidential payments to individuals as necessary to carry out the provisions of the Act. The purpose of this guide is to make available these funds needed in the furtherance of an investigation; establish steps to effectively administer such a fund; and establish processes to effectively monitor and report expenditures.

009.010 Obtaining Confidential Funds ATM Card

Any agent seeking a confidential funds ATM card must obtain approval from their Assistant Special Agent-in-Charge (ASAC) or Resident Agent-in-Charge (RAC). After ASAC/RAC approval, the agent must first review the entire chapter on Confidential Expenditures. Once this has been completed, a certification statement must be completed affirming the following:

I, _____, of SSA OIG, certify that I have read Chapter 9 – Confidential Expenditures, of the Special Agent Handbook located on OIG’s Sharepoint site. I completed this on mm/dd/yy.

Send the certification statement and the completed ATM card application to your Special Agent-in-Charge (SAC) for approval. The application can be found [here](#) or on the Office of Acquisition and Grant’s (OAG) webpage at the bottom under the **Forms and Instructions** section.

The SAC will forward his approval, the application, and the certification statement to the Assistant to the Special Agent-in-Charge (ATSAC) of the Policy and Administration Division (PAD) for forwarding to the appropriate Deputy Assistant Inspector General (DAIGI). The DAIGI will review the application, approve it, and return it to the ATSAC of PAD. PAD will then forward the information to the purchase card coordinator in the Office of Communications and Resource Management’s (OCRM), Budget and Logistics Staff for completion. Once completed, the purchase card coordinator will forward the application to OAG for processing. When approved, OAG will send the applicant an email containing their delegation of acquisition authority and Citibank will send a pre-assigned PIN and ATM card to the address shown on the purchase card account.

Upon receipt of the ATM card, cardholders will be able to obtain confidential funds from any ATM. Cardholders will withdraw only the minimum amount required (b) (7)(E) _____, the cardholder must have prior approval (see Section 009.050). ATM machines have maximum withdrawal limits, and if you need more than the maximum amount available, you will need to go inside the bank. You will also need to go inside the bank for amounts (b) (7)(E) _____

(b) (7)(E)

009.020 Disposition of Excess ATM Withdrawals

In the event that confidential fund withdrawals are made in excess of the required expenditure, the cardholder will immediately return the unexpended cash to the SAC. If the confidential funds ATM withdrawal occurs in an office, unexpended cash should be converted to a money order and express mailed to the SAC, accompanied by a copy of Form OI-28A, "Transaction Record of Each Advance or Return of Confidential Funds" (see [Exhibit 9-1](#)). The cost of the money order may be deducted from the unexpended balance.

All money orders should be made payable to: Social Security Administration.

Within 15 working days of the confidential funds withdrawal, the SAC will mail the money order with a completed "OIG Transmittal Register" (see [Exhibit 9-2](#)) to the following address for deposit:

SSA/OIG/OI
Criminal Investigations Division ATSAC
3-ME-3 Meadows East Building
6401 Security Blvd.
Baltimore, Maryland 21235

Note: When sending the money order to the Criminal Investigations Division (CID), use a traceable form of mail service.

The CID ATSAC will hand carry the money order to the OIG Budget Office and obtain a signed receipt. The Budget Office will submit the money order to the Office of Finance for deposit.

In the event that the SAC is unable to return the excess withdraw to CID within 15 working days, the SAC is responsible for safekeeping excess funds. (b) (7)(E)

The SAC is personally liable for the cash and is responsible for ensuring that adequate safeguard procedures are in place, including the following:

1. Cash must be stored in a locked location.
2. Cash should be kept locked at all times, and when not in use, kept in a safe place.
3. All safekeeping facilities must be kept out of the view of the public.
4. Under no circumstances will excess confidential fund withdrawals be commingled with private or unofficial funds.
5. A duplicate key and/or combination must be placed in a sealed envelope, which must be signed by the SAC, dated, and retained in a secure place.

Note: Matters of theft or loss must be immediately reported to the AIGL.

009.030 Confidential Expenditures

- A. Confidential funds are used to make confidential expenditures only when those expenditures are in the best interest of the OIG, and where confidentiality is crucial to the outcome of a criminal investigation.
- B. Confidential expenditures of Social Security Administration (SSA) OIG funds will be limited to:
 - 1. expenditures to secure evidence or information;
 - 2. confidential payments to; or on behalf of informants;
 - 3. expenditures made in connection with undercover operations; or
 - 4. expenditures of an emergency nature, wherein confidentiality is crucial to the outcome of a criminal investigation.

009.040 Expenditures for Confidential Informants

- A. Confidential funds may be used to pay informants for information, or on behalf of a confidential informant (CI).
 - 1. (b) (7)(E) [REDACTED]
 - 2. (b) (7)(E) [REDACTED]
 - 3. Receipt for Payment to Informant is documented on [Form OI-28B](#) (see [Exhibit 9-3](#)).

009.050 Approving Amounts by Officials

- A. A SAC must authorize all confidential fund expenditures.
- B. Amounts over (b) (7)(E) require additional approval as follows:
 - 1. All confidential fund expenditures between (b) (7)(E) must be authorized by the Assistant Inspector General for Investigations or the appropriate DAIGI.
 - 2. All confidential fund expenditures (b) (7)(E) must be authorized by either the Inspector General or Deputy Inspector General.

009.060

Funds Administration

A. [Form OI-28](#), Custodian’s Transaction Log (referred to hereafter as “the Log”) (see [Exhibit 9-4](#)), is the custodian’s **key** administrative tool. The SAC uses the Log to record ATM withdrawals and unexpended balances, to note the type of transaction, and to provide key details about the transaction.

1. When authorization to use the card is granted, the SAC records the date, transaction type, case number, the name of the special agent requesting the confidential funds, amount of funds approved for ATM withdrawal, actual amount expended, returned balance, and the signature of the special agent. The SAC and cardholder must sign each entry. In the event that the cardholder is not located near the field division (FD), the SAC will annotate the log by stating “ATM Withdrawal Granted” in the comment column. In place of the special agent’s signature, use “unavailable,” and retain a copy of the email from the cardholder requesting the confidential fund expenditure.

Note: Under no circumstances are confidential fund expenditure withdrawals to be used for any other administrative purposes (such as for paying for supplies, services, travel, etc.).

2. Unexpended cash must be converted to a money order and returned to the SAC (see Section [009.020](#), “Disposition of Excess ATM Withdrawals”). A separate entry must be made on the Log (see [Exhibit 9-4](#)) referencing the original entry and case. In the “Comments” column, record the date the funds were returned to CID. The money order amount should be reduced by the amount charged for the purchase of a money order. For example, if the unused cash difference is \$50, and the cost of purchasing a money order is \$3, the amount of the money order should be \$47. The cardholder making the ATM withdrawal is responsible for ensuring that excess ATM withdrawals are immediately returned to the SAC.
3. Once it is determined that a confidential funds expenditure is required, OI personnel are assigned the following responsibilities.

B. SAC Responsibilities

1. Approves all confidential funds withdrawals.
2. Annotates all required information on the Log. The Log is afforded the same security as are weapons and evidence.
3. Posts all confidential funds transactions to the Log and maintains all written communication related to the transaction with the Log.
4. Performs a monthly reconciliation of the “Monthly Account Summary” to the Log. The servicing bank sends the Monthly Account Summary to all Approving Officials at the beginning of each month. The Monthly Account Summary provides a detailed list of all ATM withdraws that occurred during the preceding month.
5. In the event that the amount of the confidential fund withdrawal exceeds the amount of the expenditure, and the cardholder returns unexpended funds:

6. The SAC returns unused confidential funds to CID within 15 working days from the date of withdrawal. This requirement may be waived by the appropriate DAIGI in exceptional circumstances, such as an ongoing operation in which future use of the funds is imminent. In such instances, the SAC should submit a written request to the appropriate DAIGI, via email or memorandum, documenting the waiver request. This request should be made to the appropriate DAIGI through the SAC of CID within the 15-day timeframe. A record of the DAIGI's approval of the SAC's request should be submitted with the Accountability Report described in Section [009.070](#) below.

C. Cardholder Responsibilities

1. Informs the SAC, in writing or via email, of the intention to withdraw confidential funds. The message must include the date, case number, and the amount requested.
2. After the SAC approves the confidential fund ATM withdrawal, and the withdrawal is made; the cardholder immediately places the card in a secure location.
3. Ensures that all necessary forms are complete with appropriate authorizations and associated documentation.
4. Certifies that all confidential fund ATM withdrawals are in accordance with instructions using the Purchase Card Reporting System.

Note: Certifying the confidential fund withdrawal via the Purchase Card Reporting System is deemed a critical process, and must be done timely.

5. Promptly returns unexpended funds to the SAC (see section [009.060](#) B.5).
6. Adheres to the reporting process as prescribed in section [009.070](#).

D. Special Agent (SA) Responsibilities

1. Adheres to the recording and reporting process as prescribed in sections [009.040](#) and [009.060](#) D. and E.
2. Promptly returns unexpended funds to the SAC/ASAC (see section [009.060](#) B.5).

E. Each SA/RAC/ASAC must complete [Form OI-28A](#), Transaction Record of Each Advance or Return of Confidential Funds (see [Exhibit 9-1](#)). Form OI-28A is used to record details about fund advances and return of advances to the fund custodian. The ASAC/RAC must place a copy in the case file.

F. Each ASAC/RAC/SA must obtain (if applicable) [Form 28B](#), Receipt for Payment (see [Exhibit 9-3](#)), acknowledging payment to an informant. The form must be completed by the agent and witnessed by a second party. If possible, each informant payment should be witnessed by another agent and/or designee.

009.070 Accountability Report

A. The SAC will submit to CID on a quarterly basis the following documents:

1. Accountability Report, [Form OI-28C](#) (see [Exhibit 9-5](#))
2. Custodian's Transaction Log, [Form OI-28](#) (see [Exhibit 9-4](#))
3. Transaction Record for each entry, [Form OI-28A](#) (see [Exhibit 9-1](#))
4. Receipt for Payment to Informant, [Form OI-28B](#) (see [Exhibit 9-3](#)) – if applicable
5. All documents pertaining to a return of confidential funds (OIG Transmittal Register, copy of money order, and any refund receipts from CID and the OIG Budget office)
6. A copy of a memo or report of investigation that describes the events surrounding the actual use of the funds. (Purchase of documents, etc.)
7. A copy of the DAIGI's approval to deviate from the 15-day requirement to return unused funds (if applicable).

If **no** transactions occur during the quarterly reporting period submit the Accountability Report, [Form OI-28C](#), *only*.

The Accountability Report documents must be submitted to CID no later than the fifth business day of the new quarter.

B. Upon the receipt of the Accountability Reports from the SACs, CID will take the following actions:

1. Review the documents for compliance with the SAH.
2. Update the Confidential Fund Tracking Spreadsheet ((b) (7)(E) ██████████) to acknowledge that the FD has complied with the SAH requirements and the activity for that quarter will be updated on the tab for that FD. If the activity log indicates that a FD has returned funds, the CID ATSAC will contact OCRM and obtain an e-mail confirming that the returned funds have been deposited into the appropriate account.
3. Update the Undercover Operations spreadsheet to indicate the amount of money that has been spent on that particular operation.
4. Once all FDs have complied, CID will generate a memo to the AIGI informing him of the results of the review. All documents related to CID's review will be attached to the memo.

009.080 Periodic Unannounced Audits of Unexpended Confidential Fund Balances

Although unexpended confidential fund balances should be minimal, the OIG may conduct random periodic reviews. SACs must be able to account for the unexpended balances at all times.

[9-1 — Transaction Record of Each Advance or Return of Confidential Funds \(OI-28A\)](#)

[9-2 — OIG Transmittal Register \(OI-28D\)](#)

[9-3 — Receipt for Payment to Informant \(OI-28B\)](#)

[9-4 — Custodian's Transaction Log for Confidential Funds \(OI-28\)](#)

[9-5 — Accountability Report \(OI-28C\)](#)

Exhibit 9-1

**Office of the Inspector General
Office of Investigations
Social Security Administration**

**TRANSACTION RECORD OF EACH ADVANCE
OR RETURN OF CONFIDENTIAL FUNDS**

A. Advance **Date** _____

Special Agent's Name _____

Office _____

Amount Received \$ _____ Case Number _____

Intended Purpose: _____

Advance Approved by _____ Date _____

Advanced Received by _____ Date _____

B. Return of Excess Advance **Date** _____

Special Agent's Name _____

Office _____

Amount Returned \$ _____ Case Number _____

Returned by _____ Date _____

Returned to _____ Date _____

Original filed with Fund Custodian

Copy retained by Special Agent in Case File

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.**

SOCIAL SECURITY
Office of the Inspector General

Transmittal Number 00-

TO: SSA Office of the Inspector General OIG OCRM, HRBLD 2-ME-4 6401 Security Boulevard Baltimore, MD 21235	OIG Transmittal Register
	Confidential Funds

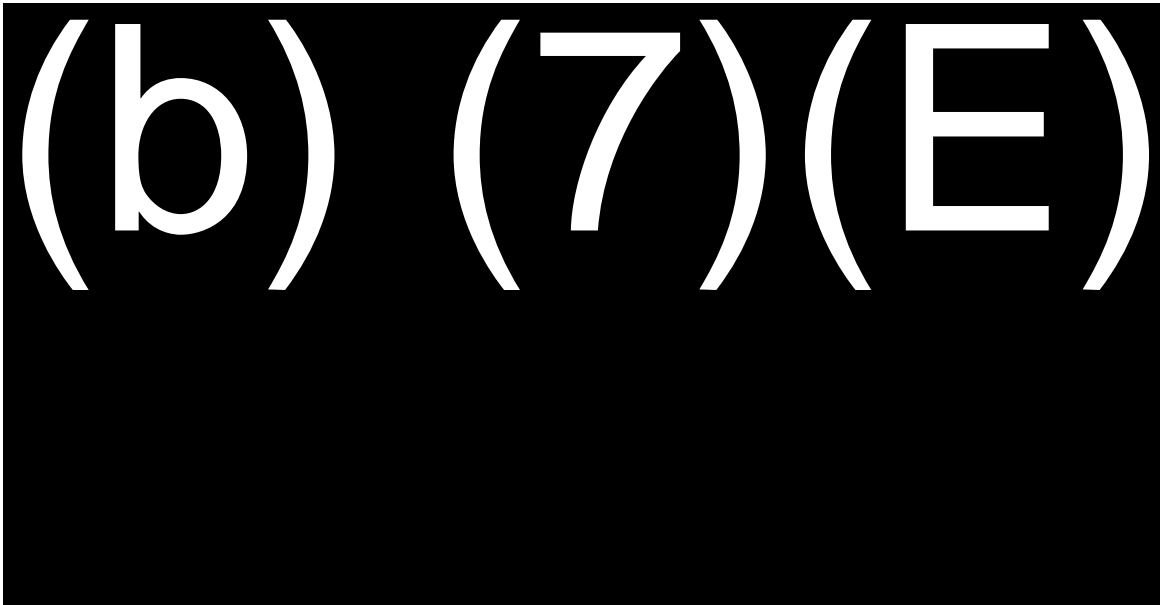
No.	Confidential Funds Deposit Common Acctg. No.	Office	\$ Amount	Money Order No. (*)	Remarks
1.	(b) (7)(E)	Boston			
2.	(b) (7)(E)	New York			
3.	(b) (7)(E)	Philadelphia			
4.	(b) (7)(E)	Atlanta			
5.	(b) (7)(E)	Chicago			
6.	(b) (7)(E)	Dallas			
7.	(b) (7)(E)	Kansas City			
8.	(b) (7)(E)	Denver			
9.	(b) (7)(E)	San Francisco			
10.	(b) (7)(E)	Seattle			

Office of Inspector General Use Only		Office of Finance Use Only	
Signature of Agent Date:		Authorized Signature	
Signature of Supervisor Date:		Date:	
Phone No.		Phone No. (b) (7)(E)	

Please enter the money order number and amount returned on the line for your home office

(*) Make money orders payable to: Social Security Administration

SOCIAL SECURITY
Office of the Inspector General



Special Agent Name _____ Date _____

Witness's Signature _____ Date _____

Original filed with Fund Custodian
Copy retained by Special Agent in Case File

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General
Custodian's Transaction Log

Date	Transaction Type*	Case Number	Special Agent	Amount Received	Actual Amount Expended/ Returned	Balance	Special Agent's Signature	SAC's Signature	Comments

Transaction Types:

- (W) ATM Withdrawal(s)
- (CE) Confidential Expenditure(s)
- (R) Returned Funds to CID

SOCIAL SECURITY
Office of the Inspector General

Accountability Report
(Quarterly)

OI Field Division: _____

_____ Quarter, FY _____

Date: _____

Beginning Cash Balance \$ _____

Were Transactions Made this Quarter (Circle One): Yes No

If **no**, submit this form **only**.

If **yes**, complete the following:

Total Number of **All** Transactions _____

(W) ATM Withdrawal(s) _____

(CE) Confidential Expenditure(s) _____

(R) Returned Funds to CID _____

Dollar Amount of Transactions:

(W) ATM Withdrawal(s) _____

(CE) Confidential Expenditure(s) _____

(R) Returned Funds to CID _____

ATM Withdrawal Fees \$ _____

Ending Cash Balance on Hand at Office \$ _____

Remarks (e.g., explanation of funds on hand past 15 days):

Fund Custodian's Signature _____ Date _____

This form serves as a cover page and is to be accompanied by Form OI-28 and Form OI-28A.

Original to be placed with Fund Custodian's Confidential Fund Records.
Copy to Headquarters via scanned PDF file.

INTERVIEWS, INVESTIGATIVE NOTES, AND STATEMENTS

010.000 Policy Directive

OIG Special Agents shall conduct interviews, advise interviewees of their rights, and obtain statements in conformity with Federal law and this directive. They shall conduct interviews and obtain statements in a fair and impartial manner, with the objective of obtaining the most accurate, relevant, timely, and complete information from the source.

Investigative notes, including those kept electronically, must be retained. These notes must be complete, accurate, objective, free of extraneous information, legible, and prepared contemporaneously with the interview. Notes and other work papers must be maintained in a logically organized manner that allows easy access and identification.

010.010 Purpose of Interviews

An interview is a planned conversation to obtain information about the subject matter of an inquiry. Interviews are conducted with witnesses, informants, sources, and subjects.

A. Information obtained during interviews:

1. explains, confirms, supplements and enlarges upon information in allegations;
2. pinpoints what witnesses observed or heard;
3. helps correlate, identify, and explain physical evidence; and,
4. permits persons involved to admit, deny, and/or explain their involvement and any irregularities that have been identified during the course of the investigation.

Successful completion of an investigation depends on the ability of the SA to obtain accurate facts from a variety of individuals. (b) (7)(E)

(b) (7)(E)

010.020 **General Instructions**

- A. Identification of Agent** – Prior to beginning the interview, the SA will verbally provide his/her name, title, and the office he/she represents to the interviewee, and will display his/her credentials for a sufficient time to the interviewee in order to establish his/her identity and authority. The SA will also identify other individuals who are present during the interview.
- B. Scope of Interview** – An interview should be confined to matters within the scope of an official inquiry or investigation. An interview should not concern private or sensitive issues or characteristics of subjects, witnesses, or others unless directly related to the matter under investigation.
- C. Interview Preparation and Planning** – Effective interviewing depends largely on preparation and the application of knowledge and skills. Special agents should define the investigative issues and elements of proof required to sustain a criminal prosecution, or administrative action. These must be kept clearly in mind to obtain responsive and complete information, and to avoid, where possible, the necessity for re-interviews.
- D. General Guidelines** – To the extent practical, review the background of the person to be interviewed through available records and the testimony of other witnesses. Determine the need for any precautionary measures, and the need, if any, for advice of rights.
1. The person making the complaint on which the investigation is based should usually be interviewed first so that complete details can be obtained. This should be considered even though the information on which the investigation was authorized appears to be complete.
 2. Determine how witnesses relate to the investigation and what information they can provide.
 3. Arrange and mark all documents that will be presented for authentication or identification.
 4. Conduct a pat-down search of the subject, if warranted.
 5. Obtain personal history information ([*Form OI-19, Exhibit 10-1*](#)).
 6. Where technical, colloquial, or slang expressions are used, obtain clarification from the interviewee, especially in written statements.
 7. When eliciting information concerning work procedures or some other activity, do not assume that procedures prescribed in agency regulations or manuals are always followed. Have the interviewee explain what actually happened.

010.030 **Definitions**

- A. Evidence** – Any means by which any alleged matter of fact, the truth of which is submitted for investigation, is established or disproved.

Evidence must be distinguished from information that is or may be conjectured, rumored, or a factually unsupported allegation that a person has committed a crime or other form of misconduct.

- B. Interview** – An interview is the formal and systematic questioning of an individual to elicit information that the individual has, or is believed to have, that is relevant to the topic(s) of the interview.
- C. Custodial Interview** – Questioning initiated or continued after a person has been arrested, jailed, or otherwise deprived of his/her freedom of action in any significant way. The circumstances of the questioning determine whether an interview is custodial - not the investigating agent's beliefs about whether an individual is free to leave.

Extreme care must be used when determining whether the subject is being interviewed in a custodial or a non-custodial situation. Numerous appellate court decisions have consistently upheld that a custodial interview is one in which the *subject believes that his/her movement has been restricted.*

Examples of judicially-recognized custodial interviews include:

1. voluntary and non-voluntary post-arrest interviews;
2. interviews within a jail;
3. interviews including subjects detained by another law enforcement agency at the scene of a raid in which OI participates; interviews in a Government vehicle; and
4. interviews in any other environment where subjects are likely to believe that they have been arrested, or are not free to leave the premises. For example:
 - a. A Federal court determined that law enforcement officers were required to give a defendant Miranda warnings when he was questioned in unfamiliar surroundings in the presence of a security officer, he was not told that he was free to leave or that he did not have to answer the questions, and he was confronted with evidence of his guilt, *United States v Carter*, 884 F. 2d 368 (8th Cir. 1989); and
 - b. Another Federal court determined that Internal Revenue Service agents were required to give a defendant Miranda warnings when he was asked to travel to the Internal Revenue Service office and was then sworn in and questioned in the office by two law enforcement agents. *United States v Gower*, 271F Supp. 644 (M.D. Pa 1967).

Notably, Federal courts have determined that if a federal agent violates a person's constitutional right to receive a Miranda warning during an investigation, the federal agent could be personally liable for damages.

- D. Non-Custodial Interview** – A non-custodial interview is one conducted in a non-coercive environment, in which the subject understands that he/she is not under arrest and is free to terminate the interview and leave the place of interview at any time. Again, the determination of whether a subject is in a non-coercive environment and feels free to leave is based on the circumstances of the questioning, not the agent's belief that the subject is free to go.
- E. Subject** – Any person who appears, by evidence, to be involved in the relevant offense(s) and/or misconduct under investigation.

- A. **Two-Agent Interviews** – A second SA or other law enforcement officer present during an interview provides additional security to the interviewing SA, acts as a witness to the circumstances of, and any statement made by, others present at the interview, and facilitates the accurate and timely recording of interview notes.

(b) (7)(E) [Redacted]
 Unless precluded by extenuating circumstances, the witness should be a law enforcement officer, an SSA OIG employee, an SSA employee, or another appropriate government employee. The circumstances surrounding subject interviews must be documented in the Report of Investigation ([Form OI-4](#), [Exhibit 10-2](#)).

Two investigators should be present when conducting interviews in potentially hazardous or compromising situations, including, but not limited to, the following:

- (b) (7)(E) [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

When two or more law enforcement officers conduct an interview, the case agent is responsible for thoroughly briefing the other participating agent(s) and/or law enforcement officers on the particulars of the investigation prior to the interview.

Cooperative Disability Investigations (CDI) Program’s policies:

The requirement for (b) (7)(E) interviews may be waived if the CDI Unit Investigator’s home agency policy allows for single agent/investigator/officer interviews, and if the CDI Unit Team Leader concurs that a witness (second law enforcement officer or any other person) does not need to be present for the interview.

(b) (7)(E) [Redacted]

(b) (7)(E) [Redacted]

(b) (7)(E) [Redacted]

(b) (7)(E)

The policy regarding established safety and security protocols remains in effect for interviews, surveillances, and/or subject observations conducted in (b) (7)(E)

- B. Notes of Interview** – How and when to take notes depends on the circumstances of the case, the complexity of the issues, and the personality of the interviewee.

Notes of Interview are discussed in more detail in [Section 010.080](#), Investigative Notes.

- C. Electronic Recording of Statements** - Effective July 11, 2014, a Department of Justice Policy ([DOJ Policy Concerning Electronic Recording of Statements](#)) was established concerning the electronic recording of statements. The policy establishes a presumption in favor of electronically recording statements made by individuals in custody (custodial interviews), with certain exceptions, and the policy encourages special agents and U.S. Attorneys to consider electronic recording of interviews outside of custodial interviews. However, it is suggested that special agents and U.S. Prosecuting Attorneys consult with one another in those circumstances before an electronic recording is conducted.

1. **Presumption of Recording** – There is a presumption that the custodial statement of a person in a place of detention with suitable recording equipment, following arrest but prior to an initial appearance, will be electronically recorded, subject to the exceptions below. Such custodial interviews will be recorded without the need for supervisory approval

a. **Electronic Recording**- The use of video recording to satisfy the presumption is encouraged; however, when suitable video recording equipment is unavailable, an audio recording may be utilized. The following considerations should be given for video and/or audio recordings:

- i. A recording must begin with the special agent stating the date, time, and place of interview, and identities of all persons present. The interviewee’s verbal acknowledgement of consent must be recorded, if applicable.
- ii. When the recording is completed, the recording (CD, DVD, etc.) must be permanently labeled by subject’s name, case number, date, person interviewed, name of interviewer, witnesses, and location. Protect the recording in the same manner as evidence.
- iii. If necessary, transcribe the recording. Subjects or witnesses may request transcripts. Such requests will generally be honored if a transcript was made of the recorded interview. If not, a copy of the recording itself may be provided. In any event, special agents are required to obtain authorization from their supervisors and/or from the appropriate prosecuting entity *prior* to release of transcripts and/or recordings.

b. **Custodial Interviews** – Currently, the presumption only applies to interviews of persons in SSA OIG custody. Interviews in non-custodial settings are excluded.

c. **Place of Detention** – A place of detention is any structure where the individual is held in connection with Federal criminal charges where they can be interviewed, which can also include any state, local, or tribal law enforcement facility, office, correctional/detention facility, jail, police/sheriff’s station, holding cell, or other structure used for holding of the individual facing

charges. Recordings under this policy are not required while a person is waiting for transportation or is en-route to a place of detention.

d. Suitable Recording Equipment – The place of detention must have suitable recording equipment. Suitable recording equipment constitutes:

- i. an electronic recording device deemed suitable by the U.S. Attorney and the SSA OIG for the recording of interviews that,
- ii. is reasonably designed to electronically capture the entire interview; (b) (7)(E)
[REDACTED]
- iii. For post-arrest custodial interviews in places of detention not controlled by the SSA OIG, special agents will decide on a case-by-case basis whether the recording equipment is suitable under the circumstances. Recording devices or systems approved for official use for other agencies (b) (7)(E) [REDACTED] capable of capturing the entirety of the interview should generally be considered suitable.

e. Timing – The presumption applies to persons in custody in a place of detention with suitable recording equipment following arrest but who have not yet made an Initial Appearance before a judicial officer under Federal Rule of Criminal Procedure 5.

f. Scope of Offense – The presumption applies to interviews in connection with all Federal crimes.

g. Scope of Electronic Recording – The electronic recording will begin as soon as the subject enters the interview area/room and will continue until the interview has been completed. The recording should cover all discussions and activity conducted during the interview, including the reading/advisement of Miranda Rights as well as a question and answer segment designed to demonstrate that the interviewee's statements are voluntary and not the product of coercion.

h. Electronic Recording (overt or covert) – The electronic recording may be overt or covert. Covert recording constitutes consensual monitoring, pursuant to Title 18 U.S.C. 2511(2)(c). Surreptitious recordings of interviews require approval from a DOJ attorney and a Deputy Assistant Inspector General for Investigations, or designee (*see Section 008.070*).

2. Exceptions to the Presumption – A decision to not electronically record an interview that would otherwise presumptively be recorded under this policy must be documented in the Form OI-4 by the special agent as soon as practicable. Such documentation shall be made available to the U.S. Attorney and should be reviewed in connection with a periodic assessment of this policy by the U.S. Attorney and the Special Agent in Charge or their designees.

a. Refusal by Interviewee – If the interviewee is informed that the interview will be electronically recorded and indicates he/she is willing to provide a statement but only if the interview is not recorded, then an electronic recording does not need to be conducted. However, the special agent must document this exemption in the Form OI-4.

b. Public Safety and National Security Exception – Electronic recording is not prohibited in any of the circumstances covered by this exception and the decision whether or not to record should be wherever possible be the subject of consultation between the special agent and the prosecutor.

There is no presumption of electronic recording where questioning is conducted for the purposes of gathering public safety information.

NOTE: The presumption of electronic recording does not apply to circumstances where questioning is undertaken to gather national security-related intelligence or questioning involving intelligence, sources, or methods, or the public disclosure of which would cause damage to national security.

c. Electronic Recording is not reasonably practicable – Circumstances (i.e. recording equipment malfunction, the unexpected need to move the interview, or the need for multiple interviews in a limited timeframe exceeding the number of recording equipment devices available) may prevent, or render not reasonably practicable, the electronic recording of an interview that would otherwise be presumptively recorded.

d. Residual Exception – The presumption in favor of recording may be overcome where the U.S. Attorney and the Special Agent in Charge, or their designees, agree that a significant and articulable law enforcement purpose requires setting the recording of the interview aside. This exception is to be used sparingly.

(b) (7)(E)



4. When an interview has been recorded, a Report of Investigation (Form OI-4) must still be completed within 10 days of the interview. The recording should be utilized while documenting the interview on Form OI-4. The Form OI-4 must include the following:

- i. Official identity of the interviewing special agent(s).
- ii. Purpose of interview.
- iii. Identity of the individual recorded.
- iv. Details of the recorded session – date, time, start and stop periods, and reason(s) for stopping.
- v. Other relevant individuals, organizations, companies, or other entities mentioned for the purpose of indexing to allow for future word search capabilities.
- vi. The interviewee/arrestee's voluntary waiver of rights and execution of the "Advice of Rights" form (Form OI-13).
- vii. Summary of the interview.
- viii. The following caveat language must be included at the beginning of the "Investigative Activity" section of the Form OI-4:

“The below is an interview summary. It is not intended to be a verbatim account and does not memorialize all statements made during the interview. Communications by the parties in the interview area/room were electronically recorded. The recording captures the actual words spoken.”

- D. Interviewing the Opposite Sex** – When interviewing a member of the opposite sex, especially in a hostile situation and/or a remote location, it is strongly recommended that the interviewing SA conduct the interview in the presence of at least one witness. The witness should not be connected to the investigation, or be a friend or relative of the subject of the investigation. The witness to the interview must be identified in the interview notes, and in the Report of Investigation, if applicable.
- E. Interviewing Juveniles** – For purposes of the SSA OIG, a “juvenile” is defined as a person who has not attained his or her 18th birthday.

Because of the requirements and prohibitions contained in the Juvenile Justice and Delinquency Prevention Act of 1974 (18 U.S.C. § 5031), as amended, agents must take special precautions when interviewing juvenile suspects.

1. Whenever a juvenile suspect is taken into custody, the agent shall immediately, or as close thereto as practical:
 - a. Advise the juvenile of his/her legal rights *in understandable language*.
 - b. Notify the appropriate United States Attorney’s Office of the arrest.
 - c. Notify the juvenile’s parent(s), guardian, or custodian of such custody.
2. The rights of the juvenile in custody and the nature of the offense shall also be conveyed to the parent(s), guardian, or custodian. If parental consent to interview the juvenile was obtained, it must be noted in the Report of Investigation.
 - a. There is no legal requirement to have a parent, guardian, or custodian present during a juvenile interview, whether custodial or *as an onlooker or source of information*.
 - b. It is *strongly recommended*, however, to the maximum extent practical, that one or more of the specified individuals are present, prior to questioning the juvenile.
3. A witness to the interview is strongly recommended to protect the juvenile’s “due process” requirements.
4. Grant the request to a juvenile *of any age* who asks to have an adult present, regardless of involvement.
5. Applicable State laws regarding interviews with juveniles should be researched and adhered to. If regulations are in question, the State Attorney General’s office should be contacted to determine the existence of such laws prior to interviewing juveniles.
6. The juvenile shall not be detained for longer than a reasonable amount of time before being released, transported to a magistrate, or transferred to the custody of another agency. The agent must be able to articulate the reasonableness of the length of detention.

- F. Hospitalized Persons** – Prior to interviewing any hospitalized person, the agent will contact the patient's physician and determine if the patient's condition will permit the interview, and whether there are any restrictions. This requirement will not normally apply to persons ill at home or being treated as outpatients.
1. The patient's physician may wish to know the nature of the interview in order to properly assess the effect on the patient. Supervisory and patient approval is *required prior* to the release of any information to the patient's physician. Any information furnished to the physician must adhere to the provisions of The Right to Privacy Act, and all other applicable provisions of law. If requested by the patient/interviewee, the physician or nurse may be permitted to be present during the interview, provided they are not personally involved in the investigation.
 2. Prior to interviewing a hospitalized patient who is mentally ill, the physician will be questioned regarding the person's current mental state, capacity to remember events, and ability to answer coherently and reliably.
 3. Contacts with physicians for the reasons listed above will be recorded in a Report of Investigation.
- G. Whistleblowers** – The identity of a "whistleblower" cannot be disclosed without that person's consent unless the Inspector General determines such disclosure is unavoidable during the course of the investigation, as stated in § 7 of the IG Act of 1978.
- H. Confidential Informants** – A confidential informant outside the definition of "whistleblower" who furnishes significant information while simultaneously requesting confidentiality must be told by the SA or other involved OIG employee that an *absolute* pledge of confidence cannot be given by the SA or OIG employee. Said notification *must* be contained in the initial Report of Investigation. Every reasonable and lawful method of protecting the identity or informant status of the confidential informant will be made, including using the information provided to establish the facts from other sources, and using a Grand Jury subpoena to remove the voluntary nature of information provided.
- Additional information concerning Pledges of Confidence is located in Chapter 4, SSA Internal Investigations, [Section 004.220](#).
- I. Report of Interview** – A Report of Investigation will be drafted within 10 days after completion of the interview, and the drafting date must be included. In a joint investigation, another agency's report of interview may be incorporated in an OIG OI Report of Investigation.

010.050 Advice of Rights

- A. Legal Issues** – The Fifth and Sixth Amendments to the United States Constitution provide individuals the basic guarantees to be free from compulsory self-incrimination and to be represented by counsel in criminal proceedings.
1. **Constitutional Law** – The Fifth Amendment to United States Constitution states: “No person shall be held to answer for a capital or other infamous crime unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the militia, when in actual service, in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; **nor shall (any**

person) be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use without just compensation” (emphasis added).

2. **Decisions of the United States Supreme Court** – Through decisions including **Miranda v. State of Arizona**, [384 US 436](#) (1966); **Escobedo v. State of Illinois**, [378 US 478](#) (1964); and **Gideon v. Wainwright**, [372 US 335](#) (1963), the United States Supreme Court established the right of an individual to have the assistance of counsel, if interrogated while in custody or deprived of his/her freedom in any significant manner. In so doing, the Court has not only affirmed the privilege against self-incrimination and the entitlement to the assistance of counsel as fundamental rights, but also established that individuals must be properly advised of their constitutional rights and waive those rights if statements taken are to be admissible in a subsequent criminal trial, **Dickerson v. United States**, [166 F.3d 667](#) (2000).
3. **Non-Custodial Interviews** – The Court has consistently refused to extend the right to counsel during non-custodial interviews. The right to counsel is established only during custodial interrogations, although it has interpreted the meaning of “in custody” to extend to “deprived of freedom of action in any significant way” (**U.S. v. Curtis**, [568 F. 2^d 643](#) [9th Cir., 1978]). The determination of whether a subject is in a non-custodial interview and feels free to leave is based on the circumstances of the questioning, not the agent’s belief that the subject is free to go.

B. Conditions and Requirements for Advice of Rights – Subjects must be advised of certain rights consistent with the circumstances enumerated as follows:

1. **Custodial** – A subject **must** be advised of his/her rights under Miranda ([Exhibit 10-3](#)) before the interview when the subject:
 - a. has been arrested;
 - b. is incarcerated in a jail, prison or other confinement facility;
 - c. whether in custody or not, has been previously arrested or otherwise formally charged and prosecution is pending, and the subject matter of the interview concerns the pending Federal charge or related Federal offense;
 - d. is the “target” of a criminal investigation and the prosecutor handling the case instructs that Miranda advices be given; or
 - e. is otherwise deprived of his/her freedom in a significant manner. This issue is resolved by considering the factors known by the individual evaluated objectively by a reasonable person. In other words, given the facts known by the person being interviewed, would a reasonable, innocent person feel that they are not free to leave? If so, they are “in custody” for the purposes of the need to provide Miranda rights. The surroundings, language, extent of confrontation with evidence of guilt and pressure to detain must all be considered factors in making this determination.

For example, a Federal court has held that agents were required to give a subject Miranda warnings when the subject was questioned in an Internal Revenue Service

office, came to the office voluntarily, and was sworn-in and questioned by two agents. The court determined that in evaluating a deprivation of freedom of action, the influence that the atmosphere and surroundings of government-oriented facilities had on the free choice of the person being interrogated had to be taken into consideration. The court also noted that coercion could be physical or mental. *United States v Gower*, 271 F Supp. 655 (M.D. Pa 1967).

2. **Non-Custodial** – There is no constitutional or judicially imposed requirement for a person who is interviewed in a non-custodial situation to be advised of their Miranda rights. A Non-Custodial Advice of Rights ([Form OI-13 NC](#), [Exhibit 10-4](#)) is to be used in those circumstances where it is necessary to advise a subject that he/she is not in custody and is free to leave or terminate the interview at any time. The circumstances generating the need for such advice generally include:
 - a. cases where a prosecutor has requested that some form of advice of rights less than full “Miranda” be given;
 - b. when an interview is initiated with a government employee;
 - c. when the individual asks what his/her rights are; or
 - d. when the circumstances leading to an interview are likely to cause confusion about the subject’s right to leave or terminate the interview. Such a situation could occur when an employee is ordered by his or her supervisor to be present for an interview.
- C. **Delayed or Follow-up Interviews** – If there is an interruption between the advice/waiver and the start of a subject’s interview, or between the initial advice/waiver/interview and a subsequent interview, advise the subject again of his/her rights, and obtain a new waiver prior to the interview.
- D. **Subject Who Does Not Understand English** – The subject must be advised of his/her rights by a person who is fluent in a language understood by the subject, and asked if he/she understands his/her rights and if he/she is willing to waive his/her rights. Document the circumstances of the advice and waiver, and consider recording the interview.
- E. **Methodology** – Advise the subject orally of the matter under investigation. The explanation should be sufficiently detailed and phrased so that the subject is made aware of the scope of the investigation. The explanation should be as precise as possible; but should not include a discussion of the case or any disclosure of information not absolutely needed.
 1. Read the "Advice of Rights" portion of the appropriate OIG Advice of Rights ([Forms OI-13, 13S \(Spanish\) and 13NC, Exhibits 10-3, 10-4, and 10-5](#)). If the subject understands his/her rights and is willing to answer questions, have the subject complete the "Waiver of Rights" portion of the OI-13 by signing and dating the form to certify that he/she read, understood, and waived their rights. The SA should sign and date the waiver as a witness, as should all other witnesses to the waiver.
 2. If the subject understands and waives his/her rights and consents to be interviewed, but refuses to sign the waiver form, note on the lower right corner of the form that
 - a. the form was read to the subject; and

- b. the subject orally waived his/her rights; and
 - c. the subject agreed to be interviewed; and
 - d. the subject refused to sign the form.
3. If the subject declines to waive his/her rights and does not wish to be interviewed, honor his/her invocation of rights and cease the attempt to interview.

F. **Request for Legal Counsel** – If the subject requests an attorney to be present during the interview, or if the subject wants to consult with an attorney before signing the waiver form, **do not** interview the subject. If the subject wants a court-appointed attorney, refer the request to the appropriate U.S. Attorney's Office.

In accordance with constitutional requirements, attorney representation must be permitted if an interview is conducted in custody or in another manner which deprives the subject of freedom in any significant way, or if adversarial judicial proceedings have been initiated by way of formal charge, preliminary hearing, indictment, information, or arraignment. To determine if a particular event or proceeding will constitute the commencement of adversarial criminal proceedings requires both an examination of the rules of criminal procedure for the jurisdiction in which the crime is charged and the Supreme Courts cases dealing with the issue of when formal prosecution begins. *Michigan v. Jackson*, 475 U.S. 625, 632 (1986); see also *Brewer v. Williams*, 430 U.S. 387, 398 (1977). Once an adversarial criminal proceeding commences, the right to counsel would apply to all of the critical stages of prosecution and investigation. A critical stage is 'any stage of the prosecution, formal or informal, in court or out, where counsel's absence might derogate from the accused's right to a fair trial.' *United States v. Wade*, 388 U.S. 218, 226 (1967); see also, *United States v. Hidalgo*, 7 F.3d 1566 (11th Cir. 1993).

G. **Avoidance of Informal Agreements** – Promises and representations made informally can adversely affect criminal liability. **Under no circumstances** should an agent or other SSA OIG official enter into an informal understanding or agreement with a witness concerning the cooperation of that witness without prior consultation with, and approval of, the Special Agent-in-Charge, and the U.S. Attorney's Office, as appropriate. Such agreements are likely to be interpreted by witnesses as waiving potential criminal liability or accountability to the Agency in exchange for cooperation in the SSA OIG investigation.

H. **Reporting Requirements** – A Report of Investigation detailing the interview of a subject(s) must indicate what form of advice of rights was provided (e.g., Miranda or non-custodial), and what affirmative verbal waiver was given (e.g., "yes, I understand," etc.), or that the subject executed the Advice of Rights/Waiver form.

010.060 **Conducting the Interview**

A. **Interview Techniques** – A significant portion of an investigation is devoted to interviewing witnesses. As such, it is essential to develop proper and effective methods of obtaining the facts.

(b) (7)(E) [REDACTED]

[REDACTED]

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

[Redacted]

B. Analyzing Answers – As the interview proceeds, analyze each answer to see that it is responsive to the question, accurate in light of known information, and complete.

(b) (7)(E) [Redacted]

[Redacted]

[Redacted]

C. Concluding An Interview – Properly concluding an interview is an extremely effective method of determining if all of the pertinent areas have been discussed, and all pertinent responses properly recorded.

1. Insure that all items on the interview outline have been covered with the interviewee.
2. In a long and/or complex interview, briefly summarize the information furnished by the interviewee. This will give the interviewee a chance to verify facts discussed, recall additional details, and make any additions or corrections.
3. Be alert to learn of other sources of information from the interviewee.
4. If it appears likely that the interviewee may obtain or remember additional information, make certain that the interviewee knows how to contact you with the least amount of effort.

010.070 Obtaining Descriptive Factors

In some cases, the most important information to be obtained during an interview is the description and identification of the offender or principal figure of interest. In obtaining a description, follow a logical order establishing the subject's gender, ethnic origin, age, height, weight, hair and eye color, and clothing.

- A. If the witness knows the subject of interest, attempt to obtain a photograph and profile of the subject.
- B. When relevant, interviewing SAs should complete an OI Personal History Information Form (OI-19) to record information furnished by a witness about a subject.

010.080 Investigative Notes

The fact that notes are often admissible at trial emphasizes the importance of following OIG policy regarding notes.

- A. **Notes of Interview** – Notes corroborate oral statements. One of the most important factors in determining whether the notes will withstand judicial scrutiny is whether the notes contain a time log. The time log may be as simple as the time the interview started and the time concluded, or it may be as complex as noting the times that pertinent remarks and/or admissions were made, which is much more preferable in terms of evidentiary value and recollection of past events.

Additional items that should be noted in the time log include telephone calls made or answered by the interviewee, and any occasions where the interviewee is out of sight of the interviewer(s); for example, if the interviewee were to go to the restroom unescorted.

- 1. Note the date, location, and circumstances surrounding the interview.
- 2. Use quotation marks to reflect that oral information is being set out verbatim, i.e. direct quotes.

3. (b) (7)(E) [Redacted]

4. (b) (7)(E) [Redacted]

5. (b) (7)(E) [Redacted]

6. (b) (7)(E) [REDACTED]
7. (b) (7)(E) [REDACTED]
8. (b) (7)(E) [REDACTED]

- B. Notes of Record Examination** – Take detailed notes of records examination which contain all relevant information needed for a verbatim copy of a document or record, an abstract of its contents, or a listing of pertinent data or figures from a record or voluminous records.
1. Transcribe information from records in a manner and form that will make it most accessible for later use. It can be written in either narrative or schedule form. Some record information will require listing on columnar paper or in an electronic medium with suitable headings.
 2. Where notes are prepared from examination of information contained on specific business forms, obtain a copy of the blank form and retain it with the notes.
 3. If a small number of business forms are involved, make copies of the forms rather than recording information in the notes.
 4. Include in the notes information concerning all files and records examined, location of records, who made them available, and the name and title of the custodian of the records.
 5. When an original document cannot be removed or copied and there is a possibility that it may be altered or replaced before trial, consider placing your initials or other identifying mark on the reverse side, or at some other obscure place on the document. Enter the fact that such marking was made in the investigative notes.
 6. When appropriate, the custodian of records or the person who prepared the records may be asked to examine a schedule prepared from the records. If that person compares the entries in the schedule with the original documents, verifies any computations for accuracy, and agrees that all pertinent documents were examined, have the person sign or initial the schedule certifying that it is a correct abstract of information in the records. The schedule will then assume the nature of a signed statement.
- C. Notes of Surveillance** – Record beginning and ending dates, and times of all significant actions associated with the surveillance, and describe those significant actions in the notes. For a moving surveillance, record all pertinent locations, addresses, landmarks, etc. If still or video pictures are made during the surveillance, the notes will help correlate and corroborate the times and locations of the pictures. Ensure that the person who made each observation is specifically identified following the event listed.
- D. Maintenance of Notes** – Release of notes to the subject may be required if requested under the Freedom of Information or Privacy Acts. The notes can also be introduced into evidence at the request of either the prosecution or defense in criminal, civil, or administrative hearings. Therefore, the original notes taken contemporaneously with an interview or immediately

following must be maintained in the case file. Only record personal information about an individual that is relevant to the objectives of the investigation.

- E. **Arranging and Submitting Work Papers** – Place work papers in envelopes; label the envelopes to show “Work Papers”; and file them in the case file. Extraneous documents or papers (i.e., MapQuest directions) that can be later retrieved in their original form need not be retained.
- F. **E-mails** – E-mails between criminal investigators and supervisors or prosecuting attorneys may be considered as investigative notes, and thereby are considered as discoverable to defense attorneys.

010.090 Statements

Any interview that might later come under the scrutiny of judicial inquiry should be preserved in some form. An organized system should be used in recording the results of an interview. That end product could be in the form of interview notes. It could also be in the more preferable and formal design of a statement. It should be noted that a statement is not necessarily a confession, but rather a basic declaration of information provided by the interviewee during the interview. Although a sworn written statement is usually the most preferable form of statement to obtain, oral, unsigned or non-sworn statements may also be judicially acceptable. Agents should inquire with the prosecuting attorney to determine what type of statement is preferred in each jurisdiction.

- A. **Oral Statements** – The most important factor to remember about oral statements is that the interviewer should translate the interview into written form, as accurately as possible, as soon as possible after the statement is made. The ideal situation is to make comprehensive notes as the interviewee is speaking. If that is not advisable or possible, commit specific quotes and substantive information from the interviewee to memory for later transcription.

The second most important factor regarding oral statements is corroboration. The primary method is one or more additional witnesses. The names of the additional witnesses need to be recorded in the Report of Investigation.

If notes can be reduced to writing as the interviewee is speaking, make certain to include a timeline in the notes, with specific emphasis on the times that the interviewee made explicit admissions or revelations.

- B. **Written Statements** – There are several types of written statements used in law enforcement including the narrative statement, and the question and answer statement. In the SSA OIG/OI, the narrative format is generally preferred.

Whenever possible, agents should elicit written statements from all likely subjects who are interviewed. Those statements should be taken near the conclusion of the interview, and serve as an adjunct to the interview. The written statement should mirror the oral admissions or denials that were made during the interview.

Written statements are significant because they:

1. preclude the likelihood of denial by the interviewee of information contained in the statement;

2. render less likely a change of testimony on the part of the maker;
3. impeach the testimony of the maker if the maker testifies in a contrary manner;
4. refresh the maker's recollection if the individual later forgets information furnished in the statement;
5. rebut charges that the maker was misquoted;
6. enable the prosecuting attorney to prepare and present a case more effectively; and
7. become admissible as evidence in certain circumstances, e.g., a confession, even if the maker refuses to take the stand at trial.

C. Exculpatory and False Exculpatory Statements – (b) (7)(E)

The purpose of obtaining these statements is to restrict the subject from altering the account of facts of the violation to a set of facts that would be more beneficial to his or her eventual defense. A false exculpatory statement is an extremely effective prosecutable tool for impeaching the credibility of a defendant at trial.

Statements given by subjects or witnesses that contain false information or denials may be used against those individuals provided they have been lawfully obtained. They may also be used to support *independent* charges against the subjects or witnesses.

D. Statement Guidelines – It is important, particularly in a confession, that the statement includes all information possessed by the subject pertaining to the elements of the violation. "State of mind" is a requisite in proving most financial crimes. If a subject confesses that he/she knew his/her actions were "criminal," "illegal," etc., include language to that effect in the written statement.

1. Preserve statements in their original condition, and handle as documentary evidence.
2. Witness Statements ([Form OI-16A](#), [Exhibit 10-6](#)) are to be used to take written statements from witnesses and, in some cases, non-custodial subjects. Non-Custodial Advice of Rights Statements ([Form OI-16B](#), [Exhibit 10-7](#)) are to be used in non-custodial interviews where the interviewee was advised of certain rights short of a full Miranda advice of rights. Full Miranda Statements ([Form OI-16C](#), [Exhibit 10-8](#)) are to be used when the interviewee has been advised of his/her complete rights under the Miranda Decision. Statement Continuation ([Form OI-16D](#), [Exhibit 10-9](#)) is to be used as a continuation page for all statements requiring more than the required first and last pages of the statements. Statement Signature Page ([Form OI-16E](#), [Exhibit 10-10](#)) is to be used as the last page of all statements.
3. If explanations and information concerning justification or mitigation of violations, or irregularities are furnished by the maker, include those in the statement, usually in one or more of the concluding paragraphs.

4. (b) (7)(E) [REDACTED]
5. (b) (7)(E) [REDACTED]
6. Prepare statements in the first person, and use language readily understandable by the person making the statement.
7. (b) (7)(E) [REDACTED]
8. All pertinent information furnished by the interviewee, but which the interviewee refuses to include in the written statement, should be accurately recorded in the report of investigation notes for later use as oral testimony.
9. Pertinent facts developed after the original signed statement was obtained may be incorporated in a supplemental statement. (b) (7)(E) [REDACTED]
10. There is seldom reason to include obscene language in a written statement. Its use should be discouraged, except in specific circumstances such as when the maker insists; or when the use of the language is clearly material or relevant; or in those rare instances when the language would usefully tend to characterize the maker.

E. When to Take a Statement – Obtain a written statement, sworn or non-sworn, unless the prosecutor advises otherwise, when it will serve a definite purpose that outweighs likely disadvantages. A sworn written statement usually should be obtained in instances involving:

1. A confession (direct acknowledgment of guilt).
2. An admission against interest (acknowledgments from which guilt or liability may be inferred) by the person under investigation or implicated in an investigation.
3. Testimony of a material witness.
4. A high probability that a person may change or retract his or her testimony, where it appears that the present statement is truthful. (b) (7)(E) [REDACTED]
5. An interview of the subject of any investigation that may lead to disciplinary, fiscal, or legal action, even though the subject denies all allegations.
6. Circumstances where the truth is more likely to be obtained through the use of a written statement. Sometimes an individual is more likely to tell the truth if placed under oath or affirmation before telling the final version of the story. For example, where there is good

reason to believe that the interviewee is deliberately withholding information or not telling the truth, or that the interviewee may later change or retract the statement.

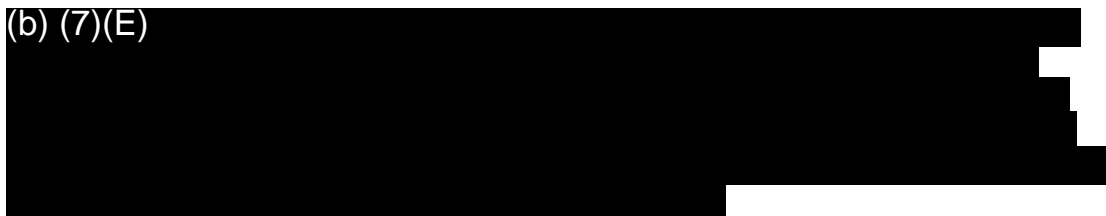
F. Methodology – The substance of a statement is the same for all types of statements. The format, preamble and closing paragraph of the statement and affidavit or sworn statement will vary as previously described in this section.

1. The basic format of the statement is narrative form. It allows the interviewee to relate the information and avoids the use of leading or suggestive questions. The interrogatory form (question and answer type) may be used when the content of the interview is highly technical, and can be better understood in a specific question and answer outline.
2. Although the interviewee is making the statement, it is preferred that the SA prepare the statement unless the interviewee insists on doing so. If the SA prepares the statement, document on the face of the statement that the statement has been written by the SA with the consent of the interviewee.

By having the SA prepare the statement, the SA can better ensure that it is legible, contains all material information, does not include irrelevant information, and is responsive to the investigation. The statement can also be organized in the most suitable way for use in the Report of Investigation.

3. Although the interviewer may actually prepare the statement, remember that the statement is that of the *interviewee*. If the interviewee desires to give partial or incomplete information, or elects to include unnecessary explanations, or even irrelevant material, that must be permitted. Conversely, it is the job of the investigator to guide the interview and the written statement, to the extent practical, to obtain truthful, relevant, material, and complete information.

4. (b) (7)(E)



5. The statement can be typed, handwritten, or hand printed, but it must be legible.
6. The opening paragraph:
 - a. must identify the interviewee and SA(s) by name;
 - b. must affirm that the statement was made voluntarily to the SA(s) in their official capacity; and
 - c. must reveal that the interviewee was advised of his/her rights under the Miranda Decision *prior* to completing the statement, as appropriate.
7. The second paragraph should contain enough information to identify the interviewee as distinct from other persons. This should include full name, address, present occupation, and other information that is essential to identify the interviewee. Show all names used by the

witness, including any common nickname(s). If the interviewee has special knowledge, training, or experience that might qualify him/her as an expert witness, briefly explain that in the identification paragraph, if it is pertinent to the case.

8. The body of the statement needs to include all of the pertinent information furnished by the interviewee, whether for or against the interviewee's interests. Prepare the statement in a clear, concise, and organized manner.
9. The last page of the statement should contain a portion of the substantive text, and should not consist of only the closing paragraph and signatures.
10. Identify each page number and total pages on the bottom of each page, e.g., "Page 1 of 3 pages".

- G. Corrections, Additions, and Changes** – Give the interviewee full opportunity to make any corrections, additions, changes, etc., to the statement prior to signing. If the interviewee asks to take a copy of the statement for study or advice prior to signing it, accede to this request. Afterwards, the interviewee should initial all corrections and sign the statement in presence of the SA, so that the SA can witness the interviewee's approval of the corrections and signing of the statement. Corrections to the statement should be made in the interviewee's own handwriting and initialed alongside the corrections. Those corrections provide support that the interviewee read and understood the statement.

Have the interviewee place the date he/she is signing the statement immediately below the closing paragraph. Have the interviewee initial at the place of each correction, addition, or other change in the statement, sign at the bottom of all pages (except the last), and then sign the last page immediately below the date. The signature should conform to the name in the opening paragraph. The interviewee's name should be typed or hand printed below the signature block prior to the signing.

- H. Signature and Date** – It is proper to point out to the interviewee that a signed statement provides an opportunity to present a true recital of his/her side of the case, helps to prevent misunderstanding of testimony, and evidences cooperation. Do not use intimidation, inducement, or force of any kind to obtain a signature on a statement.

After the subject or witness has read the statement, made corrections, and initialed and dated the top and bottom of each page, the subject or witness should sign his/her full name to the statement.

- I. Witnessing Statements** – The person(s) who witnessed the interviewee's signing of the statement are to sign below the signature of the interviewee. The SA is always a witness to statements signed in his/her presence.

010.100 Oath or Affirmation

Section 6(a)(5) of the Inspector General Act Amendments of 1988, Public Law 100-504, enacted on October 18, 1988, authorizes the Inspector General to designate to Office of Inspector General employees the authority "to administer to or take from any person an oath, affirmation, or affidavit, whenever necessary in the performance of the functions assigned by this Act..." The Inspector General has delegated that authority to SSA OIG Special Agents.

C. **Letter or Memorandum Statement** – Sometimes a person may decline to furnish a written statement at the conclusion of an interview, but return the next day with a letter or memorandum confirming the content of the interview. If this occurs, accept the letter or memorandum and, if not already signed, ask the interviewee to sign it. Furthermore, if possible, insert an oath or affirmation, and have the person swear or affirm to the statement. Sign and date the statement as appropriate.

D. **Request for a Copy of Statement** – If the interviewee or his representative requests a copy of the statement, it should be provided only after the statement has been signed and properly witnessed, preferably by the representative. Once the case has been referred outside the OIG, refer the request to the office to which the referral has been made.

E. **Language or Disability Situations** – Interviews are a form of communication between two or more people. Legitimate barriers to that communicative process must be overcome in order to safeguard the integrity and the quality of the interview. (b) (7)(E)



1. If the person is illiterate, read and clearly explain the contents of the statement, making corrections as necessary. Amend the closing statement to reflect that the contents were read to the interviewee. Ask the interviewee to place his/her mark at the end of each page. Two witnesses should witness the placement of the interviewee's mark.
2. Similarly, a blind person's statement should be read aloud. Two people should witness the interviewee's acknowledgment of the correctness of the statement.
3. Other circumstances such as deafness or physical impairments may require the SA to take extra measures to assure the person acknowledges the correctness of the statement.
4. If the interviewee cannot speak or write English, use a reliable interpreter. The statement should be in a language the interviewee understands. A translation into English must also be obtained.

Chapter 10 — EXHIBITS

[10-1 — Personal History Form \(OI-19\)](#)

[10-2 — Report of Investigation \(OI-4\)](#)

[10-3 — Advice of Rights \(OI-13\)](#)

[10-4 — Advice of Rights- Non Custodial \(OI-13 NC\)](#)

[10-5 — Advice of Rights –Spanish \(OI-13 S\)](#)

[10-6 — Witness Statement \(OI-16A\)](#)

[10-7 — Non-Custodial Advice of Rights Statement \(OI-16B\)](#)

[10-8 — Full Miranda Statement \(OI-16C\)](#)

[10-9 — Statement Continuation \(OI-16D\)](#)

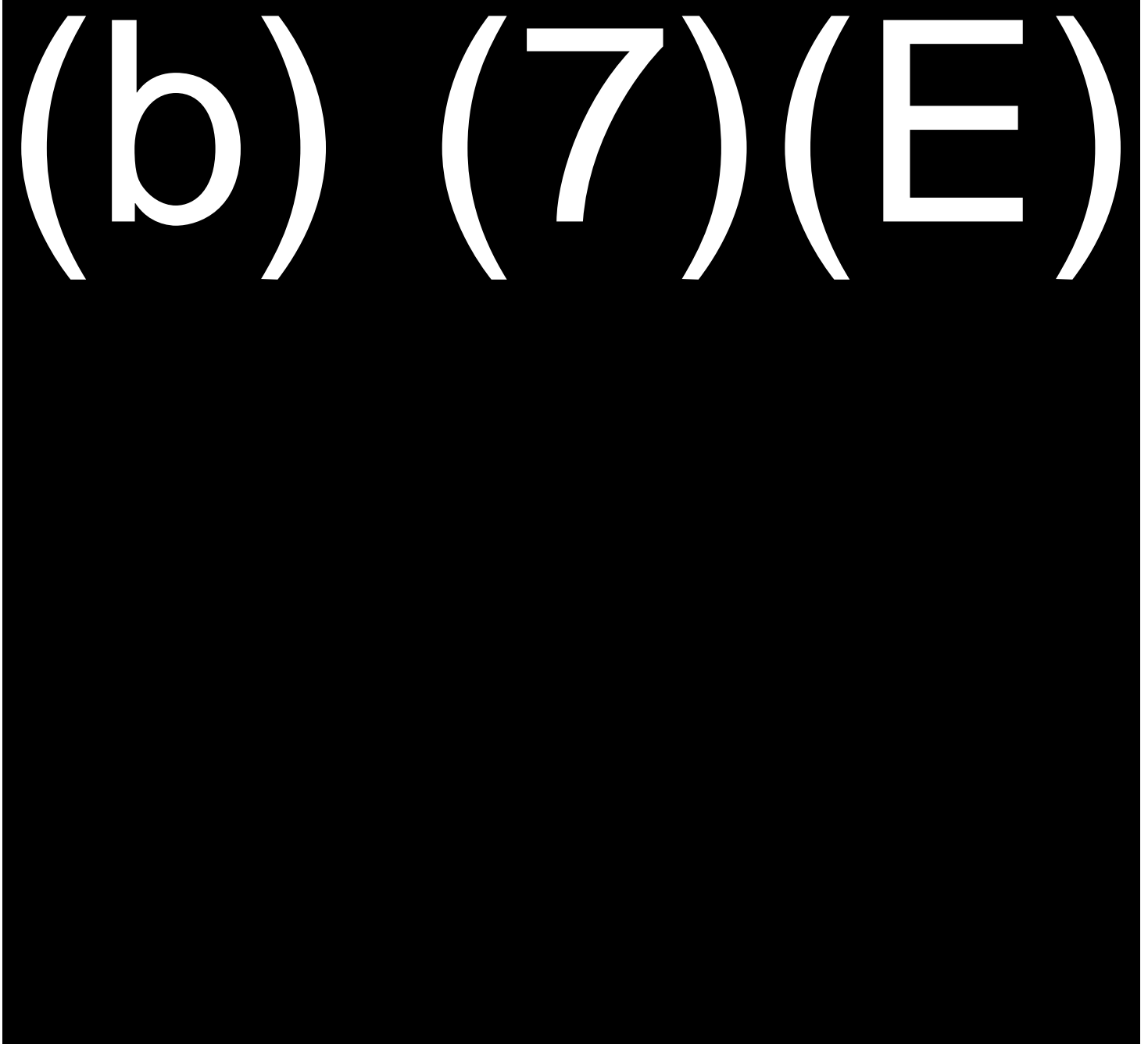
[10-10 — Statement Signature Page \(OI-16E\)](#)

SOCIAL SECURITY
Office of the Inspector General

PERSONAL HISTORY INFORMATION

Case Number: _____ Case Agent: _____

PERSONAL



SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)



Exhibit 10-2

Office of the Inspector General
Office of Investigations
Social Security Administration

REPORT OF INVESTIGATION

TITLE OF CASE:

CASE NUMBER:

PROGRAM CATEGORY:

PERIOD COVERED:

From: To:

RELATED CASE NUMBERS:

REPORT BY:

FIELD DIVISION / OFFICE:

FD: Office:

STATUS OF CASE:

() INVESTIGATION CONTINUED

- INITIAL REPORT
- STATUS REPORT
- JUDICIAL STATUS REPORT

() COLLATERAL INVESTIGATION

() INVESTIGATION CLOSED

SYNOPSIS

ALLEGATION or REFERENCE TO MOST RECENT REPORT

INVESTIGATIVE ACTIVITY

SUBJECT(S) AND/OR DEFENDANT(S)

JUDICIAL ACTION

DISPOSITION OF EVIDENCE, GRAND JURY MATERIAL, AND/OR PERSONAL PROPERTY

MONETARY ACHIEVEMENT

SUBMITTED BY: _____
Signature of Reporting Agent Date

APPROVED BY: _____
Signature of Approving Supervisor Date

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). This report is FOR OFFICIAL USE ONLY, including, but not limited to, its use in the claims adjudication process. It may not be copied or reproduced without written permission from the SSA OIG; however, for purposes of claims adjudication by SSA, including the DDS and the ODAR, it may be copied and incorporated into official claims files. Disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552 and 552a.

SOCIAL SECURITY
Office of the Inspector General

ADVICE OF RIGHTS

Before you are asked any questions, I want to advise you of the following rights:

- **YOU HAVE THE RIGHT TO REMAIN SILENT.**
- **ANYTHING YOU SAY CAN BE USED AGAINST YOU IN COURT.**
- **YOU HAVE THE RIGHT TO TALK TO A LAWYER FOR ADVICE BEFORE YOU ANSWER ANY QUESTIONS, AND TO HAVE A LAWYER WITH YOU DURING QUESTIONING, IF YOU WISH.**
- **IF YOU CANNOT AFFORD A LAWYER, ONE WILL BE APPOINTED FOR YOU BEFORE ANY QUESTIONING, IF YOU WISH.**

I have read the above Advice of Rights or it has been read to me, and I understand these rights.

(Date) (Time) (Signature)

WAIVER

I waive my right to remain silent and my right to have a lawyer present with me. No promises or threats have been made to me and no pressure or coercion of any kind has been used against me. I know and understand what I am doing.

(Date) (Time) (Signature)

(Investigator's Printed Name) (Witness' Printed Name)

(Investigator's Signature) (Witness' Signature)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

ADVICE OF RIGHTS

(Non-Custodial)

Before we ask you any questions you must understand your rights. You have the right to remain silent and make no statement at all. Any statement you do make may be used as evidence against you in criminal proceedings. You are not in custody. You are free to leave or terminate this interview at any time.

WAIVER OF RIGHTS

I have read this statement of rights, and I understand what my rights are. I have been advised as the general nature of the inquiry being made. No promises or threats have been made to me and no pressure or coercion of any kind has been used against me. I am willing to make a statement and answer questions voluntarily.

Signature (Name)

Name (Printed)

Special Agent

Witness

Date

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

ADVERTENCIA DE DERECHOS

Antes de hacerle cualquier pregunta, yo quiero avisarle de los siguientes derechos:

- **USTED TIENE EL DERECHO A PERMANECER EN SILENCIO.**
- **CUALQUIER COSA QUE USTED DIGA PUEDE SER UTILIZADO EN SU CONTRA EN LA CORTE.**
- **USTED TIENE EL DERECHO DE CONSULTAR CON UN ABOGADO ANTES DE QUE USTED CONTESTE CUALQUIER PREGUNTA, Y TENERLO PRESENTE DURANTE EL INTERROGATORIO, SI LO DESEA.**
- **SI USTED NO PUEDE PAGAR A UN ABOGADO, UNO SERA ASIGNADO ANTES DE USTED SER INTERROGADO, SI LO DESEA.**

Yo he leído el Aviso de Derechos arriba mencionado, o alguien me lo leyó, y yo entiendo estos derechos.

_____ (Fecha) _____ (Hora) _____ (Firma)

RENUNCIA

Yo renuncio mis derechos a mantenerme en silencio y mis derechos a tener a un abogado presente durante el interrogatorio. No se me hicieron promesas o amenazas y no se hizo presión o coerción de ninguna clase en mi contra. Yo se y comprendo lo que estoy haciendo.

_____ (Fecha) _____ (Hora) _____ (Firma)

_____ (Nombre del Investigador) _____ (Nombre del Testigo)

_____ (Firma del Investigador) _____ (Firma del Testigo)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

STATEMENT OF _____ PAGE 1 OF _____

“I, _____, hereby make the following free and voluntary sworn statement to _____, who has identified him/herself to me as a Special Agent with the Office of Inspector General, Social Security Administration.”

“ _____

_____”

State of: _____ Date: _____

County of: _____ Location: _____

<p>This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is <u>FOR OFFICIAL USE ONLY</u>, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.</p>

SOCIAL SECURITY
Office of the Inspector General

STATEMENT OF _____ PAGE 1 OF _____

“I, _____, hereby make the following free and voluntary sworn statement to _____, who has identified him/herself to me as a Special Agent with the Office of Inspector General, Social Security Administration. I have been advised of certain rights in accordance with the Miranda Decision (as outlined on form OI-13 NC), which I have waived, prior to making this statement.”

“

_____”

State of: _____ Date: _____

County of: _____ Location: _____

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

STATEMENT OF _____ PAGE _____ OF _____

I have read this statement, consisting of this and _____ other page(s); and it is true, accurate, and complete to the best of my knowledge and belief. I have initialed each page, where necessary, and have been given an opportunity to make any corrections or additions. I have initialed each line where a correction has been made.

SIGNATURE OF PERSON MAKING STATEMENT

Subscribed and sworn to before me this the _____ day of _____, 20____, at _____

Special Agent
Office of Investigations
Office of the Inspector General
Social Security Administration

Witness(es): _____

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

INVESTIGATIVE REPORTS

011.000 General

The investigative report is the product of a well-planned and executed work effort. The report should be prepared carefully, thoroughly, and in a timely manner, as it is a direct reflection on the competency and credibility of the special agent (SA) and the Office of the Inspector General (OIG). This chapter prescribes standards and procedures for the preparation and distribution of investigative reports.

011.010 Quality Standards

- A.** A report should address, in simple and understandable language, all relevant aspects of an investigation.
- B.** *The Council of Inspectors General on Integrity and Efficiency (CIGIE)* qualitative standards for report writing include:
 - 1. Completeness** – The report must address all aspects of an investigation to include any allegations that were not substantiated.
 - 2. Accuracy** – The report must correctly and succinctly relate the facts uncovered during the investigation to include any mitigating or exculpatory factors.
 - 3. Objectivity** – The report must be free of any personal biases or outside influences.
- C.** The report must be understandable and logically organized, and must clearly identify the issues and evidence.

011.020 Policy

- A.** All reports require supervisory approval.
- B.** When applicable, grand jury privileges must be obtained for approving authorities and their designees **prior** to submission of any related reports for supervisory approval. Grand jury privileges must also be obtained for any additional SAs and/or support staff reasonably expected to come into contact with the reports.

- C. Information identifying or tending to identify Confidential Informants (CI) or Confidential Sources (CS) will not be included within the reports. The designations issued to the individual CIs and CSs, as detailed in Chapter 9, will be used to conceal their identities in investigative case reports, files and memoranda.

011.030 Investigative Reports

- A. The following instructions apply to all investigative reports:

1. Write in the form of the first person, referring to yourself as I (Note: Form OI-4 CDI may be written in the third person, see CDI Operations Guide Chapter 6-60 Report of Investigation (Form OI-4) and CDI Summary ROI (Form OI-4 CDI) for guidance on CDI reports.)
2. When describing events that have already occurred, write in the past tense.
3. Use active voice, rather than passive voice, to clearly and concisely describe who is doing an action.
4. Acronyms and abbreviations may be used after they have been fully spelled out in the report's text, i.e., Internal Revenue Service (IRS). **Exceptions:** SSA and SSA/OIG may be used at any time.
5. The first page of all investigative reports will be printed on letterhead (SSA/OIG) stationary. Subsequent pages will be printed on plain paper.
6. All investigative reports must display the "FOR OFFICIAL USE ONLY" footer.

- B. The following eight reports and forms were designed specifically for the documentation of investigative activity:

1. **Investigative Plan** ([Form OI-2](#), [Exhibit 11-1](#)): The investigative plan serves as an outline of the investigation and guide for the Case Agent to follow as the investigation progresses. Investigative Plans are flexible and subject to change as an investigation progresses.
2. **Report of Investigation (ROI)** ([Form OI-4](#), [Exhibit 11-2](#)): ROIs will be prepared in every OIG investigation opened, throughout the course of the investigation as necessary, and at the conclusion of each case for relevant information bearing on the allegation(s) and the culpability of the subject(s). It is essential that all ROIs be presented in a clear, logical, and concise manner.

The type of investigation will determine which OI form to use in preparing the ROI. If the investigation concerns a CDI Program investigation, the case agent must use form [OI-4](#) and [OI-4 CDI](#) (Summary Report of Investigation) (see [Exhibit 11-2A](#)). For all other types of investigations, the case agent should use form OI-4.

- a. The ROI is to be completed in the following situations:

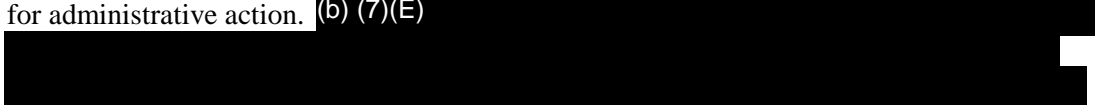
1. To document the substance of interviews conducted as part of the investigation.

2. To document the results of analysis conducted of paper and electronic documents, records and other related items.
 3. To report arrests or search warrant executions, within 10 calendar days of the event.
 4. To request assistance from other field divisions (collateral investigations).
 5. At the request of a prosecuting attorney.
 6. At the request of a Regional Commissioner for use in an administrative action.
 7. When providing information to another law enforcement agency.
 8. As a cover document for all special project/program reports.
 9. In unique circumstances at the discretion of the Special Agent-in-Charge (SAC).
 10. To report the conclusion of an investigation.
- b. The ROI will contain the following information:
1. Case number.
 2. Case name.
 3. Reporting time frame - The reporting time frame referenced in each individual OI-4 should reflect the date(s) of the investigative activity covered in that specific OI-4.
 4. A listing of all SSA/OIG special agents (SA) or agents from other law enforcement agencies involved in the investigation.
 5. Specific information where arrested subjects or suspects photographs and fingerprints may be found if they are not contained in the case file. (This information should contain the name of the law enforcement agency, address, telephone number, case number, and case agent or contact name.) If fingerprints and photographs are located in the case file, the fingerprint card will be filled out with all available information. Suspect photographs will have on the reverse, the name of the subject, DOB, FBI or state case number, and the OIG case number.
 6. Name of the SA who advised the subject(s) of Miranda, Garrity, or Kalkines warnings, and who, if anyone, witnessed this event.
 7. A summary of all interviews conducted during the course of the investigation, regardless if a formal statement is taken. A detailed reporting of the interview is required when a formal statement is not obtained.
 8. Monetary accomplishments must be documented in the OI-4. Monetary accomplishments are identified as *Savings, Non SSA Savings, Fraud Loss,*

Restitution, and Recoveries. The OI-4 must detail how the case agent determined the amount of monetary accomplishment claimed. The case file will contain a copy of the MBR for Title II and SSR for Title XVI to support the monetary accomplishments.

9. Reports are electronically signed and dated in NICMS when submitted by the agent and by the supervisor (ASAC, RAC, or SAC) approving the report. The date the agent submits the report is considered the official date of the report.
 10. A review of NICMS will be made on every subject of an OIG investigation and the results of this review will be annotated in the OI-4.
 11. OI-4s will be filed in order of date, with the first on the bottom and each subsequent OI-4 on top.
- c. Collateral ROIs will be prepared to request investigative assistance from another FD or field office. A collateral report should provide the following information:
1. A brief summary of the allegation.
 2. The issue(s) upon which the collateral request is based.
 3. The specific collateral investigation required.
 4. Available background information on individuals relevant to the request.
 5. Time sensitivities or restrictions, if any.
- d. ROIs may be used to refer criminal matters to the appropriate prosecuting authority. The preference of the prosecuting authority as to form and format is to be adhered to, to the maximum extent practical when preparing the referral documents. Use of the ROI in lieu of a Prosecution Report will be at the discretion of the SAC if the prosecuting authority does not have a preference.
- e. ROIs involving potential administrative action by SSA against an SSA employee **must** be forwarded through the SAC, using a Memorandum of Transmission, to the appropriate SSA Regional Commissioner.
3. **Specialized Report of Investigation** ([Form OI-5A](#), [Exhibit 11-5](#)): Specialized Report of Investigation forms will be developed as required to meet the unique needs of National Operations or Local Projects. Form OI-5A, for example, has been developed to record investigative information and results for the Fugitive Felon Projects. The development of a Specialized Report of Investigation requires the review and approval of the Office of Counsel to the Inspector General (OCIG) and OI HQ management.
4. **Prosecution Report** ([Form OI-6](#), [Exhibit 11-3](#)): The Prosecution Report has been designed to be the comprehensive document used to present the results of an investigation to the proper authorities for any civil/criminal/administrative remedies deemed appropriate. If the attorney charged with prosecuting the case prefers to receive the Reports of Investigation

(ROI) in lieu of a formal Prosecution Report, the ROIs should be forwarded to the attorney attached to [Form OI-6A](#) ([Exhibit 11-3A](#)).

5. **Special Investigations Report** ([Form OI-6S](#)): The Special Investigations Report has been designed to be the comprehensive document used to present the results of a special investigation to the proper authorities (Office of Special Counsel, Whistleblower, EEO, Retaliation, etc.).
6. **Memorandum of Transmission** ([Form OI-7](#), [Exhibit 11-4](#)): This report is used by the SAC as a cover document when providing official information to SSA management or outside law enforcement agencies.
7. **NICMS Criminal & Administrative Disposition Form** ([Form OI-9](#), [Exhibit 11-6](#)): This form is used to record information concerning investigative and judicial actions. It is a mandatory form, and appropriate case information/actions such as indictments, arrests, and computation of fraud losses/fraud savings should be entered into NICMS as soon as is practical after they occur, as opposed to entering all of the information at the conclusion of the investigation.
8. **OI-19 Personal History Form** ([Form OI-19](#)): The OI-19 will be completed in every case where an SA makes an arrest, has a key suspect, or if it is an employee case being referred for administrative action. (b) (7)(E)


The OI-19 is an intelligence document that provides important leads for future investigations. It may also be used to assist other law enforcement agencies or the DOJ if they contact OI for information from our records.
9. **Investigative Checklist** ([Form OI-34](#), [Exhibit 11-7](#)): This form is used to track requests made, information received, and interviews conducted during the course of an investigation. Use of this form is optional.
10. **Analysis Report** ([Form OI-8](#), [Exhibit 11-8](#)): This report was designed to provide findings on significant analytical work performed in furtherance of an active investigation or in support of proactive case development. OI-8s completed at the request of a field division by an Investigative Assistant (IA) assigned to that field division will be approved by the SAC/ASAC. OI-8s completed for or at the request of IAD, regardless of the IA's assigned location, will be approved by the IAD director.

C. Legal/User Requirements

1. Grand Jury information must be sealed in an envelope with the outside of the envelope marked, "GRAND JURY INFORMATION." In addition, the outside of the case file should be marked, "THIS FILE CONTAINS GRAND JURY INFORMATION."
2. All investigative notes will be placed in an envelope and maintained in the OIG Case Investigative File and marked, "CASE AGENT INVESTIGATIVE NOTES." Case agent investigative notes are the product of investigative activity, usually interviews of suspects,

witnesses, and defendants (regardless if a formal statement is taken).

3. NCIC QR – Computerized Criminal History queries, when no longer needed at the closing of the case, must be destroyed (i.e., shredded or burned) to prevent unauthorized viewing. Source: DOJ Enforcement Program Services, Justice Telecommunications System Student Workbook – for users of the NCIC. State and local criminal history records obtained from state or local database systems, when no longer needed at the closing of the case, must also be destroyed (i.e. shredded or burned) to prevent unauthorized viewing.

011.035 Submission of Reports/Documents

A. **OI-4 - Report of Investigation** – At a minimum (*or more frequently as directed by the supervisor*), submission of reports should follow the below timetable:

1. 45 days from the case opening date for the initial report;
2. 120 days for all subsequent reports, until the investigation has been completed and an OI-6 (Prosecution Report) or OI-6A (Prosecution Report- ROI Cover Letter) has been submitted to a Federal, State or local prosecutor. (*Note: the documentation of contact with an Assistant U.S. Attorney/prosecutor, or status of pending judicial proceedings, will be articulated on Form OI-20, Supervisory File Review Sheet, as part of the case file review process, described in SAH Section 003.100.*)
3. A Report of Investigation is required regardless of the above, under the following circumstances:
 - a. A Report of Investigation shall be prepared within 10 calendar days of the following events: arrests, search warrant executions, and interviews (refer to SAH Sections 011.030 and 010.040, respectively.)
 - b. A Report of Investigation shall be prepared within 10 calendar days for any investigative activity (e.g. interview, surveillance, collection of evidence, review of records, arrest, search warrant execution, etc.) that occurs following the submission of an OI-6 or OI-6A.
 - c. A Report of Investigation shall be prepared to report the closing of an investigation.

B. **OI-19 - Personal History Form**

1. Form OI-19 must be completed via NICMS for each subject/defendant identified in a case.
2. Since basic subject information is the only data automatically uploaded to the electronic Form OI-19 in NICMS; agents shall ensure that as additional subject/defendant information is obtained, Form OI-19 is updated via NICMS, continuously. (Note: Effective 10/01/09, Form OI-19 became electronic and is no longer required to be placed in the investigative file.)

C. **OI-31 - Table of Contents**

The OI-31 is due by the first case review; however, it should be used throughout the investigation by the case agent.

Note: File assembly is the responsibility of the of the case agent assigned to the investigation)

D. Photographs/Fingerprints

Photographs/Fingerprints of suspects/defendants are due when they become available or before the case is closed.

Note – If these items are not available, it must documented that they exist in the OI-4.

E. Charging Document

This document is due within 10 days or **as soon as is practical** following the arrest, indictment, or plea.

011.040 SSA Office of the Inspector General Fact Sheets

A. Fact Sheets are essentially reports that provide information to OI and to SSA in follow-up to investigative or judicial action that may generate media requests or requests for information from SSA officials to the Inspector General.

B. Headquarters (HQ) needs to be apprised in a timely and uniform manner about significant events, special interest cases, and cases of interest to the media. Fact Sheets are the means by which OI FDs convey this information to HQ and to the Public Affairs Officer (PAO). Fact Sheets are required to be submitted to HQ to report arrests, sentencings, and any events that trigger media coverage.

C. General rules for Fact Sheets

1. A Fact Sheet should be submitted **immediately** for any event(s) triggering media coverage.
2. Fact Sheets are required to be submitted to HQ **within five business days** of an arrest. If the arrest triggers media coverage, # 1 above applies.
3. Fact Sheets are required to be submitted to HQ **within 10 business days** of a sentencing.
4. Fact Sheets are not required when a subject appears in court in response to a summons or surrenders pursuant to an arrest warrant. Information regarding the summons or surrender should be included in the Fact Sheet submitted to report the subject's sentencing.
3. Do not use Fact Sheets to report the initiation of employee cases.

4. The approved Fact Sheet becomes part of the official electronic case file.
6. Fact Sheets containing information that should not be released to parties outside of SSA OIG are to be clearly marked as Internal Use Only. NICMS contains a drop down menu which provides this option.
7. Fact Sheets are created in NICMS. Examples of completed Fact Sheets are found in the Report Writing Guide in SharePoint.
8. Instructions on how to complete and generate a Fact Sheet are found in section 2.8 of the NICMS Manual.
9. Fact Sheets should not be prepared by cutting and pasting information from other documents. NICMS does not recognize special characters from Microsoft Office programs. NICMS does allow the agent to add text from a prior Fact Sheet onto a subsequent Fact Sheet by selecting the “Previous Fact Sheet Comments” button on the Fact Sheet template screen. This function should always be used when preparing a Fact Sheet to report events subsequent to a previously reported event.
10. Fact Sheets should be written in the third person.
11. Type the subject’s last name in capital letters, e.g. SMITH, not Smith.
12. Numbers under 10 are spelled out, e.g., one, two, three, etc. Numbers of 10 or more are not spelled out, e.g. 11, 12, 13, etc. However, when 2 or more numbers appear in a sentence and 1 of them is 10 or larger, figures are used for each number.
13. The Fact Sheet shall begin with a description of the event reported, e.g., “On January 8, 2010, John SMITH was sentenced
14. The charges should be listed in the first paragraph of the narrative. When citing a charge, the applicable U. S. Code or state statute should be listed prior to the named offense. For example, “SMITH was charged with violation of Title 18, U.S.C, Section 641 - Theft of Government Funds.”
15. The second paragraph in the initial Fact Sheet should begin with how the referral was received and the case was initiated. Do not use the name of the person who referred the allegation. List the SSA (or OIG) component, district office, or agency that referred the case, e.g., “This case was initiated based on information provided by the Annapolis, MD Social Security Administration office.” Follow the instructions listed in item # 9 when submitting a subsequent Fact Sheet to report a sentencing. Subsequent Fact Sheets always build on prior Fact Sheets.
16. If applicable, include the monetary loss to SSA.
17. The final paragraph should provide the title and name of the prosecutor, e.g., “This case was prosecuted by Assistant U.S. Attorney”

18. The phone number and/or other contact information for the prosecutor should not be included.
19. Do not list the name of the judge who presided over the sentencing of the defendant.
20. OI field division supervisors may distribute approved Fact Sheets to SSA managers.

011.050 Reports of Employee Misconduct to Headquarters

- A.** Cases involving substantive allegations of criminal conduct or of egregious non-criminal misconduct by SSA employees continue to be of special interest to the OIG. It is essential to OIG HQ effectiveness that it be aware of all such cases at an early stage.
- B.** If an OIG employee is implicated, the SAC or his/her designee shall notify the Office of Quality Assurance and Professional Responsibility (OQAPR) and the Deputy Assistant Inspector General for Investigations (DAIGI) immediately by telephone upon receipt of such an allegation. The notification will be confirmed in writing immediately thereafter. If the allegation against an agent is found to be credible and relates significant abuse of authorities conferred by section 6(e)(1) of the Inspector General Act (carrying a firearm, making arrests without warrants, seeking or executing arrest or search warrants), the written notification should be sent to the DAIGI through the SAC of CID. CID will maintain a copy of this written notification on file for use in the annual reporting to the Attorney General.
 1. The SAC shall assess the report (completed on an OI investigative report) and advise the DAIGI via memorandum within 10 days of what action, if any, the SAC proposes to take.
 2. If the DAIGI concurs with the proposal, the DAIGIs will notify the SAC via memorandum ([Exhibit 11-9](#)). If the DAIGI determines further discussion is required before any action is to be taken, the DAIGI will contact the SAC and advise of same.
- C.** In cases involving non-OIG employees at the GS-15 level or above (including Senior Executive Service [SES]) who are implicated in criminal conduct, the SAC or his/her designee shall notify CID within 24 hours, and confirm the transmittal in writing within three working days. The FD will conduct the investigation.
- D.** In other cases involving SSA employees, the SAC or his/her designee shall notify HQ within three working days of complaint receipt. The initial notification shall be by electronic mail and should contain the following information:
 1. The employee's name, position title, grade, and organizational component.
 2. The date the complaint was received or the incident was otherwise discovered.
 3. The OI file number.
 4. A brief description of the suspected violation.
 5. The action the OI FD has taken or plans to take (include dates).

6. Information as to other significant factors such as:
 - a. media interest
 - b. relation to other investigations
 - c. monetary impact
7. An indication whether the FD has any objections to OIG HQ notifying the employee's senior management of the existence of the complaint.

011.060 Annual Report to the Attorney General

A. The Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement requires the annual reporting of certain information related to investigative activities. This information includes:

1. the number of federal investigations initiated;
2. the number of undercover operations initiated;
3. the number of times electronic surveillance was used; and
4. the number of significant and credible allegations of abuse of authorities conferred by section 6(e)(1) of the Inspector General Act.

OI's Criminal Investigations Division is responsible for reporting this information at the conclusion of each fiscal year, and no later than October 31st, to:

Office of the Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

B. This report replaces the **Law Enforcement Methods Used (LEMUSE)** report required when OI agents received certain law enforcement authority under a deputation arrangement with the Department of Justice. Although not required by law, OI will continue collecting certain LEMUSE information for internal management information reports.

011.070 Management Implication Reports

- A.** Section 4 of the Inspector General Act of 1978 (IG Act) provides that the IG shall:
1. Recommend policies for promoting economy and efficiency in the administration of preventing and detecting fraud and abuse in programs and operations.
 2. Keep the Commissioner fully and currently informed concerning fraud and other serious problems, abuses, and deficiencies relating to the administration of programs and operations administered or financed by SSA.

3. Recommend corrective action concerning such problems, abuses, and deficiencies.

Furthermore, the Inspector General Reform Act of 2008 provides that members of the Council of the Inspectors General on Integrity and Efficiency (CIGIE) shall adhere to professional standards developed by the Council. CIGIE's Quality Standard for Investigation on reporting states, "Systemic weaknesses or management problems disclosed in an investigation should be reported to agency officials as soon as practicable."

To ensure SSA OIG adherence to these provisions, when the Office of Investigations (OI) uncovers a potential systemic or programmatic issue, OI may issue a Management Implication Report (MIR) to ensure SSA is aware of the issue.

- B. OI identifies potential Management Implication Report (MIR) topics in one of two ways. First, an employee of the Intelligence and Analysis Division (IAD) may identify a potential MIR topic through the course of their work. Secondly, a Special Agent (SA) or supervisor (SAC/ASAC/RAC) may identify a potential MIR topic/issue during, or as a result of, an investigation. Any potential issue will be referred to the Director/Special Agent-in-Charge (SAC) and the Assistant to the Special Agent-in-Charge (ATSAC) of IAD, where it will be assigned to an investigations analyst for development.
- C. IAD will meet with representatives of the Office of Audit (OA) to discuss the issue and avoid duplication of any current or prior OIG audit work.
- D. IAD will prepare a request memorandum through the Deputy Assistant Inspector General for Investigations (DAIGI) to the Assistant Inspector General for Investigations (AIGI). Upon approval by the DAIGI and AIGI, IAD will conduct the necessary research steps and prepare the MIR, using the following format:
 1. **Overview:** a brief introduction of the programmatic or systemic vulnerability/issue that the MIR will discuss;
 2. **Synopsis:** the background information on the vulnerability/issue;
 3. **Findings:** a definition of the vulnerability/issue. Specific examples are used to illustrate the vulnerability/issue;
 4. **Recommendations:** specific actions for SSA to eliminate or lessen the vulnerability/issue; and
 5. **Conclusion:** a summation of the vulnerability/issue and the importance of its resolution.

The MIR will contain a memo from the AIGI, through the Deputy Inspector General, to the Inspector General (IG), with a "cc" to the Assistant Inspector General for Audit (AIGA), outlining the purpose and contents of the MIR. (*See Exhibit XX for the MIR Template*).

- E. Upon approval, the AIGI will submit the MIR with the cover letter to the IG. Upon review, the IG may determine to issue the MIR to SSA.

F. IAD will maintain copies of all MIRs, to include posting copies on OI's SharePoint site.

Chapter 11 — **EXHIBITS**

[11-1 — Investigative Plan \(OI-2\)](#)

[11-2 — Report of Investigation \(OI-4\)](#)

[11-2A — Report of Investigation—Cooperative Disability Investigations Unit \(OI-4 CDI\)](#)

[11-3 — Prosecution Report \(OI-6\)](#)

[11-3A — Prosecution Report \(OI-6A\)](#)

[11-4 — Memorandum of Transmission \(OI-7\)](#)

[11-5 — Specialized Report of Investigation \(OI-5A\)](#)

[11-6 — NICMS Criminal & Administrative Disposition Form \(OI-9\)](#)

[11-7 — Investigative Checklist \(OI-34\)](#)

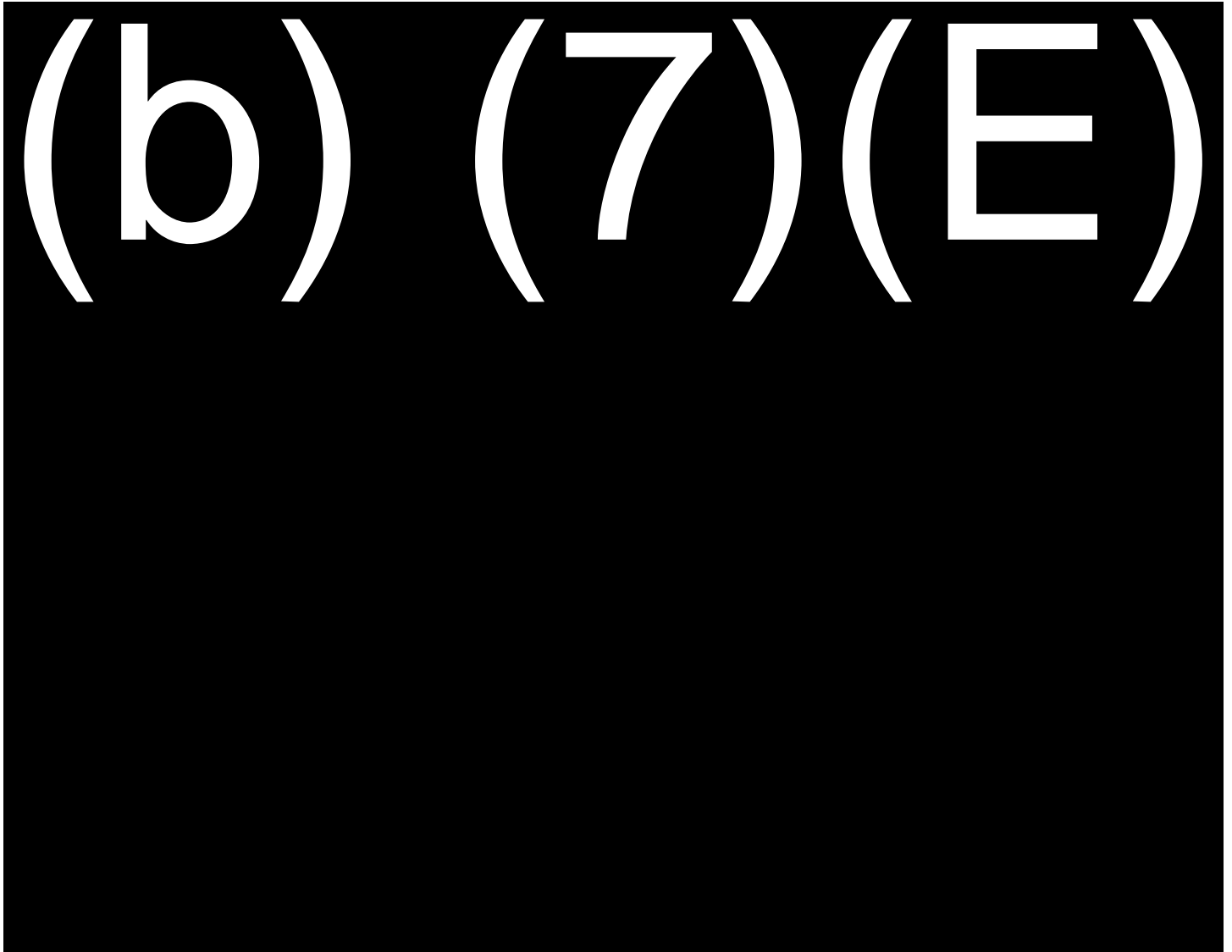
[11-8 — Case Analysis Report \(OI-8\)](#)

[11-9 — DAIGI Memorandum for Employee Misconduct Cases Involving OI SAs](#)



INVESTIGATIVE PLAN

Investigator:	Case No.:	Date Opened:
Subject:	Judicial District:	



This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

Exhibit 11-2

Office of the Inspector General
Office of Investigations
Social Security Administration

REPORT OF INVESTIGATION

TITLE OF CASE:

CASE NUMBER:

PROGRAM CATEGORY:

PERIOD COVERED:

From: To:

RELATED CASE NUMBERS:

REPORT BY:

FIELD DIVISION / OFFICE:

FD: Office:

STATUS OF CASE:

() INVESTIGATION CONTINUED

- INITIAL REPORT
- STATUS REPORT
- JUDICIAL STATUS REPORT

() COLLATERAL INVESTIGATION

() INVESTIGATION CLOSED

SYNOPSIS

ALLEGATION or REFERENCE TO MOST RECENT REPORT

INVESTIGATIVE ACTIVITY

SUBJECT(S) AND/OR DEFENDANT(S)

JUDICIAL ACTION

DISPOSITION OF EVIDENCE, GRAND JURY MATERIAL, AND/OR PERSONAL PROPERTY

MONETARY ACHIEVEMENT

SUBMITTED: _____
Signature of Reporting Agent

Date

APPROVED: _____
Signature of Approving Supervisor

Date

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). This report is FOR OFFICIAL USE ONLY, including, but not limited to, its use in the claims adjudication process. It may not be copied or reproduced without written permission from the SSA OIG; however, for purposes of claims adjudication by SSA, including the DDS and the ODAR, it may be copied and incorporated into official claims files. Disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552 and 552a.



COOPERATIVE DISABILITY INVESTIGATIONS UNIT
[CITY, STATE]

SUMMARY REPORT OF INVESTIGATION TRANSMITTAL
AND RECEIPT FORM

PLEASE DETACH THIS FORM FROM THE REPORT, COMPLETE THE BOTTOM SECTION, AND RETURN THE FORM TO THE CDI UNIT IN: [CITY, STATE]

Transmittal Date: _____ **CDI Reference Number:** _____

Destination: _____ **SSA Office:** _____ **DDS Branch:** _____

Referral Received: _____

Referral Source: Name.....
 Address.....
 Telephone.....

Allegation(s): _____

SUBJECT: Name.....
 SSN.....
 Address.....
 Telephone.....

CHECK ONE: Claimant Representative Interpreter Doctor Lawyer Other

TO BE COMPLETED BY SSA, DDS, OR ODAR EMPLOYEE: CHECK ONE

SSA DDS ODAR

___ The CDI Summary ROI was considered during the disability determination. Reg Basis/Reason Code: ___

___ The CDI Summary ROI was not considered during the disability determination. Reg Basis/Reason Code: ___

___ The disability claim was adjudicated prior to receipt of the CDI Summary ROI. Reg Basis/Reason Code: ___

___ The disability claim (initial) was allowed or disability benefits were continued. Reg Basis/Reason Code: ___

___ Other/Comments:

STAFF SIGNATURE	PRINTED NAME	TITLE	DATE



SUMMARY REPORT OF INVESTIGATION

COOPERATIVE DISABILITY INVESTIGATIONS UNIT
[CITY, STATE]

Subject:
SSN:
DOB:
CDI Reference Number:
Date of Report:

OIG Point of Contact:	Name, Title
	Telephone Number
DDS Point of Contact:	Name, Title
	Telephone Number

COOPERATIVE DISABILITY INVESTIGATIONS UNIT – [CITY, STATE]
REPORT OF INVESTIGATION

I. SUBJECT DATA

CDI Reference Number:
Name:
SSN:
DOB:
Related Reference Number(s):

II. SYNOPSIS

Highlight any inconsistencies in the claimant’s record and synopsise investigative results that directly influence the adjudication process.

III. NATURE OF REFERRAL

Identify date and source of referral.

Summarize the complaint.

IV. TYPE OF CLAIM

Specify Title II, Title XVI, or concurrent pay.

Indicate whether initial claim or in-pay.

V. ALLEGED DISABILITY / FUNCTIONAL LIMITATIONS

List the claimant’s alleged impairments.

Summarize the subject’s responses to the daily activities questionnaire, and any third-party information.

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). This report is FOR OFFICIAL USE ONLY, including, but not limited to, its use in the claims adjudication process. It may not be copied or reproduced without written permission from the SSA OIG; however, for purposes of claims adjudication by SSA, including the DDS and the ODAR, it may be copied and incorporated into official claims files. Disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552 and 552a.

COOPERATIVE DISABILITY INVESTIGATIONS UNIT – [CITY, STATE]
REPORT OF INVESTIGATION

VI. DETAILS OF INVESTIGATION

Provide appropriate background data obtained from SSA/DDS computer systems, state DMV records, NICB, and other automated resources.

Provide a detailed account of all investigative activities conducted in the field.

VII. LIST OF EXHIBITS

Include as attachments to the report all appropriate witness statements, automated printouts, photographs, etc. and list them by description and exhibit number in this section. Local preferences, as agreed to by OIG, SSA, DDS, and ODAR officials, may dictate how much supporting documentation to provide.

VII. SIGNATURES

Submitted By:

Special Agent / CDI Unit Team Leader

Date

Approved By:

Assistant Special Agent in Charge or
Resident Agent in Charge

Date

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). This report is FOR OFFICIAL USE ONLY, including, but not limited to, its use in the claims adjudication process. It may not be copied or reproduced without written permission from the SSA OIG; however, for purposes of claims adjudication by SSA, including the DDS and the ODAR, it may be copied and incorporated into official claims files. Disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552 and 552a.



[Click **here** and type return address]

17 May 2017

[Click **here** and type recipient's address]

ATTN: AUSA [Name]

Re: [Subject's Name]
[City, State]
OI Case No. BAL-09-00001-H

Dear [Click **here** and type recipient's name]:

Following are the particulars relative to and her/his scheme to defraud the Supplemental Security Income (SSI) program, administered by the Social Security Administration(SSA), by misrepresenting.....

NAME OF OFFENDER:	[Name]
DATE OF BIRTH:	[DOB]
ADDRESS:	[Street Address, City, State Zip]
SOCIAL SECURITY NUMBER:	[SSN]
PLACE OF OFFENSE:	[City, State]
DATES OF OFFENSE:	[Month, Day, Year TO Month, Day, Year]
NATURE OF OFFENSE:	[Theft of Government Property; False Statements;]

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

INTRODUCTION

This case was opened based on information received on

PROGRAM BACKGROUND

Supplemental Security Income is the first federally administered

DETAILS OF OFFENSE

In January 2009,

PERSONAL & CRIMINAL HISTORY

Thomas Fraud was born on

WITNESSES AND THEIR TESTIMONY

EXHIBITS

Exhibit 1- Photocopy of Form SSA 8000-BK, Application for

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

In the event you desire any additional information relative to this investigation, please contact me at [telephone number here].

Sincerely,

[Click **here** and type your name]

[Click **here** and type job title]

Approved by:

Name:

Title:

Date:

Enclosure: List Exhibits

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Name of Subject:
SSA/OIG/OI File:
Xref:

Date

Prosecutor Name
Office
Address

Dear Title (AUSA/DAG/etc.)_____:

This is to confirm the case presentation for prosecution by Special Agent _____, Office of the Inspector General, Office of Investigations, Social Security Administration on _____ to you, relative to above name subject(s).

The following is a brief investigative synopsis of the potential offense(s):

The Reports of Investigation (ROI) regarding this matter are attached. All evidence in this case is retained in the SSA, OIG, _____ office. Please contact Special Agent _____ at () _____ if you require further assistance.

Sincerely,

(Name)
SAC/ASAC/RAC

Enclosures

ROI dated _____
ROI dated _____
ROI dated _____



MEMORANDUM

DATE: DATE

REFER TO: OI CASE NUMBER

TO: RECIPIENT'S NAME AND ADDRESS

FROM: SENDER'S NAME AND ADDRESS

SUBJECT: SUBJECT'S NAME

REPLY REQUESTED BY: _____

Attached is an Office of the Inspector General Report of Investigation concerning the above referenced subject.

This report is being furnished for whatever action you deem appropriate. If you decide to take action in this case and have a need for the exhibits, you must request those documents in writing. You may forward your response and any request to my attention at the Office of the Inspector General, at the above address.

If you require further information, you or your staff may contact me at [Click **here** and type your telephone #].

Attachment

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Report of Investigation – Fugitive Felon

Case Number: _____

Subject: _____

Field Division/Office _____

On _____ I was informed by _____

_____ (Law Enforcement Agency – Source) that the following individual:

Name: _____

Date of Birth: _____

Social Security Number: _____

Warrant Number: _____

is the subject of an official fugitive investigation and has been determined to be:

Fleeing to avoid prosecution for a crime which is a felony

Fleeing to avoid custody or confinement after conviction of a crime which is a felony

Violating a condition of probation or parole under Federal or State laws

On _____ it was determined, through access to the SAADARS system, that the fugitive identified above is currently receiving Supplemental Security Income (SSI) payments in violation of Public Law 104-193. On _____ the Law Enforcement Agency was provided an OIG Law Enforcement Referral/Certification Form that included the SSI payment address for the fugitive.

On _____ the Law Enforcement Agency reported that _____ was:

Positively identified as the fugitive felon and apprehended on _____

Positively identified as the fugitive felon, but efforts to locate were unsuccessful.

Is not the fugitive felon. True identity and location of fugitive felon are unknown.

Positively identified as the fugitive felon. Law Enforcement Agency will not extradite.

Positively identified as the fugitive felon. Law Enforcement Agency will extradite.

Other: _____

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

On _____ I provided the OIG Investigative Summary/SSA Feedback Form to: _____
_____ (SSA component) for their use in appropriate administrative actions.

On _____ the SSA component returned the SSA Feedback Form reporting that:
___ SSI payments were suspended on _____
___ Monthly payment at the time of suspension was _____
___ No administrative action was taken by SSA
___ Possible fraud in the SSI application or continuing eligibility process was noted

This investigation resulted in the following judicial action for: _____
___ Arrested on _____ (warrant)
___ Blanket Letter of Declination dated _____
___ Other _____
___ None

Overpayment claimed for this investigation: \$ _____
Savings claimed for this investigation: \$ _____

REMARKS: _____

Investigation closed on _____.
Submitted by: _____ Date: _____
Approved by: _____ Date: _____

Attachments: ___ Investigative Summary Report/SSA Feedback Form
___ Law Enforcement Referral/Certification Form
___ Other: _____

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.



NICMS DISPOSITION FORM

Case Number:	Case Agent:
--------------	-------------

SUBJECT DATA

Subject #:	Subject Type:		
Last Name	First Name	Middle Name	
SSN	DOB	State	Zip Code
Business:			

JUDICIAL DATA

Federal Crim Prosecutor:		Phone number:		Jurisdiction:
Present:	Accept:	Decline:	Accept/Decline:	Reason:
Federal Civil Prosecutor:		Phone number:		Jurisdiction:
Present:	Accept:	Decline:	Accept/Decline:	Reason:
Local/State Prosecutor:		Phone number:		Jurisdiction:
Present:	Accept:	Decline:	Accept/Decline:	Reason:

CRIMINAL DISPOSITION DATE

Code	Plea	NoloC	Conv	PTD	Acquit	Dismiss	Total	Mistrial

<input type="checkbox"/> Arrest Date:	<input type="checkbox"/> Information Filed Date:	<input type="checkbox"/> Criminal Complaint Date:	<input type="checkbox"/> Indictment Date:
---------------------------------------	--	---	---

ADMINISTRATIVE CASE ACTION

Action Taken	Date:

MONETARY ACHIEVEMENTS

Criminal	Civil	Administrative	SSA Money	Non SSA Money	Total
Fraud Loss					
Recovery					
Savings					
Restitution					
Fine/Penalty					
Judgment					

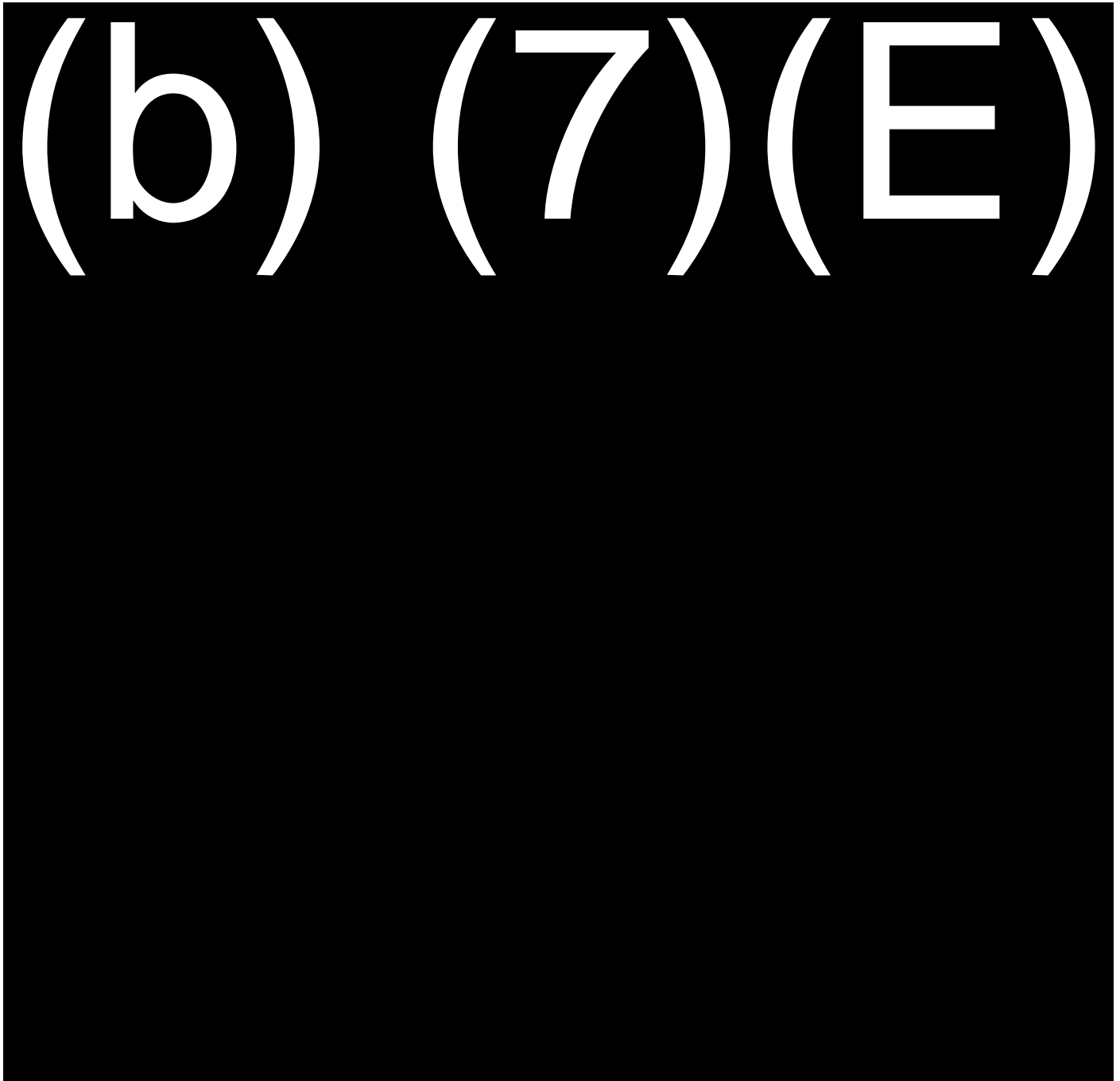
SUPERVISORY REVIEW

ASAC/RAC/SAC:	Date:	Additional OI-9's <input type="checkbox"/> Yes <input type="checkbox"/> No
---------------	-------	--

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552 and 552a.



INVESTIGATIVE CHECKLIST



This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

(b) (7) (E)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

(b) (7) (E)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.



**INSTRUCTIONS FOR COMPLETING FORM OI-12
(SSA OIG/OI FACT SHEET)**

Revised 7/2002

- Purpose:** Refer to *SAH 011.040* for complete explanation of when to submit Fact Sheet(s). Format to use to report significant events and activities by agents to the SAC, and subsequently to DAIGI. This will enable the SSA OIG/OI Headquarters to keep abreast of events occurring in the field divisions.
- This form is not to be used to replace any investigative form. It is to be used solely as an information tool from the FD to Headquarters.
- Case Agent:** The name of the assigned Case Agent, as it appears in the National Investigative Case Management System (NICMS).
- Reference #:** The SSA OIG/OI case number.
- SSA OIG Office:** The Field Division or Field Office that prepared the Fact Sheet.
- Date:** The date on which a specific event occurred, or the date for which a case update is being provided.
- OIG Contact:** Name & phone number of the SAC/ASAC/RAC who can provide additional information.
- Check whether facts of case can be released for public dissemination or should be kept "for internal use only."
- See *SAH 011.040* for explanation of when to release for Public Information or when to maintain information for internal use only.
- Issue/Event:** This portion should consist of the minimum number of paragraphs necessary to concisely describe the event(s) causing the issuance of the Fact Sheet. The paragraphs should be suitable for inclusion in a press release or the IG's weekly report. For a detailed checklist of information to be included in this portion, refer to *SAH 011.040*.
- Other Agencies Involved:** Name and telephone numbers of other Case Agents, and the respective agencies.



MEMORANDUM

Date:

Refer to:

To: (SAC's Name and FD)
Special Agent-in-Charge

From: Deputy Assistant Inspector General for Investigations

Subject: Employee Misconduct Case

I have reviewed your response dated (----Date----), addressing employee misconduct regarding (Special Agent's Name).

I concur with your recommendation. Please advise me when the action will be completed.

DAIGI's Name

INSPECTOR GENERAL SUBPOENAS

012.000 Authority

- A.** Section 6(a)(4) of the Inspector General Act of 1978, 5 U.S.C. App. 3, as amended, (Act) provides the Inspector General (IG) of the Social Security Administration (SSA) with broad authority to subpoena documents necessary to the performance of the IG’s responsibilities. This subpoena is referred to as the “IG subpoena.” The authority within the SSA to issue an IG subpoena has been delegated to the Deputy Inspector General, the Assistant Inspector General for Investigations, and the Deputy Assistant Inspector General for Investigations. The IG is authorized:

“ . . . to require by subpoena the production of all information, documents, reports, answers, records, accounts, papers, and other data in any medium (electronically stored information, as well as any tangible thing) and documentary evidence necessary in the performance of the functions assigned by this Act, which subpoena, in the case of contumacy or refusal to obey, shall be enforceable by order of any appropriate United States District Court: . . .”

- B.** Authority to issue IG subpoenas to obtain records pertinent to programs and operations of SSA applies both to the Office of the Inspector General (OIG) audit and investigative responsibilities. However, for the issuance of any IG subpoena, the following criteria must be met:
- 1.** The audit or investigation being conducted must be within the lawful jurisdiction of the SSA OIG;
 - 2.** There is reason to believe that the records sought are relevant to the audit or investigation; and
 - 3.** The demands of the subpoena must not be so broad or indefinite so as to make compliance unduly burdensome.
- C.** The policy of the SSA OIG Office of Investigations (OI) is that, generally, an IG subpoena will not be issued unless other means to obtain the required information have been exhausted or appear impractical. This would include obtaining the records under statute, regulation, or access clause of a contract or other agreement. Additionally, there are restrictions on the use of an IG subpoena:
- 1.** Subpoena power may not be used to collect records on behalf of another Federal or State agency nor may the IG subpoena any records from another Federal agency.

2. If used to compel the production of records located outside the United States, an administrative subpoena is unenforceable in a United States District Court.
3. A reasonable time must be allowed for the production of records, usually 10 working days. If the subpoena is issued pursuant to the Right to Financial Privacy Act, 12 U.S.C. § 3401, et seq., the time allowed for the production of records is either 10 or 14 days, depending on the type of service. See [Section D.3b](#) below.
4. An order of compliance from the appropriate United States District Court must be obtained if a subpoenaed party refuses to comply with the IG subpoena.
5. An IG subpoena may be used in criminal, civil, or administrative investigations. However, once an investigation has become the subject of proceedings by a Federal grand jury, the Special Agent (SA) should consult with the prosecutor(s) assigned to the case prior to requesting IG subpoenas. The SA should also advise the prosecutor(s) of any outstanding OIG subpoenas.

D. If the records being subpoenaed are from a financial institution and belong to a customer of the institution, the subpoena is potentially subject to the Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422, as described below. (See also Chapter 18 for a detailed discussion of the Right to Financial Privacy Act.)

1. General Rule.

“No Government authority may have access to or obtain copies of, or the information contained in, the financial records of any customer from a financial institution.” 12 U.S.C. § 3402.

2. Definitions.

“**Financial Institution**” is defined as “any office of a bank, savings bank, card issuer as defined in Section 1602(n) of Title 15, industrial loan company, trust company, savings association, building and loan, or homestead association (including cooperative banks), credit union, or consumer finance institution, located in any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands.”

“**Customer**” is defined in part as a “person or a person’s authorized representative.”

“**Person**” is defined as “an individual or a partnership of five or fewer individuals.”

“**Financial Record**” means “an original of, a copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer’s relationship with the financial institution.” Examples of financial records would include checking and savings accounts, loan documents, Individual Retirement Accounts (IRA) and Certificates of Deposit (CD).

3. Exception to General Rule of no access (e.g., Proper notification under the Right to Financial Privacy Act).

Financial records may be disclosed in response to an administrative subpoena or summons that meets the requirements of 12 U.S.C. § 3405 that:

- a. There is reason to believe that the records sought are relevant to a legitimate law enforcement inquiry.
 - b. Notice that the IG subpoena has been issued and served on the financial institution must be provided to the customer. Notice to the customer may be by personal service or registered or certified mail. If notified by personal service, the customer has 10 days from the date of service to contest the release of the records by filing an action in the appropriate United States District Court. If the service is by registered or certified mail, the customer has 14 days from the date of mailing to contest the release of the documents.
 - c. Notice to the customer must be served on or before the date the IG subpoena was served on the financial institution.
 - d. A Certificate of Compliance must be signed by the Special Agent-in-Charge and provided to the financial institution prior to receiving the records. The Certificate states that the IG has complied with all applicable provisions of the Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401 to 3422.
4. Pursuant to 12 U.S.C. § 3405, if a customer files an action in the United States District Court contesting the release of his/her financial records, the SA or the person served with the subpoena should immediately forward the documents to OCIG. OCIG will review the documents; prepare the response, including the supporting affidavits; and assist in the preparation for the hearing.

012.010 Subpoena Requests

- A.** When an OIG SA, in consultation with his/her supervisor, determines that there is a requirement for an IG subpoena, a memorandum should be prepared that contains the following information:
1. A summary of the SSA case and the alleged violation, including the statute or section of the Social Security Act at issue.
 2. The name, address, and commercial telephone number of the OIG SA before whom the subpoena is to be returned.
 3. The name; address; contact person or custodian of the records (if available) of the person, partnership, corporation, or business where the subpoena is to be served; and an accurate description of the records sought.
 4. The complete name, Social Security number, and date of birth of the person; or the complete name of the partnership, corporation, or business whose records are being subpoenaed.
 5. The OI case number.
 6. The proposed return date. Because OCIG and OI will review the subpoena, care should be taken in choosing the return date.

7. Whether the SA will serve the subpoena in person or by registered or certified mail.
8. Is the person/entity to be subpoenaed the subject of any non-OIG investigation or any civil, criminal, or administrative proceedings.
9. Has the subject of this investigation been discussed with the Department of Justice (DOJ).

B. In addition to the information listed above in [Section 012.010](#) 1 to 9, the memorandum should contain the following information for a Right to Financial Privacy Act subpoena:

1. The complete name and address of the financial institution to be served with the subpoena and a description of the records sought.
2. The financial institution's internal number for the financial records which are being sought. This includes applicable account numbers.
3. If the financial records being sought are in the name of multiple parties, the name and address of all persons on the financial records should be provided as all must be served.
4. Whether service on the customers whose names are on the financial records is to be personal or by registered or certified mail.
5. Whether notice to the customer should be delayed. Pursuant to 12 U.S.C. § 3409, a motion may be filed in United States District Court requesting a delay of the notice to the customer. If granted, notice may be delayed for up to 90 days, with continuances of the delay possible. To obtain the delay of notice, the following must be shown to the court's satisfaction:
 - a. The investigation being conducted is within the lawful jurisdiction of the SSA OIG.
 - b. There is reason to believe that the records being sought are relevant to a legitimate law enforcement inquiry.
 - c. There is reason to believe that such notice would result in any of the following:
 - (1) endangering the life or physical safety of any person;
 - (2) flight from prosecution;
 - (3) destruction of, or tampering with, evidence;
 - (4) intimidation of potential witness; or,
 - (5) otherwise seriously jeopardizing an investigation or official proceeding or unduly delaying a trial or ongoing official proceeding to the same extent as the circumstances in the preceding subparagraphs.

C. After completion of the memorandum, the SA should draft the appropriate subpoena using the current forms prepared and supplied by OCIG which are located on OCIG's SharePoint site:

(b) (7)(E)

█ The original subpoena and completed memorandum should be forwarded to OCIG via outlook mailbox ^OCIG Subpoenas.

- D. Upon receipt of the original subpoena and memorandum, OCIG will review the subpoena and thereafter forward the subpoena in final form to the appropriate official for signature. Once signed, the original subpoena and a duplicate original will be returned to the SA for service.

012.020 Subpoena Service

- A. Upon receipt of the completed IG subpoena from OCIG, it is the responsibility of the SA requesting the IG subpoena to:
1. Serve the IG subpoena, either by personal service or by registered or certified mail, accompanied by the appropriate transmittal letter ([Exhibit 12-2a-e](#)).
 2. Upon completion of service, complete the “Return of Service” form on the back of the original and duplicate subpoenas. The original subpoena should be left with the custodian of records or the individual named in the subpoena. The duplicate original should be sent to OCIG for its Subpoena Register and will be produced in court should the subpoena be contested. A copy of the duplicate original should be placed in the case file.
 3. Review the records presented by the subpoenaed party to ensure that the records produced are those demanded. Notation should be made in the case file if the records are complete.
 4. Notify OCIG at (b) (7)(E) if the records are not complete or the subpoenaed party refuses to comply with the subpoena.
 5. Refer to Section 018.020 for other administrative requirements when serving subpoenas subject to the Right to Financial Privacy Act.

012.030 Noncompliance

When notified by the SA of noncompliance or partial compliance by the subpoenaed party, OCIG will negotiate production of the records or refer the matter to DOJ for enforcement proceedings.

012.040 Subpoena Register

OCIG will maintain a Subpoena Register of all OIG subpoenas issued and a record of service.

Chapter 12 —

EXHIBITS

12-1 — Reserved for Future Use

Note: Templates for OIG Subpoenas are available on SharePoint:

(b) (7)(E)

Reserved for Future Use

SEARCH AND SEIZURE

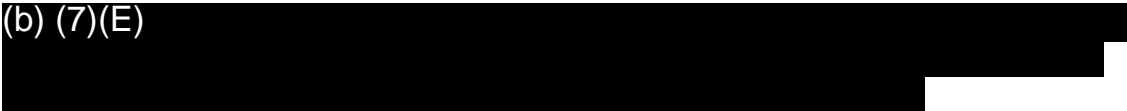
013.000 Purpose

This chapter has been designed to establish SSA/OIG investigative policy and procedures, and to provide guidance in planning and conducting search and seizure operations.

013.010 Policy

A. It is the policy of the SSA/OIG/OI that all searches be conducted, and all seizures be made in strict accordance with all applicable laws and court decisions.

B. (b) (7)(E)



013.020 Protections Afforded by the U.S. Constitution

A. The Fourth Amendment to the U.S. Constitution guarantees that people will be secure in their "persons, houses, papers and effects" against unreasonable searches and seizures. The Amendment further states that no warrant shall be issued, but "upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." The courts view the Fourth Amendment as protection for individuals in areas where they have reasonable expectations of privacy. Those expectations of privacy and the Fourth Amendment protection extend to conversations, homes, automobiles, offices, etc. Therefore, a search warrant or a voluntary consent is required before a SSA/OIG Special Agent can legally conduct a search.

B. The United States Supreme Court has ruled that searches conducted without approval of a judge or magistrate are "per se unreasonable under the Fourth Amendment" (*Coolidge v. New Hampshire*, 403 U.S. 443, 454 [1971]); *Katz v United States*, 389 U.S. 347, 357 (1967). Searches not conducted pursuant to a valid warrant are considered unreasonable, unless the Government can prove to the court that the search comes within an exception to the search warrant requirement.

C. The use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation or Gender Identity as a factor in the performance of law enforcement duties raises numerous Constitutional concerns. In light of these concerns, in December 2014 the Department of Justice (DOJ) published a document entitled "[Guidance for Federal Law Enforcement Agencies Regarding the Use of Race, Ethnicity, Gender, National Origin, Religion, Sexual Orientation, or Gender](#)

[Identity](#).” The 2014 Guidance built upon and expanded the framework of a 2003 DOJ policy on racial profiling, and it reaffirmed the Federal government’s deep commitment to ensure that its law enforcement agencies conduct their activities in an unbiased manner.

013.030 **Search Warrants - General**

- A. SSA OIG Special Agents have the authority to request search warrants as authorized Federal law enforcement officers, and they have the authority to supply an affidavit in support of that warrant application.
- B. A search warrant may be issued by a Federal magistrate or other judge upon the request of a Federal law enforcement officer who presents and swears to an affidavit containing sufficient information to sustain probable cause.
- C. **“Probable Cause”** is defined as the facts and circumstances which would lead a reasonable and prudent law enforcement officer to believe that a crime has been, is about to be, or is being committed, and that evidence of that crime is located at the particular place to be searched.
- D. When the circumstances of an investigation indicate that a search warrant is appropriate, SAs will prepare an affidavit in support of the application for the warrant. All SAs are strongly encouraged to use [Form OI-35](#), Preparatory Checklist for Search Warrant Affidavit ([Exhibit 13-1](#)) when completing the affidavit, and [Form OI-36](#), Search Warrant Supplies Inventory/Raid Kit ([Exhibit 13-2](#)) when making actual preparations to execute the warrant.
- E. Rule 41(c)(1), Federal Rules of Criminal Procedure states that: "The warrant shall be directed to a civil officer of the United States authorized to enforce or assist in enforcing any law thereof, or to a person so authorized by the President of the United States." An authorized officer named (individually or in a class) in the warrant may be accompanied by other law enforcement officers, even if they are not designated in the warrant. Therefore, a warrant specifying service by "any special agent of the Office of Inspector General, Social Security Administration" must be executed by at least one Special Agent of the SSA OIG, who may be accompanied by other Federal agents, and/or local police officers. *Anyone* participating in the warrant execution may lawfully seize evidence.
- F. Search warrants shall be executed as soon as possible after issuance, but in no event later than the ten (10) day limit imposed by Rule 41, Federal Rules of Criminal Procedure, or at a time earlier than the time frame directed by the issuing judge or magistrate.
- G. Searches will normally be made in the daytime. Rule 41(h) of the Federal Rules of Criminal Procedure defines daytime as 6 a.m. to 10 p.m., according to local time. A search that begins during the daytime may extend past 10:00 p.m., if such extension is reasonably necessary to complete the search. Rule 41(c)(1) provides that if the issuing authority finds reasonable cause from facts presented in the affidavit, the authority can, by appropriate provisions in the warrant, authorize execution at any time. Nighttime execution may be justified by extraordinary circumstances such as where the evidence sought is expected to be removed or destroyed during the night. The time of execution is deemed the time the search begins.

013.040 **Tactical Plan**

A Tactical Plan for Search Warrants, [Form OI-18 \(Exhibit 13-3\)](#) *must* be completed in its entirety and approved by the ASAC/RAC and the SAC *prior* to execution of the warrant. A signed and approved copy of the tactical plan must be retained in the case file.

013.050 Mandatory Briefing

- A. Prior to the execution of any warrant, the case agent or other authorized person shall conduct a thorough, in-person briefing of the tactical plan with all team members expected to participate in the execution of the warrant. Team members unable to attend the team briefing must be individually briefed prior to execution of the warrant.
- B. If possible, all participants in the execution of the warrant shall be provided a completed and signed copy of the Tactical Plan at or before the date and time *of the briefing*.
- C. The briefing must specifically address, but is not limited to:
 - 1. The specific location where the warrant is to be executed.
 - 2. The nature, scope and extent of the warrant.
 - 3. The names and assignments of all team members.
 - 4. Identification system for team members.
 - 5. Emergency medical information.

013.060 Video Documentation

Photographs of the point of entry and the areas to be searched shall be taken after securing the location to be searched, and prior to beginning the actual search. Upon termination of the search, photographs shall be taken of the areas searched, and of the point of exit. The photographs shall be maintained in the case file. If possible, video taping of the search should be made to ensure against later claims of impropriety or illegality.

013.070 Execution of Search Warrants

- A. **Announcement** - Title 18, United States Code, Section 3109 requires SAs to announce their identity, authority, and purpose before entry to execute a search warrant. The announcement need not be lengthy or elaborate. It *must*, however, be conveyed in such a manner as to make it unmistakable what is taking place to the person to whom the announcement is made. Following announcement of identity, authority, and purpose, the SA should demand entry. When several SAs participate in the execution of a search warrant, one should be designated to make the announcement.

- B. Exceptions to Announcement Requirement** - When SAs are aware of facts that justify the execution of a search warrant without announcing their presence, such information must be articulated to the magistrate/judge, and the SAs must include in the affidavit those particular circumstances which would support the "no-knock" situation. Accordingly, the announcement requirement need not be complied with under the following circumstances:
1. Where SAs executing the warrant reasonably believe the announcement will place themselves or other persons within the premises in imminent peril of bodily harm.
 2. Where persons within the place to be searched already know of the SA's identity, authority, and purpose.
 3. Where the SA has reason to believe that the evidence sought under the warrant is in the process of destruction or removal.
- C. Entry** - The manner of entry to conduct the search will depend upon the response of the person(s) against whom the search is directed.
1. If the person complies with the entry demand, the agents may enter immediately and conduct the search.
 2. If the person refuses to comply, an immediate forcible entry should be made. The degree of force used must be reasonable; that is, it must be *minimally* sufficient to promptly and safely gain access. That level of force would equate to forcing open a door or window.
 - a. Devices such as pry bars, axes, and battering rams may be used, if necessary to make immediate entry.
 - b. If the person to whom the announcement is made remains silent or responds ambiguously to the entry demand, agents must wait a reasonable time before making a forcible entry. There is no set minimum time. A reasonable time depends on the facts of the case, taking into account such factors as the size of the location, the destructible nature of the evidence, the time of day, and the physical condition of the occupant(s). A reasonable time also may depend on the object of the search. What may be reasonable with respect to stolen computers may not be reasonable when records on flash paper or water-soluble paper are sought.
 - c. If, during the announcement procedure, the agents have reason to believe the evidence sought is in the process of destruction, an immediate entry may be made.
 - d. Agents are under no obligation to argue or negotiate with a person whose property is to be searched nor should they display credentials through peepholes, slide a copy of the warrant under the door, or otherwise delay the execution of the warrant beyond the procedure described above.
- D. Entry by Ruse, Trickery, or Deception** - Unannounced entry to Constitutionally protected premises, obtained by fraud, deceit, or misrepresentation, to execute a search warrant, does not violate Title 18 USC Section 3109; however, entry must be effected without any force whatsoever. Nevertheless, such a practice is generally unnecessary, and should be avoided unless extraordinary

circumstances are present. (b) (7)(E)

- E. Resistance or Interference** - Title 18 USC Section 2231 makes it a felony to forcibly assault, resist, oppose, prevent, impede, intimidate, or interfere with any Special Agent authorized to serve or to execute search warrants, or to make searches and seizures while engaging in the performance of his/her duties. As such, a person may not legally obstruct the execution of a warrant, and can be immediately arrested for doing so.
1. A violation may be shown even though the person resisting does not use force or violence.
 2. Any decision to make such an arrest, as well as an announcement of the arrest to the arrestee(s), can be made by the SA, or by the Federal, State or local law enforcement officers also participating in the operation.
 3. Offensive or abusive language shall not be interpreted as resistance or opposition.
 4. Arrest(s) under this statute require proof that some overt act was performed in an effort to defeat the purpose of the warrant. Threats with a weapon are examples of such overt acts.
 5. Destruction or removal of evidence sought under warrant is a separate criminal violation (Title 18 USC Section 2232), as is any forcible attempt to rescue property already seized by the searching SA (Title 18 USC Section 2233).
- F. Scope of Search** - After having made entry, SAs should take whatever steps are reasonably necessary to protect themselves. SAs should control the movements of persons found inside the premises, and may frisk such persons for weapons based upon a reasonable suspicion that they may be armed.
1. Searches of persons found within the premises for evidence described in the warrant are not permissible unless such persons are particularly described in the warrant.
 2. If the items sought could possibly be concealed on individuals thought to be in the premises, such persons should be named in the warrant.
 3. The search may extend to all places within the premises where the evidence or the persons sought could logically be concealed. The warrant will typically authorize a search of all containers and personal property found on the premises described, including the resident/subject's automobile(s), found on the curtilage that could conceal the items sought.
- NOTE:** If the automobile is parked on the street, it *cannot* be searched under the authority of the premises warrant.
4. The scope of the search is directly related to, and is controlled by the objective of the search.
 5. Agents are under no obligation to begin or end the search at any particular place within the premises.

- G. Duration of Search** - A search under warrant must be terminated when the evidence described in the warrant has been found and seized. Where one of several items described in the warrant has been discovered, the search may continue for other evidence. If no evidence is found, or when the last item specified in the warrant is found, the search must end and SAs must leave the premises. The authority of the warrant to intrude on an individual's reasonable expectation of privacy extends only as long as is reasonably necessary to search. Special Agents who remain on the premises for an unreasonable period become trespassers, and any subsequent evidence obtained may be suppressed.
- H. Intensity of Search** - The search warrant is not a license to destroy property or to harass individuals. It will permit, however, under certain circumstances, a highly intensive search that may disrupt and damage property. Thus, a floor may be pulled up, or a wall torn down, or a garden dug up, where SAs have a reasonable belief the evidence sought under the warrant has been concealed in such a place. *Such actions should be taken only under the most persuasive circumstances.*
- I. Plain View Doctrine** - Where SAs are lawfully present on the premises (as during the execution of a warrant), and they observe evidence or contraband in plain view, such evidence or contraband may be seized, even though it is not described in the warrant and not relevant to the offense under investigation. In order to validate the seizure, a SA must have probable cause to believe that what is observed in plain sight is evidentiary, and the discovery must be inadvertent or unanticipated. The plain view doctrine will not permit the seizure of evidence from a place within the premises where the SA has no right to be, even though the agent is lawfully on the premises. The three necessary elements for a lawful plain view seizure are:
1. Special Agents must be lawfully present. Simply stated, SAs must be legally justified in being where they are at the time the plain view observation is made.
 2. Discovery must be inadvertent.
 3. Item(s) must be of an *immediately apparent incriminating nature*. SAs making the seizure must have probable cause to believe, without further investigation, that the item in plain view is evidence.
- J. Inventory and Receipt** - All property taken from the premises during the execution of a search warrant must be accounted for and inventoried on [Form OI-23](#), Inventory Form, and [Form OI-23A](#), Inventory Form Attachment (*see Exhibits 13-4 and 13-5*).
1. The inventory will consist of an itemized list of items seized, recorded on the OI-23 and OI-23A by the designated Custodian of Evidence.
 2. The inventory should be prepared in the presence of the person from whom the property was taken. If the person from whose premises the property was taken is not available, the inventory should be made in the presence of at least one credible witness and verified by two special agents.
 3. Items seized under the plain view doctrine, or a weapon taken for safety reasons, though not described in the warrant, must be accounted for on a separate receipt which may be prepared on a plain sheet of paper and accurately identified.

[See Chapter 14, Acquisition, Preservation and Management of Evidence](#), for a complete explanation of evidence handling procedures.

- K. Leaving Copy of Warrant** - Special Agents who have executed a search warrant will give a copy of the warrant to the individual whose person, premises, or property is to be/has been searched, or to the person in control of the premises, whether or not any evidence is seized under the warrant. If no one is present during the search, a copy of the search warrant will be left in a conspicuous place so that the owner of the premises may find it.
- L. Return** - The return of a search warrant is the report to the issuing judicial authority that the warrant was executed, Said return should be made as soon as practical after execution. Although a prompt return is required, a failure to make a prompt return will not invalidate the search warrant or the items seized, as that is considered to be an administrative procedure following the search.
- M. Securing the Premises** - Upon conclusion of a search made under a warrant, it is the responsibility of Special Agents to make certain the place searched has been secured. In the absence of a resident, SAs are to take whatever steps necessary to render the premises inaccessible to those having no legitimate business within the premises.
1. Where a door has been broken upon entry, it must be repaired, replaced, or boarded up before the SAs depart.
 2. If a third party, such as a carpenter, is required to secure the premises, an agent should remain until such work is completed.
- N. Damage to Property** - Where performance of duty results in damage to private property, such as a broken door, the property owner may be entitled to compensation, even where there was legal justification for the entry and search. Government funds are available for satisfaction of justified claims arising from such damage. In a case where a claim is likely to be filed, the SA in charge of the search shall ensure that photographs of such damage are obtained, and that the details surrounding the damage are recorded in a [Form OI-4](#), Report of Investigation, which will be retained in the case file.
- O. Criminal Liability** - Any Special Agent who maliciously and without probable cause procures a search warrant to be issued and executed is subject to criminal prosecution.
1. In executing a search warrant, agents are criminally liable where they willfully exceed authority or exercise their authority with unnecessary severity.
 2. Any Special Agent who maliciously and without probable cause, searches property without a search warrant, is likewise guilty of a felony violation of Federal law (Title 18 USC Sections 2234, 2235, 2236).
 3. A special agent may also be subject to a civil lawsuit as a result of improper actions. While there is no specific statute under which a Special Agent may be sued, "*Bivens v. Six Unknown Named Agents of the Federal Bureau of Narcotics*" provides the aggrieved party with a course of action.

- P. Recovery of Money** - Whenever money or other property consisting of numerous items requiring counting is obtained in connection with a search warrant, the money or property is to be independently counted by two Special Agents, and their separate results compared for the purpose of verifying the accuracy of the count and detecting any errors.
- Q. Weapons and Serialized Items** - Whenever weapons are seized as a result of a search, they shall be checked against the NCIC record to determine if they have been reported stolen or have been used in the commission of a crime. All other serialized items seized during a search should also normally be checked against the NCIC.
- R. Debriefing** - When a search warrant has been served, and all operational matters have been completed incident to the warrant, the case agent shall schedule a debriefing.
1. The debriefing should take place as soon as possible, and maximum attendance by all participants should be encouraged.
 2. Items such as the level of participation by outside agencies and "lessons learned" should be addressed at the debriefing. Participants should bring to the attention of the case agent any items or incidents that occurred during the search which may become an issue at a later date.
 3. Notes of the debriefing should be maintained in the case file.

013.080 Warrantless Searches

Exceptions to the search warrant requirements are searches incident to a lawful arrest, searches justified due to exigent circumstances, and searches made with the voluntary consent of the person being searched.

- A. Search Incident to Arrest** - When a search is made incidental to an arrest, the validity of the search depends upon the legality of the arrest. Thus, if the arrest is subsequently held to be illegal, then any search incidental to that arrest will also be illegal, and any items seized will be inadmissible as evidence.
1. Searches incident to arrest are for the purpose of protecting the arresting officers and preventing the destruction of evidence.
 2. The scope of such a search is limited to the arrestee's person and the area within their immediate control, meaning "the area from within which he might gain possession of a weapon or destructible evidence" (*Chimel v. California*, 395 U.S. 752, 763 (1969); *U.S. v. Chadwick*, 433 U.S. 1 [1977]).
 3. **“Good Faith” Arrest** - An arrest, even though lawful, may not be used as a pretext to search for evidence of a different, unrelated crime for which SAs have no grounds to arrest or to search. Where the arrest for the first offense is made in good faith, however, and evidence of an unrelated crime is discovered inadvertently in the course of a search made incidental to the arrest, such evidence may be admissible.

- 4. Contemporaneous Search** - A search incident to an arrest must be made at the same time and place as the arrest by the SAs imposing custody. To be contemporaneous, the search must occur at the same time as the arrest, or be so connected with the arrest as to form a part of the continuous, uninterrupted, lawful act.

 - a. A search of the area immediately surrounding the arrestee should be conducted at the time of or shortly after the arrest, while the person being taken into custody is still present.
 - b. A further, more thorough search of the person at some other place to which the arrestee is transported is justified as being incidental to the arrest.

- 5. Intensity of Search** - A search incident to arrest may be as thorough as necessary to protect the arresting agents and the arrestee, preserve any evidence, and to prevent escape. A court order or search warrant must be obtained before a body cavity search is conducted unless there is “imminent fear of serious bodily injury or death”, as stated in 013.010 C. Prior to seeking a court order or warrant, the SA must articulate that:

 - a. There is probable cause to believe that an item subject to seizure is concealed within the body cavity.
 - b. The item must be removed by a physician under proper medical conditions, or the person must voluntarily remove the item himself/herself, and,
 - c. There is no other known means of obtaining the item.

- 6. Use of Force** - Special Agents making a full-custody arrest have the right to search the person arrested. Resistance by the arrestee does not defeat that right. Special Agents may use a reasonable degree of force to search the arrestee when the purpose is self-protection, prevention of escape, and/or the preservation of evidence.

- 7. Scope of Search** - Following a lawful arrest, Special Agents are entitled in all cases to search the person of the arrestee, and anything within his or her immediate control at the time of arrest.

 - a. The search may include any portable personal property in actual possession of the arrestee, such as clothing, purses, briefcases, grocery bags, etc.
 - b. Absent an emergency, inaccessible, non-portable items of personal property, such as a locked suitcase, or a sealed carton or crate, may not be searched. If there are reasonable grounds to believe they contain evidence, they may be seized and a search warrant should thereafter be obtained prior to opening.

- 8. Inventory of Personal Property** - Items of personal property (any movable or tangible thing that is subject to ownership and not classified as real property) removed from a person who has been arrested must be carefully inventoried by SAs prior to being stored for safekeeping.

 - a. A receipt for such property should be prepared and given to the arrestee.
 - b. That inventory should be made in good faith, and not as a pretext or excuse for conducting a warrantless search for evidence.

- c. The purpose of a legitimate inventory is to protect the owner's property; to protect the seizing agents from false claims; and/or to protect the SAs/general public from potential danger.
 - d. The inventory should include the contents of containers such as purses, shoulder bags, suitcases, etc., whether or not the containers are locked or sealed. In the event such containers are locked or sealed, great care must be taken to minimize damage to the container or its contents while gaining access. This care-taking function must not be construed as an alternative to a search warrant whenever there is probable cause to believe that evidence or contraband is inside a container. Under those circumstances the container should be secured until a search warrant can be obtained.
 - e. Personal property *not* held as evidence shall be returned to the rightful owner. SAs must document to whom the property was returned, the means by which it was returned (e.g. hand delivered directly to the owner, given to the owner's attorney, etc.) and the date on which the property was returned. The person to whom the property is returned must sign and date a receipt, or sign and date a copy of the [OI-21](#) (see Chapter 14) on which the property is described, to acknowledge that the property was returned. The original signed receipt shall be placed in the case file. Under exceptional circumstances and with SAC approval, property may be returned to the rightful owner via registered mail.
 - f. See Chapter 14, "Acquisition, Preservation and Management of Evidence," for a complete explanation of evidence handling procedures.
- 9. Protective Sweep** - When Special Agents enter premises to effect a lawful arrest, they have the right to take reasonable steps to protect themselves and to ensure that they will not be interfered with in the performance of their duties. Therefore, they may properly conduct a cursory search of the premises if they have a reasonable suspicion that confederates, accomplices, or others are present and may jeopardize the safety of the arresting Special Agents or the arrestee.
- a. Reasonable suspicion must be based upon facts known to the SAs, such as noises in an attic or the at-large status of a dangerous confederate.
 - b. The cursory search is not justified solely by the arrest. Rather, it is an independent search authority aimed at protection of the arresting agents. It may not be an extended search, and must not be used as an exploratory quest for evidence. As such, it is limited to a brief inspection of only those places within the premises that could conceal a person capable of interfering with the arrest.
 - c. If a Special Agent, while conducting a protective sweep, observes evidence in plain view, it may be seized under that doctrine.
- 10. Receipt and Certificate** - A receipt for any property taken in a search incidental to arrest is to be given to the person from whom it is taken. The receipt is an itemized list describing each item seized, prepared in duplicate. One copy will be given to the person from whom the property was obtained, and the original of the receipt will be retained in the case file. Erasures or corrections are to be initialed by the arrestee. See Chapter 14, "Acquisition, Preservation

and Management of Evidence,” for a complete explanation of evidence handling procedures (specifically section 014.090.I, “Final Disposition of Evidence”).

11. Stop and Frisk - In *Terry v. Ohio*, the Supreme Court held that a law enforcement officer does not need probable cause to stop a suspect for questioning if unusual suspicious activity leads the officer to conclude, in light of his/her experience, that "criminal activity may be afoot." Persons who are stopped by law enforcement officers are not necessarily under arrest, even though their right to move at will is restricted for some time. Such "stop and frisks" are allowed only when a law enforcement officer with arrest authority stops a person based upon reasonable suspicion. The "frisk" in such cases must be limited to a search for weapons by a pat down of the person's outer garments.

B. Exigent Circumstances - Warrantless searches based upon probable cause have been limited to those situations involving some exigency or a compelling urgency for the protection of the police or public, or to prevent the destruction of contraband or evidence. Courts have often approved these searches as an exception to the warrant requirement where officers can establish that the circumstances were exigent, i.e., so urgent that immediate action was required justifying a failure to obtain a warrant. The Supreme Court has said that warrantless searches are permitted:

1. when officers reasonably believe that someone is in immediate need of assistance;
2. to protect or preserve life; or
3. to avoid serious injury.

C. Consent Searches - A valid search of premises may be made without a warrant and without probable cause if the person in lawful possession gives voluntary consent. **NOTE:** The key expression is “lawful possession,” not ownership. Possession is the right to occupy and enjoy use of the premises to the exclusion of all others.

1. *Mere submission to authority by the person at the premises to be searched is not valid consent.*
 - a. Obtain consent to search from the person in possession.
 - b. That consent should be obtained in writing, if possible and should specify the scope and intensity of the contemplated search on [Form OI-26](#), Consent to Search (computer-generated) or [Form OI-26L](#) (handwritten) (*Exhibits 13-6 and 13-7*).
 - c. If the search involves computers or electronic media, the agent shall execute [Form OI-91](#) Consent to Search Computers/Electronic Media ([Exhibit 4-19](#)).
 - d. The consenting party may limit the scope of the search and the items to be seized.
 - e. The consent can be revoked by the consenting party at any time prior to the completion of the search, although what has already been discovered before the revocation may be introduced in evidence or used as probable cause to obtain a warrant.
 - f. A third party may consent to a search, but only to the extent that he or she exercises authority or control over the areas or items to be searched.

- g. An employer may permit a search of common areas within the business building, but may not grant authority to search places or things reserved for the exclusive use of the employee.
2. The test of the validity of the consent is voluntariness. Whether consent is given freely and voluntarily is decided by the facts as determined by the court, which will look at all the surrounding circumstances. A Special Agent preparing to search under this authority must take three steps, as follows:
 - a. Determine whether the premises are protected by the Fourth Amendment. Some areas, such as open fields, public places, and abandoned property, can be searched lawfully without consent or a search warrant, and any incriminating evidence uncovered may be used.
 - b. If the premises enjoy the Constitutional protection against unreasonable searches, identify the person currently lawfully entitled to possession. Special Agents should make intensive efforts to identify exactly who has lawful possession and actual authority to consent to a search. That might require record checks, and most certainly entails the careful questioning of the person believed to possess the premises.
 - c. Conduct the search within limitations expressed or implied in the consent.

013.090 Abandoned Property

A longstanding doctrine of search and seizure law permits the taking of property that has been abandoned, so long as the abandonment has not been caused by prior illegal police conduct. The majority of cases dealing with the abandonment issue relates to personal property, i.e., automobiles, garbage, narcotics, gambling records, weapons, etc. Premises (homes, apartments, hotel rooms, places of business) can be abandoned as well. Abandonment of premises deprives the former possessor of the right to assert that his/her rights were violated by police entry, search or seizure. Abandoned property has no Fourth Amendment protection because either the defendant has given up reasonable expectation of privacy in that property, or the defendant no longer has standing to object to use of the evidence in court, or both.

- A. **Definition** - Abandonment in the Constitutional sense means the voluntarily casting away or relinquishing of possession of property with no present intention of reclaiming it. It is the intentional and voluntary relinquishment of the reasonable expectation of privacy. If a person abandons ownership, right to usage, possession or interest in his/her real or personal property, then that property may be searched or seized without a warrant.
- B. **Proof of Abandonment** - In order to prove abandonment, the prosecution must be prepared to show the intent of the former possessor at the time he or she abandoned the property. Because the relinquishing party seldom announces intent to abandon, the state of mind must be proven circumstantially. SAs must be prepared to present evidence bearing on the fact of relinquishment of the premises, such as present whereabouts of the former possessor, circumstances of his/her departure, duration of his/her absence, condition of vacated premises, remarks made prior to or after departure of the former possessor, provisions of rental agreements, etc.

1. Consent to enter or search need not be obtained from the abandoning party, but SAs should obtain authority from the person to whom lawful possession has reverted.
 2. Where exigent circumstances do not exist, or where the premises can be secured, a search warrant should be obtained prior to entry.
- C. **Trash** - Federal courts have held that personal property discarded in a common trash pile or garbage can placed out for collection has been abandoned. No privacy interest remains in the property and no standing may be claimed by the prior possessor. The courts also recognized no significant difference between trash seizures made directly by law enforcement officers, and those in which a third party is recruited to take and secure the discarded items for later inspection by officers.

Special Agents contemplating a warrantless trash inspection should be thoroughly familiar with state as well as Federal principles governing the search or seizure of trash, since state courts may impose, under state constitutions, more restrictive rules than those announced by Federal courts.

013.100 **Vehicle Searches**

- A. The same authority that allows searches of persons and premises applies to motor vehicles. Thus, an automobile may be searched under a search warrant if it is located in the jurisdiction where the warrant is outstanding.
1. The vehicle may also be searched by consent of a party having lawful possession of the vehicle.
 2. The vehicle may be searched pursuant to the arrest of the driver or an occupant, as long as the arrest occurs within or in close proximity to the vehicle.
 3. The general rule that the search incident to arrest may extend to those areas within the immediate control of the arrestee at the time of arrest has been construed to mean the entire passenger compartment including any containers located therein such as closed or open glove compartments, consoles, luggage, boxes, bags, or clothing, etc. If such containers are locked or sealed, they should not be searched without a warrant in the absence of some emergency or the voluntary consent of the party having possession.
 4. The search incident to arrest, however, *may not* extend into the trunk of the vehicle.
- B. **Vehicle Exception** - Due to their mobility and the diminished expectation of privacy generally associated with them, vehicles may be searched without a warrant under circumstances that would not permit the same actions against other property.
1. A search of a vehicle found on the open road or other public place may be made without a warrant, consent, or arrest, where SAs have *probable cause* to believe the vehicle contains evidence of a crime and it is impractical to obtain a search warrant.
 - a. Although a search under this doctrine should generally be made where the vehicle is found, the search may occur at the place to which the vehicle is towed or transported, so long as probable cause still exists.

[13-1 — Preparatory Checklist for Search Warrant Affidavit \(OI-35\)](#)

[13-2 — Search Warrant Supplies Inventory/Raid Kit \(OI-36\)](#)

[13-3 — Tactical Plan for Search Warrants \(OI-18\)](#)

[13-4 — Inventory Form \(OI-23\)](#)

[13-5 — Inventory Form \(Attachment\) \(OI-23A\)](#)

[13-6 — Consent to Search – Computer generated \(OI-26\)](#)

[13-7 — Consent to Search - Handwritten \(OI-26L\)](#)

SOCIAL SECURITY
Office of the Inspector General

PREPARATORY CHECKLIST FOR SEARCH WARRANT AFFIDAVIT

(b) (7) (E)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

SEARCH WARRANT SUPPLIES INVENTORY/RAID KIT

(b) (7) (E)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

Tactical Plan for Search Warrants

(b) (7) (E)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

(b) (7) (E)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

Consent to Search

Date: _____ Location: [Click **here** and type Location]

I, [Click **here** and type Consentor's Name], have been informed of my constitutional right not to have a search made of [Click **here** and type Object to be Searched] without a search warrant. I have also been informed of my right to refuse to consent to such a search. However, I hereby authorize [Click **here** and type Name] and [Click **here** and type Name], [Click **here** and type Titles of Officers or Agents and Names of Agency] to conduct a complete search of [Click **here** and type Object to be Searched] at [Click **here** and type Location]. These (officers or agents) are authorized by me to take any letters, papers, materials, or other property that is contraband or evidence in the nature of [Click **here** and type Investigation Type]. I understand that this contraband or evidence may be used against me in a court of law.

This written permission is being given by me to the above persons voluntarily and without threats, duress, or promises of any kind. I understand that I may ask for and receive a receipt for all things taken.

Signature of Witnesses:

Signature of Consenter:

Witness Signature

Date

Consenter Signature

Date

Witness Signature

Date

Print Name of Consenter

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.**

SOCIAL SECURITY
Office of the Inspector General

Consent to Search

Date: _____ Location: _____

I, _____, have been informed of my constitutional right not to have a search made of _____ without a search warrant. I have also been informed of my right to refuse to consent to such a search. However, I hereby authorize _____ and _____, _____ to conduct a complete search of _____ at _____.

These (officers or agents) are authorized by me to take from the premises and/or automobile any letters, papers, materials, or other property that is contraband or evidence in the investigation of _____. I understand that this contraband or evidence may be used against me in a court of law.

This written permission is being given by me to the above persons voluntarily and without threats, duress, or promises of any kind. I understand that I may ask for and receive a receipt for all things taken.

Signature of Witnesses:

Signature of Consenter:

Witness Signature Date

Consenter Signature Date

Witness Signature Date

Print Name of Consenter

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.**

ACQUISITION, PRESERVATION, AND MANAGEMENT OF EVIDENCE

014.000 General

- A.** Evidence, obtained through investigation, is the means by which any alleged action, the truth of which has been submitted to investigation, is established or disproved. Evidence aids in resolving issues, connecting a subject with an offense or, in general, establishing facts in criminal, civil and administrative proceedings.
- B.** Special Agents (SA) are primarily engaged in obtaining evidence for possible use in Federal criminal proceedings. As such, SAs must develop a basic understanding of the “Federal Rules of Evidence” (FRE), the Federal Rules of Criminal Procedure, and the Federal Rules of Civil Procedure. Both sets of rules are found in West Publishing Company’s *Federal Criminal Code and Rule and the Federal Civil Judicial Procedure and Rules*. SAs must be careful and refer only to the most current version. Questions regarding the admissibility of evidence should be discussed with the prosecuting attorney and/or the Office of the Counsel to the Inspector General.

014.010 Federal Rules of Evidence

- A.** The FRE apply to proceedings in Federal courts, and before United States bankruptcy judges and magistrates.
- B.** The FRE specifically address such matters as judicial notice (Rule 201), character evidence (Rules 401-406), the competency of witnesses to testify (Rules 601-606), expert testimony (Rules 701-706), and the definition and admissibility of hearsay evidence (Rules 801-806).

014.020 Admissibility, Relevancy, and Competency of Evidence

- A.** **Admissibility** – The quality that makes evidence acceptable in court. To be admissible, evidence must be relevant and competent.
- B.** **Relevancy** - If a fact offered into evidence relates in some logical way to the main fact, it is said to be relevant. The word relevant implies a traceable and significant connection.
 - 1.** FRE 401 states that “Relevant Evidence” is evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence.

2. FRE 403 requires that relevant evidence be excluded “if its probative value is substantially outweighed by the danger of unfair prejudice, confusion of the issues . . . or misleading the jury, or by considerations of undue delay, waste of time, or needless presentation of cumulative evidence.”

NOTE: Materiality used to be one of the criterions for the admissibility of evidence, but has since been included in the definition of relevancy.

- C. **Competency** - Competent evidence is evidence that is legally admissible. Evidence must be logically relevant *and* legally admissible. Relevant evidence may be incompetent and, therefore, inadmissible, such as hearsay, or not the best evidence. As applied to evidence such as documents, evidence is competent if it was obtained in a manner, in a form, and from a source, proper under the law.

014.030 Burden of Proof

Burden of proof refers to the *quantity* of evidence required by law to prove a matter in dispute, i.e., sufficient evidence to substantiate one or more violations of all elements of a crime. The *quality* of the evidence is decided by the judge and/or the jury. The burden of proof generally falls upon the proponent of the issue, and in a criminal case, the Government must prove all elements of a crime beyond a reasonable doubt. Generally, administrative or disciplinary actions need only be supported by substantial evidence. Preponderance of the evidence is a standard of proof which is met when a party's evidence on a fact indicates that it is "more likely than not" that the fact is as the party alleges it to be. The burden varies according to the type of action, as follows:

1. Beyond a reasonable doubt (criminal prosecutions).
2. Preponderance of evidence (civil actions).
3. Substantial evidence (administrative actions).

014.040 Best Evidence Rule

- A. The FRE provide that, in order to prove the content of a document, the original is required, except as otherwise provided for in the FRE. This principle is commonly known as the “Best Evidence Rule” (Rule 1002).
- B. FRE 1003, which deals with the “Admissibility of Duplicates,” provides that a duplicate is admissible to the same extent as an original unless a genuine question is raised as to the authenticity of the original, or in circumstances where it would be unfair to admit the duplicate in lieu of the original.
- C. FRE 1004 deals with the “Admissibility of Other Evidence of Contents,” and provides that other evidence of the contents of a writing, recording, or photograph are admissible if:
 1. all originals are lost or have been destroyed (unless the proponent lost or destroyed them in bad faith); or

2. no original can be obtained by judicial process; or
3. the original is under the control of the party against whom offered, who, after being notified that the contents would be a subject of proof, does not produce the original; or
4. the writing, recording, or photograph is not closely related to a controlling issue.

D. Where documentary evidence is otherwise admissible, it is necessary to have the evidence authenticated by one of the following methods:

1. Testimony of a subscribing witness or a witness with knowledge that the document is what the prosecution will claim it to be.
2. Non-expert opinion on handwriting based on familiarity of the witness not gained for trial purposes; e.g., an employee testifies as to his employer's signature/handwriting.
3. Comparisons by the trier of fact (judge or jury) or expert witnesses to other documents which have been authenticated.
4. Distinctive characteristics such as appearance, contents, substance, and patterns, taken in conjunction with other circumstances.
5. Prior admission or acknowledgment; e.g., documents acknowledged before a notary public or admitted in a statement.
6. Self-authentication of public documents (See FRE 902).

014.050

Computer-Based Evidence

A. Principles

1. Data contained on computers or other media with evidentiary potential must be preserved in the condition in which it was found.
2. In exceptional circumstances where a person finds it necessary to access original data on a target computer, that person must be competent to do so, and to give evidence explaining the relevance and the implications of their actions.
3. An audit trail or other record of all processes applied to computer-based evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
4. The case SA is responsible for ensuring that the law and these principles are adhered to until such time as the evidence is under the control of the Forensic Intelligence and Analysis Division's Digital Forensics Team (DFT).

B. To obtain DFT support, an FD agent must submit a request by clicking on the "Request DFT Assistance" button on the Case Data screen in the National Investigative Case Management

System (NICMS). Once completed, the request for DFT assistance will be routed to the FD ASAC/RAC for review and approval. Once the request is approved by the ASAC/RAC, the case will be forwarded to the SAC/ASAC of IAD for approval and assignment to a Forensic Analyst/Specialist. The request must contain the following: case number, name of case agent, and a description of the services requested.

- C. DFT provides technical assistance, on-site support, and laboratory analysis for computer-related investigations.

014.060 Evidence Management Procedures

- A. **Evidence Collection** - Special Agents will obtain evidence in a manner and form admissible in a court of law so full equity and justice are accorded the subject of an investigation.

The unique nature of OIG investigations requires practical policy and feasible procedures for identifying, securing, and handling evidence. As soon as an item is determined to be evidence, it must be documented on an Evidence/Property Report, [Form OI-21 \(Exhibit 14-1\)](#). The SA will identify each item of evidence to include the following:

1. Date of acquisition,
2. Source, and,
3. Circumstances of receipt (incident to arrest, voluntary release, etc.).

- B. **Marking Evidence for Identification** - All articles legally seized as evidence should be carefully marked for identification *unless* said marking would irreparably damage the evidentiary and/or intrinsic value of the item. If so, the evidence is to be placed in a suitable container, which should then be sealed and properly marked in front of at least one (1) witness.

1. The markings should be made in such a manner as to preclude the possibility of the marks being obliterated.
2. Identifying marks should be such as to make it possible for the person or persons who obtained the evidence to testify at a later date that this particular article was found at a certain place at a certain time. Each mark, such as an SA's initials, should be distinctive; therefore, an "x" should never be used.
3. Evidence obtained and placed in containers or envelopes must be appropriately identified.
4. Detailed notes should be made describing the articles found to include serial numbers or other distinctive markings, the place they were found, the date found, and the persons who found them and the identifying mark placed on each. The original notes should be preserved in the official case file for future references.
5. Special agents should employ good judgment and consider the shape and physical composition of evidence in determining where and how a particular item should be marked.

- C. Handling and Preservation of Evidence** - All evidence must be handled and maintained in a manner consistent with preserving it in the condition in which it was collected.
1. Evidence must not be marked, folded, or contaminated in any manner that would compromise its authenticity. Care should be taken to avoid abusing original documentary evidence by punching, blocking, stamping, stapling, or tearing.
 2. A document needed as evidence should not be touched with a pencil or pen (except for your identification marking in a corner of the reverse side), paste, liquids, or other materials which leave marks, or be exposed to moisture or prolonged heat.
 3. Physical evidence should be handled as little as possible for safekeeping. Use of special gloves and document protectors are the best ways to preserve the integrity of the document and limit contamination.

D. Methodology

1. Each SAC will designate an evidence custodian and alternates for each investigative office. The evidence custodian will assure that case SAs properly enter, maintain, transfer, document, and dispose of evidence.
2. SAs will be responsible for properly entering, maintaining, transferring, documenting, and disposing of evidence for their assigned cases. SAs will be prepared to testify regarding evidence custody.
3. Where feasible, the SAC will designate a secure room to be used solely for the storage of evidence. In offices that utilize secure multipurpose rooms to house both evidence and other items (i.e., technical equipment, case files, etc.), evidence will be stored in a fixed safe, filing cabinet, or other container suitable for storage inside the secure multipurpose room. In instances where even a secure multipurpose room is unavailable, a fixed safe, filing cabinet, or other container suitable for storage will be used to store evidence. The evidence storage facility or container will be secured by a locking device. Combinations/keys to locks for such rooms or containers will be restricted to the SAC, evidence custodian, and alternates.

E. Evidence Property Report

1. The evidence custody process will be initiated as soon as possible by the SA identifying and/or receiving the evidence. [Forms OI-21](#), Evidence/Property Report; [OI-21A](#), Description of Property Acquired; and [OI-21B](#), Chain of Custody (*Exhibits 14-1, 14-2, and 14-3*) will be completed, as necessary, by the case SA or other authorized person. **The original copy of the forms will remain with the evidence at all times.** A photocopy of the forms will be retained in the case file and the SA's working file. In instances when an [OI-23/23A](#) (Inventory Form /Inventory Form Attachment) has been established, those forms may be attached to the OI-21 to serve as the item number/description. Form OI-21 should refer to the attached OI-23/OI-23A (*see Exhibits 14-4 and 14-5*).
2. The OI-21 Evidence Property Report serves as an evidence tag, chain of custody log, and final disposition report.

3. Each office will establish a central evidence file in which photocopies of the original OI-21, OI-21A, and OI-21B will be maintained for any evidence currently housed in the evidence storage room or container. The file should be located in the evidence storage facility or container, where applicable.
4. Each office will maintain a permanently bound evidence logbook to document the initial receipt of evidence into evidence storage and the final disposition of evidence storage. The logbook will contain the date evidence was entered into storage, case number, case agent name, and the date evidence was removed for final disposition. The logbook must never have pages ripped out, as this will be a running and historical log of evidence placed into and later removed from evidence storage. The logbook should be located in the evidence storage facility or container, where applicable.
5. The SA should obtain working copies of pertinent documents, photographs, recordings, etc., in order to preclude unnecessary handling of the evidence.
6. All evidence will be inventoried and sealed in an envelope, box, or other sealable container applicable to the size and construction of the item(s), as deemed necessary and appropriate.
 - a. When used, the container will be identified as evidence with the original OI-21 attached on the outside by the SA, in the presence of a witness, if possible.
 - b. Both the SA and the witness will apply their signatures and the date across the seam of the evidence containers.
 - c. The sealed container containing evidence will then be transferred to the evidence storage room or container.
 - d. **A separate OI-21, 21A, and 21B will be prepared for each sealed container.**
7. At each subsequent change in custody of the evidence, the evidence property report/chain of custody forms will be annotated and signed by the recipient to maintain a record of the change in custody. In the event the appointed evidence custodian's duties are transferred to another individual, the change in evidence custodian will be documented on all OI-21s housed in the evidence room or container at the time the change is made.
 - a. **The original form(s) shall remain with the evidence at all times.**
 - b. Copies of all changes shall be maintained in the central evidence file and case file.

F. Handling Special Types of Evidence

1. **Money** – Evidence custodians are directly responsible for the proper handling, prompt reporting, and timely disposition of all monies and negotiable instruments handled by SAs under their supervision to be held for evidence, forfeiture, or safekeeping. All monies, whether being held for evidence, forfeiture, or safekeeping will be:
 - a. Counted and amounts recorded on Form OI-21 with a witness present, and,

b. Controlled as evidence in accordance with the *Special Agent Handbook* instruction.

2. **Video and Audio Recordings** – All original recordings, oral, digital, and video, including contemporaneously recorded backup audio recordings and CDI surveillance video recordings, will be treated as evidence, and will immediately be secured as outlined above. In addition to the previous requirements, SAs will include a statement of the make, model, serial number, and source of recording equipment used, as well as the identification of the operator.
3. **Photospreads and Identification Pictures** – Each photospread or picture displayed to a witness, including SAs, for purposes of potential use in court identification will be maintained as evidence upon conclusion of its use.

G. Transfer of Evidence – Evidence material to be transferred to the custody of a forensic laboratory, the United States Attorney’s Office (USAO), court clerks, and other authorized recipients will be hand-carried or sent by registered/certified/express mail service through the United States Postal Service, or by Federal Express (or other OIG-authorized private mail service).

1. A receipt attesting to the dispatch of the evidence will be maintained in the case file.
2. When transfers of evidence are made, the chain of custody is to be maintained by the special agent making the transfer by recording his/her name and date on the original OI-21, which must remain with the evidence.
3. Prior to transfer, all evidence should be photocopied or photographed.

H. Final Disposition of Evidence – Instructions for return, destruction, or other disposition of evidence will be sought from the appropriate prosecuting authority, when applicable. Normally, the following procedures will apply.

1. Title 28 U.S.C. § 2042 and 18 U.S.C. § 3612 provide that monies received or tendered as evidence in any United States court should be disposed of by the court. If possible, the SA should work closely with the appropriate prosecutor to ensure the proper handling of the monies. This should include pre-seizure planning when the SA becomes aware that monies may be seized in an investigation.
2. If the court has ordered restitution in a program fraud case or a fine in a non-program fraud case, the court can specify in its order that the cash held in evidence is to be applied towards the restitution and/or fine.
3. If the court orders funds to be applied towards restitution and/or a fine, the case agent must follow the SAH’s guidance (SAH 014.060, Section G) regarding the removal of funds from evidence and provide the funds to the Clerk of the Court to comply with the court’s order.
4. Monies that are not entered as evidence in court proceedings will be returned to the rightful owner or the United States Department of the Treasury through deposit with the appropriate Regional Fiscal Officer. Appropriate receipt will be obtained, and will be made part of the case file. If there is an issue as to the ownership of the monies, the SA should work closely

with the Department of Justice to ensure the monies are returned to the rightful owner or the United States Department of the Treasury.

5. Since OI does not have asset forfeiture authority, according to DOJ's Asset Forfeiture and Money Laundering Section, asset forfeiture procedures will be applicable to cash seized by OI, in the course of an investigation, only if a Federal agency with forfeiture authority "adopts" OI's case for forfeiture purposes. Case agents should consult with the prosecuting attorney to determine the appropriate method for the disposal of funds held as evidence.
6. Original oral and videotapes, including contemporaneously recorded backup tapes, shall be maintained for a period of at least 2 years after the closing of the case.
7. Original tapes of non-consensual monitoring shall not be destroyed except upon an order from the issuing or denying judge.
8. Paper and documents may be disposed of when all avenues of appeal have been exhausted. Original documents should be returned to the source. Original affidavits, forensic reports, schedules, and similar materials should be retained in the permanent case file until final disposition is determined.
9. Personal property used as evidence should be disposed of as directed by the prosecuting authority. Such property that relates to cases that are not prosecuted should be returned to the source upon case closure, except that personal property subject to claims of ownership of other rights shall be disposed of as directed by the Department of Justice.
10. Personal property not held as evidence shall be returned to the rightful owner. SAs must document to whom the property was returned, the means by which it was returned (e.g. hand delivered directly to the owner, given to the owner's attorney, etc.), and the date on which the property was returned. The person to whom the property is returned must sign and date a receipt, or sign and date a copy of the OI-21 on which the property is described, to acknowledge that the property was returned. The original signed receipt shall be placed in the case file. Under exceptional circumstances and with SAC approval, property may be returned to the rightful owner via registered mail.
11. After final disposition, the SA will annotate the original and all copies of Form OI-21 to reflect the disposition of each item of evidence. *The original OI-21 will be transferred to the case file after disposition of the evidence.*

014.070 Grand Jury Information

- A. Grand Jury materials should be kept in locked containers or file cabinets by SAs and not located with other evidence. It is not necessary to complete an OI-21 for Grand Jury materials unless the prosecuting attorney has determined that the material has evidentiary value.
- B. Rule 6(e) of the Federal Rules of Criminal Procedure imposes strict obligations upon SAs who are duly appointed agents of the grand jury to protect the secrecy of matters occurring before the grand jury. Agents who are working with grand jury materials are responsible for ensuring their confidentiality. No SA handling grand jury materials may disclose the material or their contents to any third party unless he or she is certain that the disclosure meets the applicable legal standards.

Whenever disclosure issues arise, the SA must seek clearance from the appropriate prosecuting attorney.

- C.** Because court interpretations of Rule 6(e) have made grand jury materials impossible to obtain for use in administrative actions (such as adverse personnel proceedings against employees) and very difficult to obtain in civil fraud litigation (such as false claims lawsuits), SAs are cautioned to use Inspector General subpoenas in lieu of grand jury subpoenas, and to build their cases without recourse to the grand jury whenever possible.
- D.** If the secrecy provisions of Rule 6(e) are breached, the effects can be devastating. First, Rule 6(e) provides that a knowing violation may be punished as a contempt of court. Second, breaches of grand jury secrecy may result in motions to dismiss indictments against defendants. Although these motions for the most part have been ultimately unsuccessful, they do divert the prosecutor's time and resources from the merits of the criminal case. Breaches of grand jury secrecy committed by the Office of the Inspector General (OIG) personnel can result in agency disciplinary action against the offending employee.
- E.** A Special Agent who is assisting a grand jury investigation should make certain that the Government attorney handling the case has the SA's name on the court filed grand jury access list. This list sets forth the names of all persons to whom disclosure of grand jury material has or will be made. At a minimum, the SA should also ensure that the name of his or her immediate supervisor and the Special Agent-in-Charge (SAC) is placed on the 6(e) list. Major cases may warrant adding the names of other OIG personnel.
- F.** Grand jury material should be handled in such a manner that it does not become misplaced or available to unauthorized personnel. Access must be strictly on a need-to-know basis. Files should be clearly labeled to indicate that grand jury material is included. Grand jury materials must be kept in a "limited access" investigative file. A written list of employees included on the 6(e) list allowed to access the grand jury information should be maintained on the front of this envelope.
- G.** Physical security must be strict. Only authorized personnel may have access to the area, which should be located to avoid unnecessary traffic. Cleaning services should be performed in the presence of an assigned employee. Keys to the file room should be issued only to persons authorized to enter the area. During non-duty hours, all areas where grand jury material is present should be locked and materials, to the extent practical, should be placed in locked containers.
- H.** All grand jury information will be returned to the U.S. Attorney at the termination of the investigation. If requested by the U.S. Attorney, such material may be destroyed by OIG personnel or returned to the supplier/originator.
 - 1. The ultimate method of disposal will be cleared through the U.S. Attorney.
 - 2. The SA will note in the investigative file the method used to dispose of grand jury information, and by whose authority.

EXHIBITS

- [14-1 — Evidence/Property Report \(OI-21\)](#)
- [14-2 — Description of Property Acquired \(OI-21A\)](#)
- [14-3 — Chain of Custody \(OI-21B\)](#)
- [14-4 — Inventory Form \(OI-23\)](#)
- [14-5 — Inventory Form \(Attachment\) \(OI-23A\)](#)

SOCIAL SECURITY Office of the Inspector General

SSA OIG OI EVIDENCE/PROPERTY REPORT			
DATE:	CASE NUMBER:	DATE PROPERTY ACQUIRED:	REPORT NUMBER:
SOURCE FROM WHICH PROPERTY WAS ACQUIRED:		PROPERTY WAS ACQUIRED BY:	
Property Retained At:		<input type="checkbox"/> Search Warrant <input type="checkbox"/> Incident to Arrest <input type="checkbox"/> Given Voluntarily <input type="checkbox"/> Grand Jury Action <input type="checkbox"/> Found/Abandoned <input type="checkbox"/> From Other Agency <input type="checkbox"/> Other (Specify):	

Description of Property Acquired

<i>ITEMS LISTED BELOW INCLUDE: 1. HIGH VALUE</i> <input type="checkbox"/> YES <input type="checkbox"/> NO		
ITEM NO.	DESCRIPTION	DISPOSITION CODE (SEE BELOW):
DISPOSITION CODE A) Returned to Rightful Owner B) Retained in Case File C) Retained by Court/AUSA D) Destroyed (See Below or Attached Certificate) E) Retained Pending Appeal		F) Other (Please Specify)

See attachment for additional description of property acquired.

Destruction Certification

DATE	ITEM # LISTED ABOVE	HOW DESTROYED	SA'S SIGNATURE
I Have Witnessed the Destruction of the Property Above in the Manner and on the Date Stated Above.			
DATE:	WITNESS:	DATE:	WITNESS:

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

SOCIAL SECURITY
Office of the Inspector General

Description of Property Acquired
 (ATTACHMENT)

<i>ITEMS LISTED BELOW INCLUDE: 1. HIGH VALUE</i> <input type="checkbox"/> YES <input type="checkbox"/> NO		
ITEM NO.	DESCRIPTION	DISPOSITION CODE (SEE BELOW):
A) Returned to Rightful Owner B) Retained in Case File	DISPOSITION CODE C) Retained by Court/AUSA D) Destroyed (See Below or Attached Certificate) E) Retained Pending Appeal	F) Other (Please Specify)

This report contains sensitive law enforcement material and is the property of the Social Security Administration, Office of the Inspector General (SSA OIG). It may not be copied or reproduced without written permission from the SSA OIG. This report is **FOR OFFICIAL USE ONLY**, and its disclosure to unauthorized persons is strictly prohibited and may subject the disclosing party to liability. Public availability to be determined under 5 U.S.C. §§ 552, 552a.

CRIMINAL PROCEDURE

015.000 **General**

- A.** The Office of the United States Attorney in the district in which a violation occurs is responsible for deciding the action the government will take with regard to the violator. If the attorney for the government has probable cause to believe that a person has committed a Federal offense within his/her jurisdiction, he/she should consider whether to:
1. Request or conduct further investigation;
 2. Commence prosecution;
 3. Decline prosecution and refer the matter for prosecutorial consideration in another jurisdiction;
 4. Decline prosecution and initiate or recommend pretrial diversion or other disposition; or
 5. Decline prosecution without taking other action.

As Federal investigators, OI special agents are required to coordinate criminal investigative activities relating to OIG investigations through the Office of the United States Attorney. Agents may consider alternative means of prosecution for cases that do not meet Federal prosecutorial thresholds previously established in writing, or cases in which Federal prosecution is formally declined.

- B.** A complaint, indictment, arrest, or summons is an important step in the investigation and prosecution of those who commit criminal violations involving Social Security Administration (SSA) programs or operations. In addition to purposes served by formally charging a person with the commission of a crime or taking a subject into custody, the criminal prosecution process has an impact that may deter others from committing violations.
- C.** Because of the impact such actions may have, the consequent likelihood of inquiries by Government officials and news media, and in some cases the need to notify selected management officials, the procedures shown in [Chapter 2, section 002.150](#) should be followed if an investigation is expected to draw media attention.
- D.** When communicating with prosecutors, agents must be aware that any text message or e-mail they send regarding a specific investigation is subject to discovery by defense attorneys.

Therefore, agents are encouraged to discuss cases with prosecutors via telephone or in person instead of by text message or e-mail.

015.010 Entrapment

- A.** Entrapment is a legal defense raised by the defendant when he claims that, but for the inducement of Government agents, he would not have committed the crime with which he has been charged. This defense is most apt to be raised in situations involving informants and agents working undercover.

- B.** Government agents may afford the defendant the opportunity to commit a crime. This in and of itself does not constitute entrapment. Agents may devise a scheme to reveal criminal activity without entrapping a defendant. It is only when the criminal design originates with a Government agent, who induces an otherwise innocent person to become involved, that entrapment arises.

- C.** The term “Government Agent” includes not only Government employees, agents, and investigators, but also Government informants as well. A Special Agent (SA) cannot do, through an informant, what the SA cannot lawfully do himself. If an informant for an agency induces an otherwise innocent person to commit a crime, the defense of entrapment will be valid.

- D.** The courts have placed few limitations on the roles that agents and informants can play in the crime itself. The fact that an informant had provided the contraband in a narcotics sale has been held by the United States Supreme Court not to constitute entrapment, where the defendant was already predisposed to commit the crime.

- E.** The United States Supreme Court has clearly established the predisposition of the defendant as the focal point in determining whether there has been entrapment. If the defendant was predisposed (meaning that the criminal intent was already in his/her mind and was not placed there by the Government agent) to commit the crime, entrapment will not be a viable defense.

- F.** Even though entrapment is not a defense when predisposition is present, the court may find a violation of due process where the Government’s conduct, through the actions of the SA, was outrageous and shocking to the conscience of the court.

- G.** Any questions concerning entrapment should be directed to the United States Attorney’s Office or to the Office of the Counsel to the Inspector General at Headquarters.

015.020 Arrest Warrants – General

- A.** The complaint is a written statement of the essential facts constituting the offense(s) charged. It is prepared by a complainant, who has to swear to the truth of its contents while under oath before a magistrate. ([*Exhibit 15-1*](#))

- B.** The complaint form contains:
1. Name of the defendant (if name unknown, a complete description by which the defendant can be identified with reasonable certainty).
 2. Statutory language of the offense charged.
 3. Facts of complainant's charge (a brief synopsis of the investigation explaining how the facts of the case became known to the agent. An affidavit may be used if the synopsis is lengthy).
- C.** In order to obtain an arrest warrant, SAs must prepare a complaint and provide it for review, if possible, to the appropriate Assistant United States Attorney (AUSA). The complaint is then filed before a United States magistrate judge who reviews it and determines whether probable cause has been established.
- D.** If it appears from the complaint that there is probable cause to believe that an offense has been committed and that the defendant committed it, a warrant for the arrest of the defendant will be issued to any officer authorized by law to execute it. ([Exhibit 15-2](#)) In instances where the Office of Investigations (OI) SA has executed a warrantless arrest, the complaint must be filed before the magistrate judge after the arrest.

015.030 **Indictment and Information**

- A.** Appearance before a grand jury – obtaining an indictment
1. Federal grand juries are composed of 16 to 23 jurors who serve an appointed term not to exceed 18 months.
 2. Under existing rules, the only persons permitted to be present during grand jury proceedings are attorneys for the Government, the witness under examination, interpreters when needed, and a stenographer or operator of a recording device. No person other than the jurors may be present when the grand jury is deliberating or voting.
 3. When preparing to appear before a grand jury, SAs should discuss proposed questions and expected testimony with the AUSA handling the matter. Witnesses giving testimony are sworn before the grand jury. Hearsay evidence is permitted before a grand jury, and SAs may be called upon to display selected items of evidence.
 4. An indictment is a formal written accusation charging a person(s) with the commission of a crime. It is presented by a grand jury to the court after the examination of the evidence reveals that there is a probable cause to believe the defendant has committed the offense charged. A grand jury may return an indictment upon concurrence of 12 or more jurors.
 5. The Federal magistrate judge to whom an indictment is returned may direct that the indictment be kept secret until the defendant is in custody or has been released pending trial. Upon indictment, an arrest warrant or summons is issued. In some Federal districts, the

Clerk of the United States District Court will issue the arrest warrant or summons after an indictment has been returned. The local United States Attorney should be contacted for direction in this matter.

B. Prosecution by information

1. Any offense punishable by death or imprisonment for a term exceeding 1 year shall be prosecuted by indictment.
2. Any other offense may be prosecuted by information.
3. The information is a plain, concise, and definite statement of the essential facts constituting the offense charged. The attorney for the Government signs the information.
4. The court may direct the filing of a bill of particulars in matters prosecuted in this manner. The counsel for the defense may also make a motion for a bill of particulars.
5. Decisions regarding the use of this technique of prosecution are within the purview of the United States Attorney in each district. Further details concerning prosecution by information are found in Rule 7, Federal Rules of Criminal Procedure.

015.040 Arrest Warrants – Execution

- A.** An arrest warrant is executed with the arrest of the defendant. The warrant may be executed any place within the jurisdiction of the United States by a United States Marshal or any other officer authorized by law.
1. Prior to enactment of section 812 of the Homeland Security Act of 2002 (Pub. L. No. 107-296), the Inspector General Act did not provide arrest or search warrant authorities for investigators of those offices.
 2. Arrest warrants for defendants who are outside of the geographical boundaries of the Case Agent will be forwarded to the field division (FD) where the defendant currently resides for that FD to execute.
- B.** The SA is not required to have the warrant in hand when making the arrest, but the defendant must be advised that a warrant has been issued and the offense(s) charged. The SA must also read the contents of the warrant to the defendant as soon as practical after the physical arrest and show the defendant, upon request, a copy of the warrant.
- C.** The agent executing the warrant shall bring the defendant (along with a copy of the warrant) before the nearest Federal magistrate judge, or State or local judicial officer if a magistrate judge is unavailable.
- D.** Unexecuted warrants are returned and cancelled by the magistrate judge or, at the request of the United States Attorney, may be given by the magistrate to the United States Marshal for execution.

015.050 Obtaining a Summons

- A. A summons orders the defendant to appear before a United States magistrate judge at a stated time and place. To obtain a summons, the agent should use the same procedures and forms used in obtaining an arrest warrant.
- B. The summons is served by personally delivering a copy to the defendant or by leaving it at the defendant's dwelling or place of employment with a person of suitable age or discretion. An agent may also mail a copy of the summons to the defendant's last known address.
- C. If the defendant fails to appear in response to the summons, an arrest warrant shall be issued.

015.060 Arrests Without a Warrant

- A. The SSA Office of the Inspector General (OIG) OI policy is that arrests will not be executed without an arrest warrant unless extraordinary circumstances exist. However, agents may make an arrest without a warrant while engaged in official duties as authorized under the Inspector General Act or other statute, or as expressly authorized by the Attorney General, for any offense against the United States committed in the presence of such individual, or for any felony cognizable under the laws of the United States if such individual has reasonable grounds to believe that the person to be arrested has committed or is committing such felony.
- B. When making an arrest without a warrant, the arrestee must be taken without unnecessary delay before the nearest Federal magistrate judge, or if none is available, before a State or local judicial officer (as authorized and defined by [18 U.S.C. § 3041](#)). At that time, a complaint has to be filed with the magistrate judge. If time allows, the complaint should be reviewed by the appropriate AUSA prior to presentation.
- C. If the magistrate judge or other local judicial officer determines that probable cause exists, then the magistrate judge will instruct the defendant that probable cause has been established and proceed with other judicial requirements. If probable cause is not found, the defendant will be released.

015.070 Initial Appearance

- A. During the initial appearance before a United States magistrate judge, defendants are:
 - 1. Not called upon to plead.
 - 2. Informed of the complaint against them.
 - 3. Informed of their right to counsel or their right to request assignment of counsel.

4. Advised that they are not required to make any statement and that any statement they make can be used against them.
 5. Advised of their right to a preliminary hearing.
 6. Given reasonable time to consult counsel.
 7. Admitted to bail.
- B.** A defendant who waives preliminary examination is held to answer in the district court. If the defendant does not waive preliminary examination, a date is set for one during the initial appearance before the magistrate judge.

015.080 Preliminary Hearing

- A.** The preliminary examination is a probable cause hearing. The United States magistrate judge shall hold the defendant to answer in the district court if, from the evidence, it appears there is probable cause to believe:
1. An offense has been committed and
 2. The defendant committed the offense.
- B.** Hearsay evidence may be used in whole or in part, and defendants may cross-examine witnesses against them.
- C.** If no probable cause is found to believe that an offense has been committed and that the defendant has committed the offense, the magistrate shall dismiss the complaint and discharge the defendant.
- D.** Even though the defendant does not waive it, many times the preliminary examination will never materialize. After the initial appearance before the magistrate judge, the case may be presented directly to the Federal grand jury. An indictment by the grand jury satisfies the Government's obligation to establish probable cause.

015.090 The Arraignment

- A.** Arraignments are conducted in open court and consist of reading the indictment or information to the defendant, or stating to him the substance of the charge and calling on the defendant to enter a plea to the charges.
- B.** The defendant is given a copy of the indictment or information before being called upon to plead.
- C.** The court does not accept guilty or nolo contendere pleas without addressing the defendant personally and determining that the plea was made voluntarily, and that the defendant understands the nature of the charge and consequences of the plea.

- D. If the defendant pleads guilty and the court accepts the defendant's plea, the court then sets a sentencing date and orders the Probation Office to conduct a pre-sentencing investigation.

015.100 Transfer from the District for Plea and Sentencing (Rules of Criminal Procedure – Rule 20)

- A. When there is an indictment or information pending, a defendant arrested or held in a district other than that in which the indictment or information is pending may state in writing that he or she wishes to plead guilty or nolo contendere.
- B. This allows a defendant to waive trial in the district in which the indictment or information is pending and to consent to disposition of the case in the district in which the defendant was arrested or is held. However, this approach is subject to the approval of the United States Attorney in each district.
- C. Upon receipt of the defendant's statement and approval of the United States Attorney, the clerk of the court in which the indictment or information is pending transmits the papers in the proceeding to the district in which the defendant is held, and prosecution continues in that district.
- D. Once the proceeding is transferred, if the defendant changes his or her plea to not guilty, all papers are returned to the court where prosecution was commenced, and the proceedings are restored to the docket of that court. The defendant's original guilty or nolo contendere plea may not be used against him or her.

015.110 Removals (Rules of Criminal Procedure – Rule 40)

- A. The purpose of a removal proceeding is to accord safeguards to a defendant against an improvident removal to a distant point for trial.
- B. In the case of defendants arrested who are the subject of a complaint and warrant but have not yet been indicted for the offense, the magistrate judge will require the following:
 - 1. A certified copy of the complaint and warrant and
 - 2. Evidence to demonstrate that there is "reasonable cause" to believe that the defendant is guilty of the charge.
- C. In the case of defendants arrested who have been indicted, the United States magistrate judge will require the following:
 - 1. A certified copy of the indictment and
 - 2. Evidence to demonstrate that the person apprehended is, in fact, the person named in the indictment.

- D.** In those cases where fugitives are being sought and it is possible that the fugitive is in another judicial district, the SA should prepare for removal proceedings. In these cases, the SA should, in advance of its need:
1. Secure a certified copy of the complaint or indictment and
 2. Secure a set of the fugitive's fingerprints and/or fingerprint classifications, as well as a recent photograph of the fugitive.

015.120 Declinations of Prosecution

- A.** The IG Act requires the reporting of substantiated violations of Federal criminal law to the Office of the United States Attorney. If the United States Attorney declines prosecution, the case file **must** address how Federal prosecution was declined, either by formal declination by an approved representative from the Office of the United States Attorney (see section B) or by blanket declination (see section C).
- B.** Investigations in which a member of the Office of the United States Attorney provides verbal or written declination of prosecution (including blanket declinations) require the case agent to memorialize the declination and reason for the declination in an [OI-4 Report of Investigation](#). The name of the AUSA giving the declination and the date the prosecution was declined must appear in the report.
- C.** Blanket Declinations
1. In some jurisdictions, the United States Attorney or his/her designee may prefer to exercise prosecutorial discretion by issuing "blanket declinations" in certain types of cases.
 2. Should the United States Attorney or his/her designee issue a written blanket declination, a copy of the blanket declination shall be placed in the case file.
 3. Some U.S. Attorneys may not issue written blanket declinations. In those instances, the field division SAC or his/her designee shall meet with the U.S. Attorney or his/her designee to discuss prosecutorial thresholds. Following the meeting, the SAC or his/her designee shall prepare a memorandum to the U.S. Attorney or his/her designee to memorialize the types of violations or fraud loss levels that will not be approved for prosecution in the district, absent exacerbating circumstances. The memorandum should also include whether or not the U.S. Attorney requested to receive a notification from OI whenever a violation of Federal law is substantiated, along with the frequency of these notifications (e. g. each event, monthly, quarterly, yearly, etc.). These memoranda must be updated whenever there is a change in U.S. Attorneys or when the U.S. Attorney announces changes in his or her policy. A copy of the memorandum shall be placed in the case file, when applicable. Additionally, the reason for the declination must also be articulated in an OI-4, Report of Investigation.

015.130 Pretrial Diversion

- A.** The United States Attorneys use pretrial diversion as an alternative to prosecution in certain situations favorable to the Government. The pretrial diversion program is an alternative to prosecution which seeks to divert certain offenders from traditional criminal justice processing into a program of supervision and services administered by the United States Probation Service or any other appropriate community agency providing such services.
- B. Principles of Operation**
1. Pretrial diversion is an exercise of prosecutorial discretion according to standardized guidelines. The plan attempts to identify offenders most suitable to rehabilitation and focus rehabilitation efforts on such offenders early in the criminal justice process, generally prior to indictment.
 2. The exercise of prosecutorial discretion centers on determining which offenders have not adopted a criminal life pattern and should be diverted out of the system. If program participation is successful, charges are dismissed and no criminal record is permanently established; if unsuccessful, prosecution is resumed.
 3. In order to consider a case for diversion, prosecutors must ascertain that the case is one they could successfully prosecute. In addition, defendants must have the benefit of counsel during the diversion decision-making process. The diversion is finalized by a written contract agreed to by prosecution, defendant, and defendant's counsel.
- C. Eligibility Criteria**
1. The United States Attorney may divert any individual against whom a prosecutable case exists and who is not:
 - a. Accused of an offense which, under existing guidelines, should be diverted to the State for prosecution.
 - b. A person with two or more prior felony convictions.
 - c. A drug addict.
 - d. A public official or former public official accused of an offense arising out of an alleged violation of public trust.
 - e. Accused of an offense related to national security or foreign affairs.
 - f. Accused of an offense in which the money involved is above monetary guidelines established as a threshold for prosecution in the judicial district.
- D. Services**
1. Upon determining eligibility of a defendant for pretrial diversion, United States Attorneys should refer the case to the United States Probation Service (or other supervision

organization as they deem appropriate) for a recommendation on potential suitability of the defendant.

2. As part of the background investigation, the Probation Service should request notification of any prior record from the Federal Bureau of Investigation Identification Division when the defendant's fingerprints are submitted.
3. Services should be tailored to the defendant's needs and include employment, counseling, education, job training, psychiatric care, etc.
4. Many districts have successfully required restitution or forms of community service as part of the rehabilitation program. Innovative approaches are strongly encouraged.
5. The Pretrial Diversion Agreement outlines the recommended program of supervision and services agreed upon by all parties and administered by the Probation Service or other community agency, which will report quarterly to the United States Attorney regarding the individual's progress.

E. Termination

1. The United States Attorney will formally decline prosecution upon satisfactory termination of program requirements.
2. The Probation Service or supervising agency will provide notice of satisfactory completion to the United States Attorney.
3. If the divertee breaches conditions of the agreement, the Probation Service will so inform the United States Attorney, who will initiate prosecution.
4. When prosecution is resumed, the United States Attorney must furnish the defendant with notice.
5. The decision to terminate an individual for breach of conditions rests exclusively with the United States Attorney.

015.140 Policy Regarding the Disclosure to Federal Prosecutors of Potential Impeachment Information Concerning SSA Office of the Inspector General Employees Who are Affiants and/or Witnesses in Federal Criminal Cases (Giglio Policy)

A. Introduction

1. **Intent of Policy.** The following policy ("Giglio Policy")¹ is established for the Social Security Administration, Office of the Inspector General (SSA/OIG), pursuant to the

¹ While this Giglio Policy applies only to criminal investigations or cases, SSA/OIG employees have a duty to provide this same information to the USAO and DOJ in civil investigations or cases. In addition to the obligation that

Attorney General's December 9, 1996, memorandum, "Policy Regarding the Disclosure to Prosecutors of Potential Impeachment Information Concerning Law Enforcement Agency Witnesses," and the Attorney General's October 19, 2006 amendment to this policy to conform to the Department of Justice's (DOJ) policy regarding the disclosure of exculpatory and impeachment information.² (copy of amended Giglio Policy attached)

This Giglio Policy addresses the disclosure of potential impeachment information regarding SSA/OIG employees who are affiants or witnesses in a criminal investigation or case to the United States Attorneys' Offices (USAO) and the DOJ criminal litigating sections. This policy is intended to ensure that prosecutors in a federal criminal proceeding receive sufficient information to meet their obligations under *Giglio v. United States*, 405 U.S. 150 (1972), while protecting the legitimate privacy rights of SSA/OIG employees. However, as noted by DOJ, "this policy is not intended to create or confer any rights, privileges, or benefits to prospective or actual witnesses or defendants. It is also not intended to have the force of law. *United States v. Caceres*, 440 U.S. 741 (1979)." See United States Attorney's Manual (USAM), § 9-5.100, Preface.

- 2. Background.** This Giglio Policy is the result of a series of Federal court decisions. In *Brady v. Maryland*, 373 U.S. 83 (1963), the Supreme Court held that the failure of the prosecution to turn over evidence favorable to the defendant upon request on the issue of guilt violates due process "irrespective of the good faith or bad faith of the prosecution." Subsequently, in *Giglio v. United States*, 405 U.S. 150 (1972), the Court held that information known by one Federal prosecutor, including any impeachment information, is deemed known by all Federal prosecutors in the same office. In applying this law, the Ninth Circuit, in *United States v. Henthorn*, 931 F.2d 29 (9th Cir. 1991), held that Federal prosecutors have an obligation to review the personnel file of testifying government employees when requested to do so by defense counsel. The prosecutor must also disclose any information favorable to the defendant that meets the appropriate standard of materiality. In response to the series of aforementioned Federal court decisions, DOJ promulgated a policy that (upon a request from DOJ) requires Federal agencies to review the personnel files of employees who are to be affiants or witnesses and report such findings to Federal prosecutors. This DOJ policy has been favorably reviewed in *United States v. Quinn*,

an Assistant United States Attorney has to provide such information to the Court in a civil case pursuant to Rule 11 of the Federal Rules of Civil Procedure, it is important to remember that what begins as a civil investigation or case may end up as a criminal investigation or case.

² In addition to the impeachment information that must be provided pursuant to Giglio, a prosecutor must also disclose impeachment information that "either casts a substantial doubt upon the accuracy of any evidence—including but not limited to witness testimony—the prosecutor intends to rely on to prove an element of any crime charged, or might have a significant bearing on the admissibility of prosecution evidence. This information must be disclosed regardless of whether it is likely to make the difference between conviction and acquittal of the defendant for a charged crime." See USAM 9-5.001C.2.

123 F.3d 1415 (11th Cir. 1997); *United States v. Herring*, 83 F.3d 1120 (9th Cir. 1996); and, *United States v. Jennings*, 960 F.2d 1488 (9th Cir. 1992).

3. **Obligation of SSA/OIG Employees to Provide Potential Impeachment Information to Federal Prosecutor.** This policy does not replace the obligation of all SSA/OIG employees to inform prosecuting attorneys with whom they work of potential impeachment information prior to providing a sworn statement or testimony in any criminal investigation or case. This obligation arises when a Federal prosecutor has identified an SSA/OIG employee as a potential affiant or witness in a specific criminal investigation or case and continues until the investigation or case has been concluded, regardless of whether the prosecutor has made a specific request for such information. Examples of "Potential Impeachment Information" are provided in paragraph 7 below. All SSA/OIG employees should familiarize themselves with the examples. However, this list is not all-inclusive.

4. **Initiation of Giglio Request by Federal Prosecutor.** In the majority of criminal investigations and cases in which SSA/OIG employees may be affiants or witnesses, it is expected that the Federal prosecutor will be able to obtain all potential impeachment information directly from SSA/OIG employee witnesses during the normal course of investigations and/or preparation for hearings or trials. However, because the Federal prosecutor has a duty to learn of potential impeachment information³, pursuant to the Attorney General's December 9, 1996 memorandum, as amended, a Federal prosecutor may also choose to request potential impeachment information directly from SSA/OIG. When this occurs, the following Giglio Policy sets forth the procedures to be followed.

B. Definitions

1. **Requesting Official.** A senior official in each USAO and DOJ prosecuting office will be designated as the Requesting Official for that office. The Requesting Official serves as the contact point for the USAO and DOJ criminal litigating office seeking impeachment information. In addition, it is the responsibility of the Requesting Official to inform the SSA/OIG CIG and Contact Official (as defined in paragraph 6, below) of relevant case law, court practices, and rulings that govern the definition and disclosure of impeachment information in that district.

2. **SSA/OIG Contact Officials.** The SSA/OIG person responsible for the review of SSA/OIG employee personnel files and administrative files will be the CIG or the CIG's designee. The "Contact Officials" listed below will assist the CIG in this

³ The Supreme Court reaffirmed the responsibility of prosecutors to locate material exculpatory to the defense. *See Kyles v. Whitley*, 514 U.S. 419 (1995) (noting that an individual prosecutor has a duty to learn of any favorable evidence known to others acting on the government's behalf in the case, including the police). In January 2010, DOJ issued a Memorandum to Federal Prosecutors entitled "Guidance for Prosecutors Regarding Criminal Discovery." It expands the responsibility of Federal Prosecutors to search for potential exculpatory evidences. *See* Department of Justice, *United States Attorney's Manual, Criminal Resource Manual* 165.

review. Their duties include being the point of contact in their region for the Requesting Official, forwarding any requests to the CIG, and providing information necessary to respond to the Giglio requests for SSA/OIG employees under their supervision.

<u>Office</u>	<u>Contact Official</u>
Headquarters Office of Investigations	DAIGI
Headquarters Office of Audit	DAIGA
Office of Communications and Resource Management	DAIGOCRM
Office of External Relations	DAIGER
Counsel to the Inspector General	DCIG
Office of Investigations Divisions	SAC
Office of Audit Divisions	Director

3. **Potential Impeachment Information.** Potential impeachment information is generally defined as impeaching information that is material to the defense and includes information that provides evidence of perjurious conduct, acts of dishonesty, or otherwise exculpatory information. The Attorney General's December 9, 1996 memorandum, as amended, provides the following list as examples of potential impeachment information that must be disclosed. This list reflects the minimum amount of information required to be disclosed and should not be considered all-inclusive.
- a) **Substantiated allegations** - any finding of misconduct demonstrating bias or lack of candor or truthfulness;
 - b) **Pending investigations or allegations** - any credible allegation of misconduct that reflects upon the truthfulness or possible bias of the SSA/OIG employee that is the subject of a pending investigation;
 - c) **Criminal charges** – any past or pending criminal charge against the SSA/OIG employee;
 - d) **Allegations that are unsubstantiated, not credible, or have resulted in exoneration** - generally, unsubstantiated allegations, allegations that are not credible, or allegations that result in the exoneration of an SSA/OIG employee are not disclosed. However, when those allegations can be said to go to the truthfulness of the SSA/OIG employee, they are required to be disclosed under the following circumstances:
 - 1) when the Requesting Official advises the CIG that disclosure is required by a court decision in the district where the investigation or case is being pursued;

- 2) when, on or after the effective date of this policy,
 - (i) the allegation was made by a federal prosecutor, magistrate judge; or,
 - (ii) the allegation received publicity;
- 3) when the Requesting Official and the CIG agree that such disclosure is appropriate, based upon exceptional circumstances involving the nature of the case or the role of the SSA/OIG witness; or
- 4) when disclosure is otherwise deemed appropriate by SSA/OIG.

C. **SSA/OIG Procedure for Review and Disclosure**

1. **Request for SSA/OIG Giglio Information by Requesting Official**. Once a Federal prosecutor determines to request all potential impeachment information from SSA/OIG, the prosecutor should direct the request to the Requesting Official in the prosecutor's office. In turn, the Requesting Official should request from SSA/OIG, in writing, all potential impeachment information regarding a specific SSA/OIG employee. The Requesting Official should direct the request to either the appropriate SSA/OIG Contact Official or the CIG. Upon receipt of a request from the Requesting Official, the SSA/OIG Contact Official should forward the request to the CIG.
2. **SSA/OIG Procedure Upon Receipt of Request for Giglio Information**. Upon receipt of a request for potential impeachment information from a Requesting Official, the CIG is responsible for obtaining the SSA/OIG employee's Official Personnel File and other relevant administrative files for review. The Contact Official is responsible for reviewing any relevant files within his or her control and forwarding their findings to the CIG. After the review has been completed, the CIG shall notify the Requesting Official, in writing, of any potential impeachment information located in the SSA/OIG employee's Official Personnel File or other relevant administrative file. The CIG shall transmit a copy of the response to the Assistant Inspector General and Contact Official with supervisory authority over the SSA/OIG employee.
3. **Potential Impeachment Information Based Upon Allegations that are Unsubstantiated, Not Credible, or Have Resulted in Exoneration**. If the potential impeachment information forwarded to the Requesting Official is based upon "allegations that are unsubstantiated, not credible, or have resulted in exoneration," the CIG shall also advise the Requesting Official, to the extent determined, whether any of the allegations were found to be unsubstantiated, not credible, or resulted in the SSA/OIG employee's exoneration. In addition, the CIG shall stress, with regard to any allegations disclosed, the importance of maintaining the confidentiality of the report and the privacy interests of the SSA/OIG employee-witness to whom the report refers.

4. **SSA/OIG Request Not to Disclose Potential Impeachment Information.** If the SSA/OIG believes that the Federal prosecutor should not disclose certain potential impeachment information to defense counsel, the CIG should communicate this view, along with the reasons, to the Requesting Official, so that the Federal prosecutor will be aware of all relevant issues prior to determining whether to disclose the potential impeachment information.
5. **Retention by USAO and DOJ of Information Provided by SSA/OIG.** In order to ensure that special care is taken to protect the confidentiality of privacy interests and reputations of SSA/OIG employee-witnesses, at the close of the criminal investigation or case, the Contact Official shall request that all information and documentation that was not disclosed to the defense counsel be expeditiously returned to SSA/OIG.⁴
6. **Continual Duty to Disclose Potential Impeachment Information During the Pendency of the Criminal Case.** During the pendency of the criminal investigation or case, the CIG and SSA/OIG employee who is the subject of the Giglio request each have a duty to immediately inform the Requesting Official of potential impeachment information that arises after an initial request for such information. Therefore, Contact Officials shall immediately inform the CIG of any such potential impeachment information regarding SSA/OIG employees under their supervision during the pendency of the criminal investigation or case.
7. **Retention by SSA/OIG of Potential Impeachment Information Provided to USAO or DOJ.** The CIG shall retain a copy of all potential impeachment information provided to a Requesting Official, whether or not the information is disclosed to defense counsel. This information, along with copies of all correspondence, memoranda, and any relevant court pleadings and rulings shall be maintained in a secure location, accessible only by the CIG, the SSA/OIG employee affiant or witness who is the subject of the information, and supervisory officials with an official need to know. The information shall be stored so that it is readily accessible, as necessary.
8. **Removal of SSA/OIG Employee's Records Upon Transfer, Reassignment, or Retirement.** The CIG or Contact Official shall inform the Requesting Official of the SSA/OIG employee's retirement, transfer to an office in another judicial district, or reassignment to a position in which the SSA/OIG employee will neither be an affiant nor witness and request that all records previously forwarded that are accessed by the identity of the SSA/OIG employee be returned to SSA/OIG. Upon such notification and subsequent to the resolution of any litigation pending in the Federal prosecuting office in which the SSA/OIG employee could be an affiant or witness, the Requesting Official shall remove from the Federal prosecuting office's system of records any record that can be accessed by the identity of the SSA/OIG employee.

⁴ The Attorney General's December 9, 1996 memorandum, as amended, does not prohibit the USAO or DOJ prosecuting offices from keeping motions, responses, legal memoranda, court orders, and internal office memoranda or correspondence, in the relevant criminal case file.

9. **Destruction of Potential Impeachment Information Records.** The CIG shall destroy its records of all potential impeachment information that it has maintained pursuant to paragraph 14 no earlier than five (5) years after the retirement or severance of the employee from the SSA/OIG. However, the CIG will not destroy any records it has maintained on the SSA/OIG employee pursuant to this Giglio Policy due to the transfer or reassignment of the employee within the SSA/OIG.

10. **Implementation of the Giglio Policy.** This Giglio Policy should be disseminated to all SSA/OIG employees and incorporated into future training. SSA/OIG employees should address questions concerning the obligation to disclose potential impeachment information to prosecutors to the applicable Contact Official or the CIG.

Chapter 15 —

EXHIBITS

[15-1 — Criminal Complaint](#)

[15-2 — Arrest Warrant](#)

Reserved for Copy of Criminal Complaint

Note: Field Divisions can insert a copy of one or more criminal complaints relating to closed investigations in their judicial district(s).

UNITED STATES DISTRICT COURT

UNITED STATES OF AMERICA,

v.

WARRANT FOR ARREST

C.

CASE NUMBER:

To: The United States Marshal
and any Authorized United States Officer

YOU ARE HEREBY COMMANDED TO ARREST _____
Name

and bring him or her forthwith to the nearest magistrate to answer a(n)

___ Indictment ___ Information ___ Complaint ___ Order of court ___ Violation Notice ___ Probation Violation Petition
charging him or her with (brief description of offense)

in violation of Title _____ United States Code, Section(s) _____

Name of Issuing Officer

United States Magistrate Judge
Title of Issuing Officer

Signature of Issuing Officer

Date and Location

(By) Deputy Clerk

Bail Fixed at \$ _____

by _____
Name of Judicial Officer

RETURN		
This warrant was received and executed with the arrest of the above-named defendant at _____		
DATE RECEIVED	NAME AND TITLE OF ARRESTING OFFICER	SIGNATURE OF ARRESTING OFFICER
DATE OF ARREST		

INFORMATION ONLY:

THE FOLLOWING IS FURNISHED FOR

DEFENDANT'S NAME: _____

ALIAS: _____

LAST KNOWN RESIDENCE: _____

LAST KNOWN EMPLOYMENT: _____

PLACE OF BIRTH: _____

DATE OF BIRTH: _____

SOCIAL SECURITY NUMBER: _____

HEIGHT: _____ WEIGHT: _____

SEX: _____ RACE: _____

HAIR: _____ EYES: _____

SCARS, TATTOOS, OTHER DISTINGUISHING MARKS: _____

FBI NUMBER: _____

COMPLETE DESCRIPTION OF AUTO: _____

INVESTIGATIVE AGENCY AND ADDRESS: _____

CIVIL MONETARY PENALTIES and ADMINISTRATIVE SANCTIONS

016.000 Section 1129 – False Statements and Representations

- A.** Under Section 1129 of the Social Security Act (Act), and pursuant to delegations signed by the Commissioner and Inspector General of Social Security, the Office of Counsel to the Inspector General (OCIG) may impose civil monetary penalties against certain persons who make (or cause to be made) false statements or omissions of material facts to SSA.
1. “Persons” who may be liable include individuals, corporations, organizations, or other entities.
 2. “Material facts” include facts that the Social Security Administration (SSA) **may** consider in evaluating initial or continuing:
 - entitlement to benefits under title II; or
 - eligibility for benefits or payments under title XVI.
 3. Liability standard:
 - a. knows or should know the statement is false (or false due to an omission of material fact from a document) or
 - b. makes the statement with knowing disregard for the truth.
 4. This section also applies to attempted fraud; i.e., material false statements and omissions in benefit applications that are ultimately denied. (A civil monetary penalty (CMP) may be imposed even if no overpayment results.)
- B.** Penalties and Assessments under Section 1129.
1. Up to \$5,000 for each false statement or representation.
 2. An assessment of not more than twice the amount of benefits or payments paid as a result of such false statement or representation.
 3. Factors in determining the amount of penalties or assessments include the:

- a. nature and circumstances of the statements and representations;
 - b. degree of culpability;
 - c. prior history of offenses in connection with the Social Security programs; and
 - d. financial condition of the person.
- 4. A CMP may be imposed in addition to other penalties prescribed by law, such as criminal prosecution.
 - 5. A CMP may be imposed even if the subject has repaid, or agreed to repay, the overpayment that resulted from the false statement(s) or omission(s).

016.010 Procedural Requirements Under Section 1129

- A. The Office of the Inspector General (OIG) must initiate a CMP proceeding within six years of the date of the violation.
- B. Civil and criminal declinations from the appropriate United States Attorney's Office (USAO) must be obtained before a CMP action can be initiated.
- C. Prior written notice of the OIG's intent to take CMP action is required to be given to the subject. If a subject does not request a hearing within 60 days, a CMP may be imposed without further right of appeal.

016.020 Hearings and Appeals

- A. A person may request a hearing before an Administrative Law Judge (ALJ) to contest the penalty or assessment in cases under Section 1129.
- B. A decision of the ALJ may be appealed. SSA has retained the Departmental Appeals Board (DAB) at the Department of Health and Human Services to conduct hearings and issue recommended decisions in CMP cases. Final decisions of the DAB may be appealed to the Commissioner, and then to the appropriate Federal Circuit Court of Appeals.

016.030 Collectability

- A. The subject's financial condition and ability to pay are considerations in developing a CMP case. If financial information has been obtained during an investigation, it should be included in the CMP investigative referral.

016.040 Injunctions and Testimonial Subpoenas

- A. The Inspector General (IG) has been delegated the authority under Section 1129 to request an appropriate district court to enjoin (1) any activity which makes a person subject to Section 1129 or (2) a person from concealing, removing, encumbering, or disposing of assets which may be required in order to pay any penalty or assessment.
- B. If it appears that a target is about to destroy or hide assets, it is important to notify the OCIG immediately.
- C. The IG has also been delegated the authority under Section 1129 to issue testimonial subpoenas in Section 1129 CMP cases.

016.050 Civil Monetary Penalty Investigative Referrals

- A. Any investigation of a program violation may be considered for CMP action (see [Exhibit 16-1, Civil Monetary Penalty Authorities under Section 1129](#)); the evidentiary record developed for presentation of a case to a United States Attorney will generally be sufficient for CMP consideration, with emphasis on the following:
 - 1. A false statement(s) or representation(s) made within the past six (6) years.
 - 2. The false statement(s) or representation(s) must involve a “material fact” that SSA may consider in its determination to award (or continue) benefits or to calculate benefit amounts under titles II and XVI.
 - 3. The false statement(s) or representation(s) must be one which the person knew or should have known was false, or was made with knowing disregard for the truth.
- B. An automated process is used to refer cases to OCIG for consideration for a CMP, and is as follows:
 - 1. Before an agent can close a case, he/she is required to complete a brief CMP checklist in NICMS. The responses to the checklist will result in one of two actions:
 - a. The case will be closed and referred for CMP; or
 - b. The case will be closed (when the case does not meet the CMP requirements).
 - 2. The agent will be notified of the case status automatically upon completion of the checklist.

016.060 Civil Monetary Penalty Reports of Investigation

- A. If OCIG requests, at the conclusion of the screening conversation, that the case be referred, a Report of Investigation (ROI) outlining the facts of the case should be prepared by the case agent and forwarded through the Special Agent-in-Charge (SAC) to OCIG. The ROI must address the following issues:
 - 1. Dates of the violations.

2. Number of violations (false statements or representations).
 2. Amount of any overpayments resulting from the violations.
 3. Status of any overpayments resulting from the violations.
 4. A description of each element of evidence, including witness interviews, subject interviews, and documentary evidence.
 5. Information concerning the subject's ability to pay (optional).
 6. Date of the criminal and civil declinations.
 7. Whether the beneficiary or recipient has a representative payee.
- B.** The ROI should also contain the following as attachments:
1. SSA's calculation of the overpayment.
 2. Witness/subject concerns.
 3. Any other relevant documents.
- C.** NICMS entries should reflect both criminal and civil declinations and referral of the CMP case.
1. The SAC should ensure a CMP case number has been entered into NICMS (see Chapter 3 for NICMS case numbering guidelines).

016.070 Post-Referral Activities

- A.** OCIG will conduct all negotiations of settlements and litigation of CMP cases and will periodically provide a status on CMP cases to OI.
- B.** OI agents and staff may be needed to perform certain duties or provide assistance to OCIG, including participation as witnesses during the course of litigation of CMP cases, or obtaining personal service when certified mail is refused by the subject.
- B.** OCIG shall notify the referring FD, in writing, of its declination of a CMP case that OCIG requested be referred within 20 days from receipt.
- C.** If OCIG declines a case after requesting that it be referred, then, if appropriate under the provisions of *Administrative Sanctions*, the FD shall forward the results of the investigation to the SSA Regional Security Office within 10 days of receipt from OCIG for any administrative action deemed appropriate.

016.080 Collections

- A. General: Collection of any final penalty will be the responsibility of the agency.
- B. The Commissioner or his/her designee may compromise the penalty and may bring a civil action in Federal district court to collect a penalty or assessment imposed under Section 1129.
- C. Penalties imposed under Section 1129 may be deducted from:
 - 1. Monthly title II or title XVI payments payable to the subject.
 - 2. A tax refund to which the subject is entitled after notice to the Secretary of the Treasury.
 - 3. Any sum then or later owed by the United States to the subject.
 - 4. As permitted by authority provided under the Debt Collection Act of 1982, as amended, to the extent applicable to debts arising under the Act.
 - 5. Any combination of the foregoing.

016.090 Section 1129A – Title XI of the Social Security Act – Administrative Sanctions

- A. *Administrative Sanctions* (imposed by SSA, not OIG): Section 1129A of the Social Security Act provides for the imposition of a penalty when an individual makes, or causes to be made, a statement or representation of a material fact for use in determining Title II or Title XVI benefit eligibility or amounts, which the person knows or should know is false or misleading or omits a material fact, or that the person makes with a knowing disregard for the truth. Under the statutory effective date, *administrative sanctions* may apply to any false or misleading statement or misrepresentation of a material fact made on or after December 14, 1999.
 - a. Fraudulent Social Security number applications or SS-5s are not a part of the administrative sanction process.
- B. The penalty is nonpayment of benefits under title II that would otherwise be payable to that person and ineligibility for cash benefits under title XVI. The duration of penalties is 6 months for the first occurrence, 12 months for the second occurrence, and 24 months for each subsequent occurrence.
- C. SSA will impose any such sanctions in accordance with POMS GN 02604.430. Accordingly, the SSA must continue administrative sanction actions in all cases that meet all of the following four criteria:
 - 1. The OIG investigated the case;
 - 2. The Department of Justice (DOJ) declined to prosecute the case;

3. The Office of Counsel to the Inspector General (OCIG) did not impose a civil monetary penalty (CMP); and
4. The OIG returned the case with the following statement: “SSA has asked OCIG to identify cases that both DOJ and OCIG have considered but declined to pursue, and that may warrant further action by the agency. This case meets these conditions. Therefore, we are referring it to SSA.”

D. OCIG will facilitate all OIG referrals for administrative sanction to SSA.

016.100

Section 1140—Misuse of SSA Program Words, Emblems, and Symbols

- A.** Section 1140 of the Social Security Act authorizes the Commissioner to impose penalties against those who use SSA’s program words, emblems, and symbols in advertisements, solicitations, or other communications in a manner that may mislead people into believing that the communication originated with, or was endorsed or approved by, SSA.
- B.** The Commissioner delegated authority to impose such penalties to the IG, who re-delegated the authority to the Chief Counsel to the Inspector General. A penalty of up to \$5,000 may be imposed for each communication that violates Section 1140. In the case of mass mailings, each piece of mail constitutes a separate violation. Inclusion of a disclaimer of non-governmental affiliation is not sufficient to avoid imposition of a penalty.
- C.** In addition to the authority to impose penalties, Section 1140 provides authority to seek and obtain injunctive relief against those in violation of the statute. Such relief may include a Court order to:

 - 1.** stop the violative communications;
 - 2.** permit an administrative search of business premises;
 - 3.** freeze assets in anticipation of the imposition of a penalty; and/or
 - 4.** permit a mail stop to be imposed on the violators’ incoming U.S. mail.
- D.** Any Special Agent who receives a document or other communication that may constitute a violation of Section 1140 should refer it to OCIG, or contact the Attorney-on-Call to discuss the possible violation.
- E.** From time to time, OCIG may request the assistance of OI in a Section 1140 case. Such requests will be made and approved at OI Headquarters, and the appropriate FD will be advised by OI Headquarters on how to proceed.
- F.** If OCIG’s request for investigative assistance is granted, any Special Agents assigned will work under the joint direction of his or her own OI supervisors, OCIG, and, when appropriate, the United States Attorney’s Office with jurisdiction over the case.

Chapter 16 — **EXHIBITS**

[16-1 — Civil Monetary Penalty Authorities under Section 1129](#)

Exhibit 16-1 Civil Monetary Penalty Authorities under Section 1129

Civil Monetary Penalty Authorities under Section 1129

Authority	Relevant Dates	Examples
<p>False statement or representation, or omission of material fact for use in determining any right to or amount of Social Security benefits</p> <p>(The total CMP could be up to \$5,000 for each false statement, representation or omission and up to twice the resulting overpayment amount)</p>	<p>Six years statute of limitations between the false statement, false representation, or omission and when OCIG sends the penalty letter</p>	<ul style="list-style-type: none"> • A double check negotiation qualifies as a false representation that the original check was not received • An individual reports to SSA that he is not working when in fact he is working • An individual omits answering a question on an SSA form that asks whether the person has any assets when that person has savings accounts and stock accounts • An SSI applicant does not list her spouse as living with her when in fact the spouse is living with her • A beneficiary or rep payee continues to cash Social Security checks (as opposed to direct deposit) knowing that he is not entitled to the benefits <p>(SSA should have made an overpayment determination if applicable)</p>
<p>A Representative Payee's (either individual or organizational) wrongful conversion of all, or any part, of a beneficiary's funds.</p> <p>(The total CMP could be up to \$5,000 for each monthly payment that involved conversion and up to twice the resulting misuse amount)</p>	<p>Beginning March 2, 2004</p>	<ul style="list-style-type: none"> • A rep payee spends a beneficiary's money on himself while the beneficiary is a ward of the state • A rep payee spends half of a beneficiary's payment on food for the beneficiary and spends the other half on personal items for the Rep Payee <p>(SSA should have made an overpayment determination)</p>
<p>Failure to report a change in status by withholding material facts relating the determination of any right to or amount of Social Security benefits</p> <p>(The total CMP could be up to \$5,000 for each payment received while withholding disclosure of a material fact and up to twice the resulting overpayment amount)</p>	<p>Beginning November 27, 2006</p>	<ul style="list-style-type: none"> • An individual works under one SSN and receives benefits under another SSN. • A beneficiary and another individual are listed on a joint bank account into which SSA direct deposits benefits; the beneficiary dies and the surviving individual does not inform SSA of the death and SSA continues to direct deposit benefits into the bank account which the surviving individual spends. • A current disability beneficiary returns to work and does not tell SSA • A current SSI beneficiary has a change in resources (e.g. inheritance, court settlement) and does not tell SSA • An SSI beneficiary does not report a change in living arrangements <p>(SSA should have made an overpayment determination if applicable)</p>

Please call the OCIG Duty Attorney with any questions at (b) (6) or send an e-mail to (b) (7)(E)

VICTIM AND WITNESS ASSISTANCE PROGRAM

017.000 **General**

- A. The Social Security Administration (SSA) Office of the Inspector General (OIG) has established procedures to be followed when responding to the needs of crime victims and witnesses.
- B. All employees must be aware of these procedures to ensure that requirements are met that are placed on Federal law enforcement agencies by the *Victim and Witness Protection Act of 1982*, the *Victims Crime Control Act of 1984*, the *Victims' Rights and Restitution Act of 1990*, the *Violent Crime Control and Law Enforcement Act of 1994*, the *Antiterrorism and Effective Death Penalty Act of 1996*, the *Victims Rights Clarification Act of 1997*, and the *Justice for All Act of 2004*.

017.010 **Authority**

- A. The *Victim and Witness Protection Act of 1982* (VWPA), 18 U.S.C. §§ 1512 to 1515, was enacted, in part, to “enhance and protect the necessary role of crime victims and witnesses in the criminal justice process, and to ensure that the Federal Government does all that is possible within limits of available resources to assist victims and witnesses of crime without infringing on the constitutional rights of the defendant...” The VWPA requires the Attorney General (AG) to develop and implement guidelines concerning “services to victims of crimes” for Department of Justice (DOJ) personnel, and to assure that other Federal law enforcement agencies adopt policies consistent with the DOJ guidelines.
- B. Starting with VWPA and continuing through later legislation, Congress established a list of victims' rights, commonly referred to as the “victims’ bill of rights,” and directed DOJ and other Federal Government agencies involved in the detection, investigation, or prosecution of crime to make their “best efforts” to see that crime victims are afforded the rights. Congress also defined a group of services that Federal agencies have the responsibility to provide to crime victims. The basic list of responsibilities appears in [42 U.S.C. § 10607](#).
- C. The *Justice for All Act of 2004* expanded and recodified the victims’ bill of rights at 18 U.S.C. § 3771(a) (they were previously listed at 42 U.S.C. § 10606), and gave victims standing to enforce those rights. Crime victims have two mechanisms for enforcing the rights listed in section 3771(a): (1) Judicial enforcement—crime victims, or the Government on their behalf, may move in Federal district court for an order enforcing their rights (18 U.S.C. § 3771(d)(3)); and (2) Administrative Complaint—crime victims may file an administrative complaint if DOJ employees fail to respect the victims’ rights. The Attorney General must take and “investigate complaints relating to the provision or violation of the rights of a crime victim” and provide for

disciplinary sanctions for DOJ employees who “willfully and wantonly fail” to protect those rights (18 U.S.C. § 3771(f)(2)).

- D.** In May 2005, the Attorney General issued the Attorney General Guidelines for Victim and Witness Assistance (AG Guidelines), which supersede the 2000 AG guidelines. While the guidelines specifically apply to those components of the DOJ engaged in investigative, prosecutorial, correctional, or parole functions within the criminal justice system, they also provide definitive guidance to State and Federal law enforcement agencies on the implementation of the *Justice for All Act of 2004*, as well as prior enacted legislation on the fair treatment of crime victims and witnesses.
- E.** The AG Guidelines are intended to apply in all cases when individual victims are adversely affected by criminal conduct or in which witnesses provide information regarding criminal activity. Individuals who are culpable for the crime being investigated or prosecuted should **not** be considered as victims for purposes of the rights and services provided under the AG Guidelines. However, a person who may be culpable for violations or crimes other than the crime being investigated or prosecuted may be considered a victim under the AG Guidelines.

017.020 Policy

- A.** It is the OIG Office of Investigations’ (OI) policy that all matters pertaining to crime victims and witnesses are addressed in accordance with the governing statutes and the procedures contained in this chapter. Application will come into effect in all cases in which individual victims are adversely affected by criminal conduct or in which witnesses provide information regarding criminal activity. While special attention shall be paid to victims of serious, violent crime, **all** victims and witnesses of Federal crime who have suffered physical, financial, and/or emotional trauma shall receive the assistance and protection to which they are entitled under the law. A victim is covered by the following “Bill of Rights” at 18 U.S.C. § 3771(a):
 - 1.** The right to be reasonably protected from the accused.
 - 2.** The right to reasonable, accurate, and timely notice of any public court proceedings, or any parole proceeding, involving the crime or of any release or escape of the accused.
 - 3.** The right not to be excluded from any such public court proceeding, unless the court, after receiving clear and convincing evidence, determines that testimony by the victim would be materially altered if the victim heard other testimony at that proceeding.
 - 4.** The right to be reasonably heard at any public proceeding in the district court involving release, plea, sentencing, or any parole proceeding.
 - 5.** The reasonable right to confer with the attorney for the Government in the case.
 - 6.** The right to full and timely restitution as provided in law.
 - 7.** The right to proceedings free from unreasonable delay.
 - 8.** The right to be treated with fairness and with respect for the victim’s dignity and privacy.

- B. Field division (FD) personnel have the responsibility of providing services and information to victims and witnesses of a crime (see 017.040 E).

017.030 Definitions

- A. The term *crime victim* is defined differently by different Federal statutes. The AG Guidelines use the following definitions:
 - 1. **Enforcement of Rights**—For purposes of enforcing the rights, a victim is “a person directly and proximately harmed as a result of the commission of a Federal offense or an offense in the District of Columbia” (18 U.S.C. § 3771(e)) if the offense is charged in Federal district court. If the victim is under 18 years of age, incompetent, incapacitated, or deceased, a family member or legal guardian of the victim, a representative of the victim’s estate, or any other person so appointed by the court may exercise the victim’s rights, but in no event shall the accused serve as a guardian or representative for this purpose (18 U.S.C. § 3771(e)). A victim may be a corporation, company, association, firm, partnership, society, or joint stock company (1 U.S.C. § 1).
 - 2. **Provision of Services**—For purposes of providing services, a victim is “a person that has suffered direct physical, emotional, or pecuniary harm as a result of the commission of a crime” (42 U.S.C. § 10607(e)(2)). If a victim is an institutional entity, services may be provided to an authorized representative of the entity. If a victim is under 18 years of age, incompetent, incapacitated, or deceased, services may be provided to one of the following (in order of preference) for the victim’s benefit: a spouse, a legal guardian, a parent, a child, a sibling, another family member, or another person designated by the court.
- B. The term *witness* means a person who has information or evidence concerning a crime, and provides information regarding his/her knowledge to a law enforcement agency. Where the witness is a minor, the term “witness” includes an appropriate family member or legal guardian. The term “witness” does not include a defense witness or an individual involved in the crime as a perpetrator or accomplice.
- C. The term *serious crime* (as used in the VWPA) means a criminal offense that involves personal violence, attempted or threatened personal violence, or significant property loss.
- D. The term *financial* or *pecuniary harm* shall not be defined or limited by a dollar amount; thus, the degree of assistance must be determined on a case-by-case basis.
- E. The term *child abuse* means the physical or mental injury, sexual abuse or exploitation, or negligent treatment of a child.
- F. The term *negligent treatment* means the failure to provide, for reasons other than poverty, adequate food, clothing, shelter, or medical care so as to seriously endanger the physical health of a child.
- G. The term *child abuse* shall **not** include discipline administered by a parent or legal guardian to his or her child provided it is reasonable in manner and moderate in degree and otherwise does not constitute cruelty.

017.040 Responsibilities

- A. The Assistant Inspector General for Investigations is responsible for developing policies and procedures to assure the proper exercise of law enforcement authority by special agents (SA) in identifying the victims of crime and performing the required services.
- B. The Deputy Assistant Inspectors General for Investigations are responsible for general oversight of compliance with this chapter through the Special Agent-in-Charge (SAC).
- C. Special Agents-in-Charge are responsible for ensuring that SAs comply with the OIG OI policy and procedures when dealing with victims and witnesses of crime. SACs are to perform the following:
 - 1. Designate in writing the appropriate Assistant Special Agent-in-Charge (ASAC), or Resident Agent-in-Charge (RAC) in each office of the field division (FD) and an alternate as the victim/witness contact for providing assistance to victims and witnesses.
 - 2. Establish internal procedures to ensure the proper oversight of providing services to victims and witnesses, tracking and recording the procedures used in providing these services, and training all FD personnel in their victim/witness responsibilities under the law.
 - 3. Establish contact with the Victim/Witness Coordinator (VWC) in all United States Attorneys' Offices (USAO) located in the respective FD. Determine the required coordination between the OIG OI and the USAO to ensure that victims and witnesses receive all of the services enumerated under the law. Assign staff to serve as a member of the USAO, Victim/Witness Subcommittee if requested.
- D. **Assistant Special Agents-in-Charge and Resident Agents-in-Charge**
 - 1. Carry out all duties associated with the position of victim/witness contact.
 - 2. When necessary, make arrangements for the reasonable protection of a victim/witness by contacting the responsible Federal agency (i.e., United States Marshals Service, Federal Bureau of Investigation, etc.).

E. Case Agent/Special Agent

- 1. Identification of Victims**—At the earliest possible opportunity after the detection of a crime at which it may be done without interfering with an investigation, the agent shall identify victims/witnesses and inform them of their right to receive services mandated by law. (see [Exhibit 17-1](#)). In cases involving large numbers of victims, both new technology and traditional law enforcement methods can be utilized to identify and locate victims. For example, officials may use notices on official Web sites or in print or broadcast media to ask victims to contact the Agency. Access to a toll-free number can be arranged so that victims can both provide identification information and receive information about available assistance and services.
- 2. Initial information**—A victim must be informed of the following (see [Exhibit 17-1](#)):
 - a. his or her rights as enumerated in 18 U.S.C. § 3771(a);
 - b. his or her right entitlement, on request, to the services listed in 42 U.S.C. § 10607(c);
 - c. name, title, business address, and telephone number of the responsible official to whom such a request for services should be addressed;
 - d. the place where the victim may receive emergency medical or social services;
 - e. availability of any restitution or other relief to which the victim may be entitled;
 - f. public and private programs that are available to provide counseling, treatment, and other support to the victim;
 - g. the right to make a statement about the pretrial release of the defendant in any case of interstate domestic violence, violation of a protection order, or stalking;
 - h. available protections from intimidation and harassment.
- 3. Referral**—The agent shall assist the victim in contacting the person or official responsible for providing the services and relief described in E.2.b above. When charges are filed, the responsibility for making referrals is transferred to the responsible official in the prosecutor's office.
- 4. Notice**—Provide earliest possible notice to victims regarding the status of the investigation of the crime, to the extent it is appropriate to inform the victim and to the extent that it will not interfere with the investigation, the arrest of the suspected offender, the filing of charges against a suspected offender, the scheduling of each court proceeding that the witness is either required to attend or entitled to attend, the release or detention status of an offender or suspected offender, the acceptance of a plea of guilty or nolo contendere or the rendering of a verdict after trial, and the sentence imposed on an offender, including the date on which the offender will be eligible for parole.
 - a. Statutes and regulations, including the Privacy Act, limiting the information that may be disclosed regarding an ongoing investigation.

- c. the death of the offender, if the offender dies while in custody.
12. In conjunction with the USAO, provide the victim with general information regarding the corrections process, including information about work release, furlough, probation, and eligibility for each.
13. Report suspected incidents of child abuse to the local law enforcement agency or local child protective services agency that has jurisdiction to investigate reports of child abuse or to protect child abuse victims in the land, area, or facility in question. Such agencies are designated as the agencies within their respective jurisdictions, provided that such agencies, if non-Federal, have entered into formal written agreements to do so with the Attorney General, his/her delegate, or a Federal agency with jurisdiction for the area or facility in question. If the child abuse occurred outside the Federal area or facility in question, the designated local law enforcement agency or local child protective services agency receiving the report shall immediately forward the matter to the appropriate authority with jurisdiction outside the Federal area in question.

For Federal lands, federally operated facilities, or federally contracted facilities where no agency qualifies for designation pursuant to the above paragraph, the Federal Bureau of Investigation is designated as the agency to receive and investigate reports of child abuse made pursuant to 42 U.S.C. 13031, until such time as another agency qualifies under the parameters set forth above.

017.050 Implementation with Respect to Confidential Informants

- A. In recognition of the confidential and clandestine nature of the relationship with a confidential informant (CI), no action should be taken pursuant to this chapter that could otherwise jeopardize the safety of a CI or compromise his or her identity.
- B. Services that would otherwise be afforded to a private person who is a victim or witness of a crime should be made available to a CI only:
 - 1. after his or her identity has been disclosed on a witness list; or
 - 2. the CI has become a victim of a crime.
- C. Accordingly, an SA need not identify resources available, send correspondence, distribute materials, and/or otherwise engage in conduct that would expand the existing communications between the agent or another Federal agency and the CI, and could jeopardize the safety or compromise the identity of the CI in performing responsibilities under this Act.

017.060 Victim and Witness Awareness Training

- A. All OIG/OI agents who attend the Criminal Investigator Training Program at the Federal Law Enforcement Training Center receive training in Victim and Witness Awareness.
- B. SAs are required to review the victim/witness requirements annually. A memorandum indicating completion of this requirement shall be filed in Administrative File [017.000](#).

SOCIAL SECURITY
Office of the Inspector General

INFORMATION FOR VICTIMS AND WITNESSES OF CRIME

As Federal law enforcement professionals, we are concerned about the problems that victims and witnesses often experience. We know that you may feel anger, confusion, frustration, or fear as a result of your experience. The following information will help you deal with the problems and questions that often surface during an investigation and will provide you with a better understanding of how the Federal criminal justice system works. Included is a description of your rights under Federal law, and information and services available to you as a victim and/or witness. We encourage you to contact your case agent if you have any questions.

YOUR RIGHTS AS A VICTIM

1. The right to be reasonably protected from the accused.
2. The right to reasonable, accurate, and timely notice of any public court proceedings, or any parole proceeding, involving the crime or of any release or escape of the accused.
3. The right not to be excluded from any such public court proceeding, unless the court, after receiving clear and convincing evidence, determines that testimony by the victim would be materially altered if the victim heard other testimony at that proceeding.
4. The right to be reasonably heard at any public proceeding in the district court involving release, plea, sentencing, or any parole proceeding.
5. The reasonable right to confer with the attorney for the Government in the case.
6. The right to full and timely restitution as provided in law.
7. The right to proceedings free from unreasonable delay.
8. The right to be treated with fairness and with respect for the victim's dignity and privacy.

THE INVESTIGATION

Even though the days and months ahead of you may be difficult for you and your family, we need your continued assistance to ensure the aims of justice are fully achieved. A Federal investigation can be complex and lengthy, and it may involve several organizations. During the investigation, you will be kept informed of the status of your case, if you so request. Your case agent will be your principal contact throughout the investigative process. Contact your case agent as soon as possible if you have any questions.

IF YOU ARE THREATENED OR HARASSED

Penalties have been established for harassment and other threats, so if anyone threatens you or you feel that you are being harassed because of your cooperation with the investigation, contact your case agent immediately. The case agent can refer you to the United States Marshal's Service to discuss protective measures.

SOCIAL SECURITY
Office of the Inspector General

IF AN ARREST IS MADE

If you request, you will be notified if a defendant is apprehended. Following the arrest, the case agent will make every effort to advise you of the status of the case.

THE EMOTIONAL IMPACT OF CRIME

Crime emotionally affects many victims and witnesses. Although everyone reacts differently to a crime, victims and witnesses report some common behaviors, such as:

- Increased concern for their personal safety and that of their family.
- Trouble concentrating on their job.
- Difficulty handling everyday problems.
- Going over the circumstances of the crime again and again, thinking about what might have gone differently.

If the defendant either pleads guilty or is found guilty, you may be able to submit an “impact statement” detailing the emotional effects of this crime on your life and the lives of the members of your family. The Federal Victim Witness Coordinator, whose name appears below, can provide further information in preparing such a statement.

RESTITUTION

If you believe that you may be entitled to restitution, which is a legal action to cause restoration of money and/or property lost as the result of your status in this case as a victim and/or witness, you should contact Assistant United States Attorney _____ at (____) ____ - _____ or the United States Attorney’s Office for the _____ District of _____ at (____) ____ - _____ for additional guidance in pursuing your claim.

FEDERAL VICTIM WITNESS COORDINATOR (name and telephone number)

CASE AGENT (name, telephone number, and case file number)

NATIONAL HOTLINE NUMBERS:

1. Elderly Abuse Hot Line: 1-800-392-0210
2. Child Abuse and Neglect Hot Line: 1-800-392-3738
3. Youth Crisis Hot Line: 1-800-448-4663
4. Domestic Violence Hot Line: 1-800-873-6363
5. Mental Health Crisis Hot Line: 1-800-955-8339
6. Suicide Prevention Hot Line: 1-800-784-2433
7. Alcohol and Drug Abuse Hot Line: 1-800-821-4357
8. Compulsive Gambling Crisis Center: 1-800-332-0402
9. Victims of Crime Resource Center: 1-800-842-8467

GENERAL LEGAL MATTERS

018.000 The Right To Financial Privacy Act of 1978

The Right to Financial Privacy Act of 1978 (RFPA), Title 12, United States Code, Sections 3401 – 3422, generally prohibits the disclosure to the Government of the “financial records” of the “customers” of “financial institutions,” except where Government access is required in connection with a legitimate “law enforcement inquiry.” See also Chapter 12 regarding Inspector General Subpoenas.

018.010 Exclusions and Limitations

- A. The RFPA expressly exempts any financial record or information not identifiable with a particular customer. The RFPA, therefore, does not directly protect:
 - 1. Records pertaining to a person that appear in the account of another customer (e.g., check endorsements) or,
 - 2. Items drawn by an individual and deposited into the account of a corporation, if the item is obtained through a search of the corporation’s account.
- B. The RFPA does not pertain to the customer records of corporations, associations, partnerships with *more* than five (5) partners, or other legal entities.
- C. The RFPA includes all banking-type and consumer finance businesses, as well as credit unions and companies issuing credit cards, located in any State or territory of the United States, the District of Columbia, Puerto Rico, Guam, American Samoa, or the Virgin Islands. Court decisions have extended interpretation of this term to include all institutions that extend credit, such as telephone companies, department stores, or gas companies, with regard to charges made to their credit cards.

018.020 Access to Records

- A. An *absolute prerequisite* to Government access to financial records under *any* provision of the RFPA requires that an official of the Government agency seeking such access must submit a written statement to the financial institution certifying the Government’s compliance with all applicable provisions of the RFPA ([Form OI-57](#), [Exhibit 18-1](#))

- B.** Three of five access mechanisms of the RFPA (administrative summons/subpoena, judicial subpoena, and formal written request) require that the Government authority seeking access to a customer's financial records provide such customer with advanced written notification of the fact that access is being sought unless a "delayed notice" order is obtained from an appropriate court, or as part of the exceptions provisions in the RFPA (see *Exceptions*, [018.120](#)).
- C.** When there is reason to believe that a customer will consent to the release of his/her financial records:
1. The customer will be given [Form OI-58](#) entitled "Statement of Customer Rights Under Right to Financial Privacy Act of 1978" ([Exhibit 18-2](#)), and will be asked to complete and submit to the Office of Investigations (OI) [Form OI-59](#), entitled "Customer Consent and Authorization for Access to Financial Records." ([Exhibit 18-3](#))
 2. If such consent is to be obtained by mail rather than in the course of face-to-face interview, the model "Customer Notice" letter ([Form OI-60](#), [Exhibit 18-4](#)) will be used, omitting all of the text after the second paragraph, and the inappropriate enclosures.
- D.** Administrative subpoenas served upon a financial institution pursuant to the RFPA must be accompanied with the appropriate transmittal letter ([Exhibit 18-5](#)). At or before the time of service of an administrative subpoena upon a financial institution for records covered by the RFPA, the following documents must be served upon the individual whose records are being sought (see *Exceptions*, [018.120](#)). These documents must be sent to the customer as part of the transmittal letter ([Exhibit 18-6](#)).
1. Customer Notice ([Form OI-60](#), [Exhibit 18-4](#)).
 2. Statement of Customer Rights Under Right to Financial Privacy Act of 1978 ([Form OI-58](#), [Exhibit 18-2](#)).
 3. Customer Consent and Authorization for Access to Financial Records ([Form OI-59](#), [Exhibit 18-3](#)).
 4. Instructions for Completing and Filing the [Customer's] Enclosed [Challenge] Motion and Sworn Statement (Form OI-61A, [Exhibit 18-7](#)).
 5. Motion for Order Pursuant to Customer Challenge Provisions of the Right to Financial Privacy Act of 1978 ([Form OI-61](#), [Exhibit 18-8](#)).
 6. Sworn Statement of Movant. ([Exhibit 18-9](#))
- E.** The customer has 10 days in which to give consent to or challenge Government access to his/her financial records (14 days if service upon the customer is by mail).
- F.** After the minimum time period has elapsed, the investigator must present the financial institution with a Certificate of Compliance With the Right to Financial Privacy Act of 1978 ([Exhibit 18-1](#)), and may then collect the subpoenaed records.

- G.** Should a motion to quash be filed, usually the agency official seeking the access will be notified. He or she, in turn, must immediately notify the Case Agent, Office of the Counsel to the Inspector General (OCIG), the appropriate United States Attorney, and Civil Division.

018.030 Exceptions

- A.** The RFPA does not pertain to a record or to information that is “not identified with or identifiable as being derived from the financial records of a particular customer.”
- B.** The RFPA’s requirements that a customer be given notice and an opportunity to challenge *do not* apply where:
- 1.** The Government requires access to financial records in connection with a lawful investigation directed at the financial institution in possession of the records, or at any other “legal entity” which is a target within the context of that investigation. No customer notice is required, but customer records obtained pursuant to this exception may be used only for the purpose for which they were originally obtained and may not be used against the customer, and may be transferred to another Federal agency only in connection with that original purpose; or
 - 2.** The Government seeks only basic identifying information concerning an account such as customer name, address, account number, and type of account. The transmittal to be used for this request is shown in [Exhibit 18-5](#).
 - 3.** The RFPA does not apply to subpoenas issued by Federal grand juries. See [12 U.S.C § 3420](#).

NOTE: § 3420 (a)(1) and (3) *require* that financial records (or a description of voluminous records) so obtained *must be actually presented to the grand jury*, and that the records must be destroyed or returned to the financial institution if they are not used in connection with a criminal proceeding.

018.040 Delayed Notification

- A.** In situations where any notice to the customer that his/her records are being (or were) sought or obtained under the RFPA would seriously jeopardize a law enforcement inquiry or some related law enforcement interest, the Government may apply to a court for a delay of its notification obligation of up to 90 days (180 days under [Title 12, U.S.C. § 3406\(c\)](#) for an initial delay of search warrant notification).
- B.** Pursuant to [12 U.S.C. § 3409\(a\)](#), to obtain such a delay of notice order, the Government must make a showing to a judge or magistrate sufficient to support findings that:
- 1.** The pertinent investigation is within the agency’s lawful jurisdiction, and,
 - 2.** There is reason to believe the records sought are relevant to a legitimate law enforcement inquiry, and,
 - 3.** There is reason to believe that notice would result in:

- a. Danger to the life or physical safety of any person,
 - b. Flight from prosecution,
 - c. Destruction of, or tampering with evidence,
 - d. Intimidation of a potential witness, or,
 - e. Otherwise seriously jeopardize an investigation or official proceeding or unduly delay a trial or ongoing official proceeding.
- C. Further delays may be granted for periods not exceeding 90 days upon the same showing of necessity.
- D. Any court order delaying notice under the RFPA not only relieves the Government of its notification responsibility, but also *expressly prohibits* the financial institution from disclosing, during the delay period, that records were sought or obtained.
- E. After expiration of the period of delay, the customer must be served with or mailed a copy of the process or request together with the following notice, which shall state with reasonable specificity the nature of the law enforcement inquiry.

018.050 Transfer of Records

- A. The Government’s transfer of any records originally obtained under the RFPA may be transferred to “another agency or department” only if an official of the transferring agency certifies in writing that there is reason to believe that the records are relevant to a legitimate law enforcement inquiry within the jurisdiction of the receiving agency or department. ([Exhibit 18-10](#)).
- B. Additionally, the customer must be provided with notice ([Exhibit 18-11](#)) of any such transfer within 14 days, unless the Government first obtains a court order delaying such notice.
- C. The requirement for customer notice does not apply when financial records obtained by OI are disclosed or transferred to a United States Attorney, upon the certification by a Special Agent-in-Charge or his/her supervisor that:
- 1. There is reason to believe that the records may be relevant to a violation of Federal criminal law and,
 - 2. The records were obtained in the exercise of OI’s lawful authority to conduct investigations relating to the programs and operations of the Social Security Administration (SSA).
- D. The RFPA does not apply to transfers to State or local agencies. However, these transfers would continue to be subject to other applicable restrictions, such as the Privacy Act of 1974.

**018.060 Policy Regarding Notice to Executor or Administrator of Estate
When Requesting Records of a Deceased Beneficiary**

- A. A “customer” under the RFPA includes any person or *authorized representative* of that person who utilized any service of a financial institution.
- B. A “customer”, therefore, could be an administrator or executor of the estate of a deceased beneficiary, as the deceased beneficiary’s “authorized representative.” When requesting bank records for an individual who is deceased, it should be determined whether an administrator or executor exists and if so, notice should be provided to that individual. If it is determined that no administrator or executor exists, the subpoena may be issued without providing customer notice.

018.070 *Touhy* Regulations

- A. On April 13, 2001, the Social Security Administration's new "*Touhy*" regulations (20 CFR part 403) became effective. Under these new regulations, the Inspector General will determine whether testimony of an Office of the Inspector General (OIG) employee and/or OIG records will be provided in private litigation. The Inspector General has delegated his authority to do so to the Chief Counsel to the Inspector General.
- B. When an OIG employee receives any request (a simple inquiry, a subpoena, a discovery request or a proper application under these regulations) for testimony and/or records in connection with a covered proceeding, he/she must immediately refer the request to the Office of Counsel to the Inspector General (OCIG). If the OIG employee is uncertain whether the request is covered by these regulations, he/she should contact the Attorney-on-Call at (b) (6).

018.080 Federal Tort Claims Act

The Federal Tort Claims Act (FTCA), [28 U.S.C. § 2671, et seq.](#) is the primary law that governs Federal officer liability. It permits aggrieved individuals to bring suit against the Government for damages arising from certain tortious acts by Government employees; e.g., automobile accidents and other torts.

018.090 Liability of Federal Officers

- A. The general rule regarding the liability of Government officials sued as individuals for acts performed in the discharge of official duties is that a Government official has an absolute privilege against damage suits when the acts complained of were taken by him/her within the outer perimeter of his/her official duties.
- B. Government officials; e.g., SAs, performing discretionary functions generally are shielded from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights which a reasonable person would have known.
- C. When a Federal officer knowingly violates clearly established constitutional (or civil) rights, there is no liability protection. Typical kinds of constitutional rights violations include:

1. Compelling a confession – particularly the use of physical force to extract a confession.
 2. Conducting a warrantless search when the SA knew, or should have known that a warrant was required to conduct the search.
 3. Making an arrest when there is no probable cause for the arrest.
 4. Using excessive force when the SA knows/should know there is no necessity for the force.
- D. Intent and knowledge are critical issues in civil rights criminal prosecutions. The prosecution must prove that the defendant intentionally violated a known constitutional right.

018.100 Duty of Care While in Official Custody

- A. Once the Government [OI] takes a person into its custody and holds him there against his will (restricting his liberty), the 14th Amendment to the Constitution imposes a duty to assume some responsibility for his safety and general well-being.
- B. A person in official custody has a right to be free from harm inflicted by third persons, and an official who willfully subjects a custodial subject to a deprivation of that right is subject to criminal liability.

018.110 Motor Vehicles

- A. Congress amended the FTCA to provide that the remedy by suit against the United States under the FTCA for damages to property or personal injury or death resulting from the operation of any motor vehicle by an employee of the Government while acting within the scope of his/her office or employment, is to be exclusive of any other civil action or proceeding against the employee.
- B. Upon certification by the Attorney General that the employee was acting within the scope of his/her employment at the time of the incident, the United States will defend and assume all liability for claims arising from the incident.
- C. The DOJ will determine whether the driver was within the scope of his/her employment based upon consideration of the driver's duties, authorized destination, instructions, whether the driver was engaged in the performance of an official function or acting in furtherance of his/her own personal interests, and any other relevant data.

018.120 Representation

- A. Pursuant to [28 U.S.C. § 2679](#), the Attorney General of the United States will defend a civil action brought against a Federal employee for actions taken by the employee within the scope of his/her employment.

- B. Any OI SA against whom such civil action is brought and who desires representation by the Government is required to provide to OCIG a copy of any process served upon him/her.

Note: Failure to respond to a summons or complaint in an appropriate manner could result in the entry of a default judgment against the defendant/employee. Therefore, it is imperative that OCIG be promptly advised of all such civil suits.

- C. Upon receipt of the process, OCIG will prepare appropriate transmittal documents including a letter for the signature of the defendant/employee requesting the DOJ to authorize representation of him/her. It should be noted that the SA is free to retain private counsel of his/her choice at his/her expense.
- D. Upon notification that the defendant/employee desires representation by the DOJ, the request and other accompanying documents will be forwarded by OCIG to the DOJ for its review.
- E. Determinations as to whether an employee will be afforded representation by the Government are made on a case-by-case basis and are contingent upon a finding by the DOJ that the employee was acting within the scope of his/her employment and that providing representation would be in the interest of the United States.
- F. All questions concerning SA liability issues should be directed to OCIG.

018.130 Legal Considerations Regarding the Use of Text Messaging and E-mails

- A. The use of text messaging and e-mails allows other sources of potentially discoverable material, which may be difficult to preserve. For that reason, OIG Special Agents must limit the use of text messages and e-mails when handling case related issues. The following guidelines are provided:

1. (b) (7)(E) [Redacted]
2. (b) (7)(E) [Redacted]
3. (b) (7)(E) [Redacted]

¹(b) (7)(E) [Redacted]

²(b) (7)(E) [Redacted]

- B.** Understandably, it may be unavoidable to use text messaging or e-mails as a means of communication. The purpose of this guidance is to make the use of messaging and e-mails the exception and not the norm. It is important to preserve any substantive text messaging or e-mail either by saving the message/e-mail long-term or by reducing the message/e-mail to paper in a memorandum or as part of a report of investigation³.

³ (b) (7)(E)

Chapter 18 —**EXHIBITS**

- [18-1 — Certificate of Compliance with the Right to Financial Privacy Act of 1978 \(OI-57\)](#)
- [18-2 — Statement of Customer Rights Under Right to Financial Privacy Act of 1978 \(OI-58\)](#)
- [18-3 — Customer Consent and Authorization for Access to Financial Records \(OI-59\)](#)
- [18-4 — Customer Notice \(OI-60\)](#)
- [18-5 — Transmittal Letter \(Right to Financial Privacy Act\) to Financial Institution](#)
- [18-6 — Transmittal Letter to Customer](#)
- [18-7 — Instructions for Completing and Filing the Enclosed Motion and Sworn Statement \(OI-61A\)](#)
- [18-8 — Motion for Order Pursuant to Customer Challenge Provisions of the Right to Financial Privacy Act of 1978 \(OI-61\)](#)
- [18-9 — Sworn Statement of Movant](#)
- [18-10 — Transfer of Records to Another Agency or Department](#)
- [18-11 — Notice to Customer for Transfer of Records](#)
- [18-12 — Transmittal Letter to Financial Institution \(Account Information Only Under Right to Financial Privacy Act\)](#)

CERTIFICATE OF COMPLIANCE
WITH THE RIGHT TO FINANCIAL PRIVACY ACT OF 1978

Dear _____:

Pursuant to 12 U.S.C. § 3403(b), I hereby certify that the applicable provisions of the Right to Financial Privacy Act of 1978, 12 U.S.C. §§ 3401-3422, have been complied with as to the subpoena duces tecum presented on _____, 2003, for the following financial records of _____:

See specific wording in Chapter 12 of this Handbook

Special Agent-in-Charge

(Date)

Pursuant to the Right to Financial Privacy Act of 1978, good faith reliance upon this certificate relieves your institution and its employees and agent of any possible liability to the customer in connection with the disclosure of these financial records.

Form OI-57 (revised 12/31/02)

STATEMENT OF CUSTOMER RIGHTS UNDER RIGHT TO FINANCIAL PRIVACY ACT OF 1978

Federal law protects the privacy of your financial records. Before banks, savings and loan associations, credit unions, credit card issuers, or other financial institutions may give financial information about you to a Federal agency, certain procedures must be followed.

Consent to Financial Records

You may be asked to consent to the release of your financial records to the Government. Your consent or refusal to consent has no bearing on your relationship with the financial institution. If you give your consent, it can be revoked in writing at any time before your records are disclosed. Any consent you give is effective for 3 months, and your financial institution must keep a record of the instances in which it discloses your financial information.

Without your Consent

Without your consent, a Federal agency that wants to see your financial records may do so ordinarily only by means of a lawful subpoena, summons, formal written request, or search warrant for that purpose.

Generally, the Federal agency must give you advance notice of its request for your records explaining why the information is being sought and telling you how to object in court. The Federal agency must also send you documents to be prepared by you with instructions for filling them out and filing them with the court. While these procedures will be kept as simple as possible, you may want to consult with an attorney before making a challenge to a Federal agency's request.

Exceptions

In some circumstances, a Federal agency may obtain financial information about you without advance notice or your consent. In these instances, the Federal agency is required to establish in court that the Government's investigation and request for your records are proper, before permission is granted by the court to obtain your records without giving you prior notice.

When the reason for the delay of notice no longer exists, you will usually be notified that your records were obtained.

Transfer of Information

Generally, a Federal agency which obtains your financial records is prohibited from transferring them to another Federal agency unless it certifies in writing that the transfer is proper and sends a notice to you that your records have been sent to another agency.

Penalties

If a Federal agency or financial institution violates the Right to Financial Privacy Act, you may sue for damages and demand compliance with the law. If you win, you may be repaid your attorney's fees and costs.

Additional Information

If you have any questions about your rights under this law, or about how to consent to release your financial records, please notify the official whose name and telephone number appears below:

Special Agent _____
(SA's telephone number)

**CUSTOMER CONSENT AND AUTHORIZATION FOR ACCESS TO
FINANCIAL RECORDS**

I, (Customer's Name), understanding my rights under the Right to Financial Privacy Act of 1978 (12 U.S.C. §§ 3401-3422), hereby authorize (Name of Financial Institution) to disclose the following financial records:

See Chapter 12 for specific information to be included

to the Social Security Administration, Office of the Inspector General, Office of Investigations, for the following purpose(s):

See Chapter 12 for specific information to be included

I understand that this authorization may be revoked by me in writing at any time before my records are disclosed, and that this authorization is valid for no more than three months from the date of my signature.

Date: _____

Signature: _____

CUSTOMER NOTICE

Dear _____:

Records concerning your financial transactions held by the financial institution named in the enclosed subpoena are being sought by the Social Security Administration, Office of the Inspector General, Office of Investigations, in accordance with the Right to Financial Privacy Act of 1978, 12 U.S.C., Sections 3401-3422, for the following purpose(s): ***Example: to aid in an official investigation concerning the possible fraudulent or otherwise improper receipt and/or use of Social Security benefits.***

A statement of your rights under the RFPA as a customer of the financial institution named above is enclosed. If you have no objection to having the financial records identified released by the financial institution, please complete the Customer Consent and Authorization form enclosed and return it to this office.

If you desire that such records or information not be made available, read the enclosed instructions for completing and filing the enclosed motion paper and sworn statement. Then:

1. Fill out the accompanying motion paper and sworn statement (as indicated by the instructions beneath each blank space) or write one of your own, stating that you are the customer whose records are being requested by the Government, and either giving the reasons you believe that the records are not relevant to the legitimate law enforcement inquiry stated in this notice or any other legal basis for objecting to the release of the records.
2. File the motion and sworn statement by mailing or delivering them to the Clerk of any of the following United States District Courts (in some cases, there will be only one appropriate court):
 - a) United States District Court, District of _____
 - b) United States District Court, District of Columbia
 - c) United States District Court for the district in which you reside.

(It would simplify the proceeding if you would include with your motion and sworn statement a copy of the enclosed subpoena, as well as a copy of this notice.)

3. Serve the Government authority requesting the records by mailing (by registered or certified mail) or by delivering a copy of your motion and sworn statement to Special Agent _____, Social Security Administration, Office of the Inspector General, Office of Investigations.
4. Be prepared to come to court and present your position in further detail.

You do not need a lawyer, although you may wish to employ one to represent you and protect your rights.

If you do not follow the above procedures, upon the expiration of 10 days from the date of service or 14 days from the date of mailing of this notice, the records or information requested therein may be made available. These records may be transferred to other Government authorities for legitimate law enforcement inquiries, in which event you will be notified after the transfer.

Sincerely yours,

Deputy Assistant Inspector General
for Investigations

6 Enclosures:
Statement of Customer Rights
Customer Consent and Authorization Form
Motion/Statement Instructions
Motion Form
Sworn Statement Form
Subpoena (Copy)

CERTIFIED MAIL – RETURN RECEIPT REQUESTED

Re: OI Case No. _____

Dear _____:

Accompanying this letter is a subpoena addressed to you as the Custodian of Records for (*name*), returnable to the Social Security Administration, Office of the Inspector General, Office of Investigations, in (*name of city*) before my designee, Special Agent (*name*). The subpoena has been issued pursuant to the authority provided to the Inspector General under the Inspector General Act of 1978, as amended, 5.U.S.C. app. 3 § 6(a)(4).

Fully legible and complete copies of the records called for by the subpoenas will be accepted in response to the subpoenas, provided that the original records will be made available to employees of my office, upon request, during normal business hours. Otherwise, original documents (including copies as maintained in your files) should be produced.

Failure to appear at the time and place specified in the subpoena may be taken as a failure to comply with the subpoena. However, as a convenience, you may assemble the documents requested and mail them by certified mail on or before (*date*) to:

Social Security Administration
Office of the Inspector General/Office of Investigations

ATTN: Special Agent (*name*)

This subpoena is issued pursuant to section 3413(g) of the Right to Financial Privacy Act of 1978 (12 U.S.C. § 3401 *et seq.*). Pursuant to this section, customer notification is not required. Enclosed for your records is a Certificate of Compliance with the RFPA notice.

If you have any questions, please feel free to contact Special Agent (*name*) at () *phone number*.

Sincerely,

Deputy Assistant Inspector General
for Investigations

Enclosure

CERTIFIED MAIL – RETURN RECEIPT REQUESTED

Re: OI Case No. _____

Dear _____:

This letter is to inform you that the Social Security Administration, Office of the Inspector General, Office of Investigations intends to subpoena certain documents under your name from ***(name of financial institution)*** in ***(city, state)***. This action is being taken as part of a current investigation.

You have certain rights guaranteed by the Right to Financial Privacy Act of 1978 (12 U.S.C. Sections 3401-3422), which the accompanying paperwork explains in detail. You have 14 days from the date of this letter to either give consent or to challenge Government access to your financial records. If you fail to challenge or fail to give consent, the subpoenaed materials will then lawfully be collected.

If you have any questions regarding this case, please contact Special Agent ***(name)*** at () ***phone number.***

Sincerely,

Deputy Assistant Inspector General
for Investigations

7 Enclosures:

Customer Notice
Statement of Customer Rights
Customer Consent and Authorization Form
Motion / Statement Instructions
Motion Form
Sworn Statement Form
Subpoena (Copy)

**INSTRUCTIONS FOR COMPLETING AND FILING THE
ENCLOSED MOTION AND SWORN STATEMENT**

1. Except where signatures are required, the indicated information should be either typed or printed legibly in ink in the spaces provided on the enclosed motion and sworn statement forms. The information required for each space is described in parentheses under each space to be completed.
2. The most important part of your challenge application is the space on the “sworn statement” form where you must state your reasons for believing that the financial records sought are not relevant to the legitimate law enforcement inquiry stated in the CUSTOMER NOTICE, if that is your ground to challenge the Government’s access to your financial records. You may also challenge the Government’s access to the financial records if there has not been substantial compliance with the Right to Financial Privacy Act, or for any other reasons allowed under the law. You should state the facts that are the basis for your challenge as specifically as you can.
3. To file your challenge with the Court, either mail or deliver the original and one copy of your challenge to the “Clerk” of the Court. (You must pay any filing fee.)
4. One copy of your challenge papers (motion and sworn statement) must be hand delivered or mailed (by registered or certified mail) to the Government official whose name appears on the CUSTOMER NOTICE.
5. If you have further questions, contact the Government official whose name appears on the CUSTOMER NOTICE.

UNITED STATES DISTRICT COURT

(Customer's name)

Movant,
-vs-

Miscellaneous No. _____

SOCIAL SECURITY ADMINISTRATION
OFFICE OF THE INSPECTOR GENERAL
Respondent.

MOTION FOR ORDER PURSUANT TO
CUSTOMER CHALLENGE PROVISIONS OF THE
RIGHT TO FINANCIAL PRIVACY ACT OF 1978

(Movant's Name) hereby moves this court, pursuant to Section 1110 of the Right to Financial Privacy Act of 1978, 12 U.S.C., Section 3410, for an order preventing the Government from obtaining access to my financial records. The agency seeking access is the Social Security Administration, Office of the Inspector General. My financial records are held by *(Name of Financial Institution)*.

In support of this motion, the court is respectfully referred to my sworn statement filed with this motion.

Respectfully submitted,

(Signature)

Name: _____

Address: _____

City / State: _____, _____

Zip Code _____

UNITED STATES DISTRICT COURT

(Customer's name)

Movant,
-vs-

Miscellaneous No. _____

SOCIAL SECURITY ADMINISTRATION
OFFICE OF THE INSPECTOR GENERAL
Respondent.

SWORN STATEMENT OF MOVANT

I, _____, (am presently/was previously) a customer of _____, and I am the customer whose records are being requested by the Government.

The financial records sought by the Social Security Administration, Office of the Inspector General, are not relevant to the legitimate law enforcement inquiry stated in the Customer Notice that was sent me because:

or should not be disclosed because there has not been substantial compliance with the Right to Financial Privacy Act of 1978, 12 U.S. C. §§ 3401-3422, in that: _____

or should not be disclosed on the following other legal basis:

I declare under penalty of perjury that the foregoing is true and correct.

_____, 20____
(Month) (Day) (Year)

(Signature)

(Name – Print or Type)

SOCIAL SECURITY ADMINISTRATION
BALTIMORE, MARYLAND 21235

*OFFICE OF THE INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS*

CERTIFICATION FOR TRANSFERRING RECORDS
OBTAINED PURSUANT TO THE RIGHT TO
FINANCIAL PRIVACY ACT OF 1978

TO: _____
(Name and Address of Receiving Agency)

FROM: _____
(Name and Address of Transferring Government Agency)

The records of the following customer of a financial institution are in our possession:

(Name of Customer)

(Address of Customer)

(Type of Records and Account Number)

(Name of Financial Institution)

Pursuant to § 1112(a) of the Right to Financial Privacy Act of 1978, 12 U.S.C. § 3412(a), the records described above are being transferred to you. I certify that there is reason to believe that the records being transferred are relevant to a legitimate law enforcement inquiry within the jurisdiction of your agency or department.

_____, 20____
(Date)

(Name and Title of Official)

(Telephone)

(Government Agency)

Copies to the Following Files:

SOCIAL SECURITY ADMINISTRATION
BALTIMORE, MARYLAND 21235

*OFFICE OF THE INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS*

CERTIFICATE OF LEGITIMATE LAW ENFORCEMENT INQUIRY

Pursuant to 12 U.S.C. § 3412(a), I hereby certify that there is reason to believe that the financial records of (**name of the customer**) originally obtained by the Social Security Administration, Office of the Inspector General, Office of Investigations, by a subpoena dated , issued pursuant to the Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401, et seq. are relevant to a legitimate law enforcement inquiry within the jurisdiction of (**name of the receiving agency or department**).

Special Agent-in-Charge

SOCIAL SECURITY ADMINISTRATION
BALTIMORE, MARYLAND 21235

OFFICE OF THE INSPECTOR GENERAL
OFFICE OF INVESTIGATIONS

CUSTOMER NOTICE

CERTIFIED MAIL – RETURN RECEIPT REQUESTED OR HAND DELIVERED

Dear _____:

This is to notify you that copies of, or information contained in, your financial records lawfully in possession of the Office of the Inspector General, Office of Investigations, Social Security Administration, have been furnished to (**name of agency or department records have been transferred to**) pursuant to the Right to Financial Privacy Act of 1978 [12 U.S.C. § 3401 et seq.] for the following purpose: (**the nature of the law enforcement inquiry must be stated with reasonable specificity**).

If you believe that this transfer has not been made to further a legitimate law enforcement inquiry, you may have legal rights under the Right to Financial Privacy Act of 1978 [12 U.S.C. § 3401 et seq.] or the Privacy Act of 1974 [5 U.S.C. § 522a].

Sincerely,

(Name and Title of Official)

(Government Agency)

(Address)

Enclosure – (**Copy of the certification that records are relevant to a legitimate law enforcement inquiry within the jurisdiction of the receiving agency or department.**)

NOTE: THIS NOTICE MUST BE SENT TO THE CUSTOMER WITHIN 14 DAYS OF THE DATE OF THE TRANSFER OF THE FINANCIAL RECORDS SUBJECT TO THIS CHAPTER.

HAND DELIVERED OR CERTIFIED MAIL – RETURN RECEIPT REQUESTED

ATTN: Custodian of Records

Re: OI Case No. _____

Dear Sir/Madam:

Accompanying this letter is a subpoena addressed to you as the Custodian of Records for *(name)*, returnable at the Social Security Administration, Office of the Inspector General, Office of Investigations, (city and state) before my designee, Special Agent *(name)*. The subpoena has been issued pursuant to the authority provided to the Inspector General under Public Law 95-452 (5 U.S.C. Appendix 3, Section 6(a)(4)), as amended by Public Law 100-504.

Fully legible and complete copies of the records called for by the subpoena will be accepted in response to the subpoena, provided that the original records will be made available to employees of my office, upon request, during normal business hours. Otherwise, original documents (including copies as maintained in your files) should be produced. Please note this subpoena is not for specific financial transaction records but for basic account identification information.

Failure to appear at the time and place specified in the subpoena may be taken as a failure to comply with the subpoena. However, as a convenience, you may assemble the documents requested and mail them by certified mail on or before (date) to:

Social Security Administration
Office of the Inspector General/Office of Investigations

ATTN: Special Agent *(name)*

This subpoena is issued pursuant to section 3413(g) of the Right to Financial Privacy Act of 1978 (RFPA) (12 U.S.C. § 3401 et seq.). Pursuant to this section, customer notification is not required. Enclosed for your records is a Certificate of Compliance with the RFPA. You may assemble and deliver the account identification information, pursuant to the subpoena, at your earliest convenience but no later than the specified return date.

If you have any questions, please feel free to contact Special Agent *(name)* at *(telephone number)*.

Sincerely,

Deputy Assistant Inspector General
for Investigations

Enclosure

FREEDOM OF INFORMATION and THE PRIVACY ACT

019.000 The Freedom of Information Act

The Freedom of Information Act (FOIA), Title 5, United States Code, Section 552, was enacted in 1966, and provides that any person has the right to request access to federal agency records or information. All agencies of the United States Government are required to disclose records upon receiving a written request for them, except for those records that are protected from disclosure by the nine exemptions and three exclusions of the FOIA. This right is enforceable in court. Each agency responds to requests for its own records. The Federal FOIA does not, however, provide access to records held by Congress, the courts, state or local government agencies, or by private businesses or individuals.

- A.** The Social Security Administration, Office of Public Disclosure (OPD) is the Agency component responsible for responding to FOIA requests for Agency records (including OI criminal investigative files). However, the Office of the Inspector General, Office of the Counsel to the Inspector General (OCIG) first reviews the records being sought and recommends to OPD whether the entire record, or portions thereof should be withheld from disclosure under one or more of the FOIA exemptions and/or exclusions. OCIG is the *only* OIG component authorized to decide what information, if any will be released as a result of FOIA requests.
- B.** Once an agency is in receipt of a proper FOIA request, it is required to inform the requester of its decision to grant or deny access to the requested records within 20 working days. Agencies are not necessarily required to release records within the 20 days, but access to releasable records should be granted promptly thereafter.
- C.** Requests for records that are normally prepared for public distribution, such as press releases, fact sheets marked for public release, final audit reports, information brochures, and speeches *are not* FOIA requests. The Office of Communications and Resource Management (OCRM) at HQ will promptly provide such records to any requester without reference to the FOIA, without referral to OCIG, and without collecting any fees.

019.010 Policy Statement

It is OI policy not to release any records in connection with an ongoing investigation. Further, discussions with persons who are seeking specific information under the FOIA about OI criminal investigative records is prohibited without the express authorization of the OCIG and the DAIGI.

019.020

Methodology

- A. FOIA requests are considered “time sensitive,” therefore, all FOIA requests received by any OI component/office must be forwarded without delay to the OCIG.
 - 1. All FOIA requests must be forwarded to OCIG within seventy-two (72) hours of receipt, unless compelling circumstances exist which prevent compliance. An OIG Memorandum detailing the reason(s) for the delay must be attached to the forwarded FOIA request.
 - 2. All FOIA requests must be sent to OCIG via USPS certified mail, FedEx or other common carrier which will produce written documentation as to date of delivery to OCIG. In the event that the FOIA request is received by a Headquarters component, the component delivering the request to OCIG must document same on the request.
- B. OCIG is responsible for forwarding the FOIA Request to the SSA/OPD, and obtaining a Control Number from OPD documenting receipt.
- C. OCIG will request a records search through the OI Regional Desk Officer. If records responsive to the request exist in OI, the Regional Desk Officer should be so advised, and a complete copy of the records forwarded to OCIG. If the records are incomplete, OCIG may contact the field division for full compliance.

NOTE: Do not send the original investigative file.

- D. Where the request is for records maintained in an OI investigative file, the OI Special Agent (SA) must confirm the status of the investigation with the Regional Desk Officer; i.e., open or closed. It is also essential that OCIG know whether the case is before the grand jury or at trial, and any other details relating to its judicial status.
 - 1. OI offices will make every effort to locate and retrieve all records responsive to a particular FOIA request (including OI investigative files).
 - 2. If the initial search did not reveal the existence of certain records which are subsequently discovered, OCIG must be immediately informed of the existence of such records.
 - 3. Documents and records which originated with another agency and which are contained in OI investigative files must be “flagged” in such a manner as to alert OCIG of same so that OCIG can segregate them for referral to the originating agency for review and direct response to the requester.

019.030 Information Protected from Disclosure

The Freedom of Information Act protects certain information from being disclosed.

- A. Information Concerning the Identity of Confidential Informants - It is imperative that all individuals and information obtained pursuant to an express or implied grant of confidentiality be clearly identified and made known to OCIG. *Special care must be taken to avoid disclosing the actual or constructive identity of such persons to FOIA requesters.* Failure to adhere to this policy could subject sources to the possibility of physical retaliation, and could also have a “chilling effect” on persons coming forward with vital information in future cases.
- B. Information Concerning Certain Investigative Techniques - Protection of non-public law enforcement techniques is crucial to an agency’s ability to carry out its law enforcement functions. Release of investigative techniques to FOIA requesters could result in serious harm to OI investigations in the future. The OI investigative file must “flag” or otherwise clearly identify any investigative techniques not generally known to the public, e.g., special surveillance techniques employing high tech equipment.
 - 1. OCIG will decide whether the information may be withheld under the FOIA.
 - 2. Special Agent personal case notes contained in OI investigative files are subject to the same scrutiny and potential disclosure as any other record contained in the OI case file, unless exempted under one or more of the FOIA exemptions or exclusions. Therefore, SAs should exercise common sense and good judgment when writing their personal notes. Care should be taken to avoid statements or remarks that could potentially be construed as prejudicial, embarrassing, derogatory or otherwise unprofessional.

019.040 Contact with Persons Seeking Records Under the Freedom of Information Act

- A. All OI employees are responsible for ensuring that requests made pursuant to the FOIA are directed to SSA/OPD. Under no circumstances should any OI employee release records to the public without first consulting with OCIG.
- B. Advise the requester that he/she must submit a written request reasonably describing the records being sought to:

Social Security Administration
Office of Public Disclosure
3-A-6 Operations Building
6401 Security Boulevard
Baltimore, MD 21235

- C. OI employees will direct all questions concerning FOIA, access to records, circumstances under which records may be withheld in whole or in part, etc., to OCIG at (410) 965-6211.

019.050 **The Privacy Act of 1974**

The Privacy Act of 1974 (PA), Title 5, United States Code, Section 552a, can generally be characterized as an omnibus code of fair information practices which attempts to regulate the collection, maintenance, use, and dissemination of personal information by Federal Government agencies. Broadly stated, the policy objectives of the PA are to balance the Government's need to maintain information about individuals with the rights of individuals to be protected against unwarranted invasions of their privacy stemming from Federal agencies' collection, maintenance, use, and disclosure of personal information about them.

019.060 **Privacy Act Requests**

- A. Only individuals are entitled to access information under the PA, and that access is limited to information retrievable under the individual's name or other identifiers. OI systems of records containing records compiled for law enforcement purposes (such as criminal investigative files) are often exempt from disclosure, to be determined on a case-by-case basis.
- B. PA requests are processed under the Freedom of Information Act.

019.070 **Privacy Act Violations**

- A. The OI has the authority to investigate suspected violations of the PA where such matters involve SSA programs or operations.
- B. Where the matter involves suspected illegal disclosure of information; and it is not clear whether the information disclosed was part of a system of records, as defined in the PA, and/or whether its disclosure would constitute a violation of the penal provisions of the PA. The matter will be referred to OCIG for a preliminary determination.
- C. In collecting information that will be made part of a criminal investigative file of the OI, an SA is not required under the PA to inform an interviewee of the following:
 - 1. SAs authority to solicit information, and whether providing the information is mandatory or voluntary.
 - 2. Purpose for which the information is intended to be used.
 - 3. Routine uses which may be made of the information.
 - 4. Consequences of the interviewee not providing the information.
- D. The PA provides criminal penalties for willful unlawful disclosure of protected agency information, or willfully maintaining an unauthorized system of records, or knowingly and willfully requesting or obtaining any record from an agency under false pretenses.

TRAINING POLICY

020.000 **General Policy**

The Office of Investigations (OI) recognizes the importance of training. This includes training for newly hired personnel and periodic training for seasoned personnel. The goal of OI training is to provide each employee with the knowledge and skills that provide the necessary tools needed to successfully accomplish the OI mission.

- A. There are five main categories of training: On-the-Job Training, Essential Training, Enhancement Training, Specialized Training, and Management Training.
1. On-the-Job Training: *Training for new Social Security Administration (SSA) Office of the Inspector General (OIG) employees that begins as soon as they report for duty. Initial training received is through an on-the-job training program and a formal mentoring program.*
 2. Essential Training: *Training that is necessary in order to carry out the mission of the office. This training consists of two formal law enforcement programs, which are usually conducted at the Federal Law Enforcement Training Center (FLETC), and one formal programmatic course at SSA.*
 - a. The first essential training program is basic criminal investigator training for Federal agents. This requirement is usually met through completion of the **Criminal Investigator Training Program (CITP)** at FLETC. The length of this program is determined by FLETC through a process that involves curriculum conferences attended by representatives from the agencies that participate in this program. Agents who have successfully completed basic investigator training for another Federal agency (including the Federal Bureau of Investigation, Drug Enforcement Administration, Postal Inspection Service, and any other agency as approved by a Deputy Assistant Inspector General for Investigations (DAIGI)) have met this requirement.
 - b. The second essential training program is conducted at the Inspector General Criminal Investigator Academy (IGCIA) co-located at FLETC. Agents must attend one of two IGCIA programs based on their previous Federal law enforcement experience.
 - Agents new to Federal law enforcement shall attend the **Inspector General Investigator Training Program (IGITP)**, a program designed to provide entry-level training in investigative techniques and types of investigations specific to the

mission of the Inspector General (IG) community. This course builds on the foundation provided in CITP.

- Agents who come to the SSA OIG after serving as an 1811 with a Federal law enforcement agency outside the IG community (i.e., Drug Enforcement Administration; Federal Bureau of Investigation; DHS-Homeland Security Investigations; United States Secret Service, etc.) **and** have attended the basic training program required for that agency shall attend the **Inspector General Transitional Training Program (IGTTP)** at FLETC. The IGTTP is designed to familiarize the agent with the practices and resources that are IG-specific.

REMEDIAL POLICY—Completion of FLETC's CITP and IGITP requires passing a written examination(s). If an employee fails any required examination, he/she will be given one opportunity to repeat the examination, or to repeat the entire training program. Probationary employees who fail to complete these training programs after a second attempt will be subject to termination.

NOTE: In rare circumstances, an 1811 may be exempted from attending the IGITP and/or the IGTTP if they have three full years of experience as an 1811 prior to employment with SSA OIG **and** have experience or training judged to be equivalent to that which they would receive in a formal IGICIA program. Any 1811 who believes he/she may qualify for such an exemption should submit a request to the appropriate DAIGI through his/her SAC immediately after being hired. The request must consist of a complete statement of experience and training (*see Exhibit 20-3*) in all of the following elements:

- interviewing
- report writing
- conducting investigations
- legal training
- firearms
- defensive tactics/arrest techniques

A DAIGI and the OIG OI Training Program Manager (TPM) will evaluate the request to determine if the experience and training are equivalent to the IGICIA program from which the agent is requesting exemption. Waivers will not be granted unless all elements are sufficiently met.

- c. The third essential training program is Title II/Title XVI Fundamentals course administered by SSA. Agents who come to OI from SSA positions in which they have received training in Title II and Title XVI are exempt from this requirement.
3. **Enhancement Training:** *Training that is necessary to improve the professionalism and competence of Special Agents (SA).* This training is needed to refine law enforcement skills and to keep agents current with changing laws, investigative methods, and technology. As part of the Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority (*see Chapter 1, Exhibit 1-2*), OIG agents are required to complete periodic refresher training in the following areas: trial process, Federal criminal and civil legal updates, physical conditioning, firearms, and defensive tactics.

4. Specialized Training: *Training that qualifies an agent as a specialist in a given field.* Areas of specialized training include defensive tactics instructor, extendible baton instructor, firearms instructor, OC pepper spray instructor, physical fitness instructor, photographer, seized computer and evidence recovery specialist (SCERS), and technical investigative equipment specialist.
5. Management Training: *Training to develop, improve, or maintain the competence of managers and aspiring managers.* This training can be conducted by a variety of Government and non-government entities.

B. All authorized training of agents will be job-related and otherwise consistent with the training policies of the SSA, Office of Personnel Management (OPM), and the OIG.

020.010 **Responsibilities**

A. The following outlines the training responsibilities for SACs, Divisional Training Officers (DTO), and the TPM.

1. The SAC for each field division (FD), in consultations with the Assistant Special Agents-in-Charge (ASAC) and Resident Agents-in-Charge (RAC), shall be responsible for determining the training needs of SAs assigned to their divisions. The SAC shall designate an agent as the DTO. In the absence of a DTO, the SAC will assume the duties of the DTO.
2. The DTO is a collateral duty assignment. The DTO coordinates the attendance at FLETC programs through the OI TPM, assists in the planning of divisional training conferences, and identifies local training opportunities. The DTO is responsible for the on-the-job training program and mentoring program for new OIG agents.
3. The TPM is the primary training advisor in OI and is the agency-designated point of contact for FLETC and the IGCIA at FLETC regarding issues relating to curriculum development and program content. All training for OI agents at FLETC will be coordinated by the DTO through the OI TPM.
4. In addition to designing, developing, and tracking training programs for OI, the OI TPM is responsible for scheduling training at FLETC. The DTO shall advise the OI TPM when an agent has been designated to attend training at FLETC. The OI TPM will contact FLETC and enroll the SA in the training course upon notification from the DTO or the SAC. A Training Nomination and Authorization form, [SSA-352](#) (formerly HHS 350), ([Exhibit 20-1](#)) is no longer required for training at FLETC. The only exception to this would be training that is being paid for outside of the OIG's Inter-Agency Agreement (IAA) with FLETC. **The individual who has been designated by the SAC and has been granted access must enter all training requests into the Office of Communications and Resource Management (OCRM) training database.**

B. When an SSA-352 is appropriate, it is the responsibility of each SA to prepare his/her own SSA-352. The SA should forward the SSA-352 to the appropriate ASAC and SAC for approval. The SSA-352 is maintained in the field as a record of training and is not part of the payment process

for FLETC or the IGCIA. Vouchers for reimbursement are initiated monthly by FLETC and processed via the On-line Payment and Collection System (OPAC) directly and the SSA Office of Finance. The IGCIA also bills using this procedure.

- C. Once an SA has been registered for a training course, every effort should be made to attend the course. If an SA who is registered for a course is unable to attend due to extenuating circumstances, a replacement should be obtained from the division. Cancellations should be made only in emergencies, and every effort must be made to obtain a refund from the vendor.

FLETC must be informed of a cancellation 20-working days in advance; otherwise, OIG/OI will be billed for the course. Therefore, it is imperative that the OI TPM be notified of a FLETC cancellation in sufficient time to avoid incurring unnecessary training costs.

Upon successful completion of training, the record will be updated on the completed training screen. As with any data added to this section, appropriate documentation (diploma, transcript, certificate, etc.) should be reviewed prior to data entry.

A Training and CPE Reporting Form ([SSA OIG Form EDU-6750](#)) must be submitted through the SAC after completion of all training and forwarded to the OI TPM.

020.020 Payment

The OIG/OI FDs assume responsibility for the completion of the SSA-352 forms as a record of training. Except for FLETC and IGCIA training, the FDs will also assume responsibility for the subsequent payment for training. Whenever possible, FDs are encouraged to use the SSA International Merchant Purchase Authorization Card (IMPAC) for payment. The normal limit of \$3,000 per purchase should be observed. When the FLETC IAA or IMPAC process is used, the SSA-352 need not be forwarded to the vendor.

020.030 Training Database

- A. The OIG Office of Communications and Resource Management (OCRM) manages a database containing information about all training OIG employees complete. Each FD is responsible for entering training information into the database. The information should be entered in a timely fashion after the training has been completed.
- B. The OCRM training database is the official source of information for reports on the training activities of OIG personnel. These reports include:
 - 1. Reports relating to the OIG Strategic Plan goal for annual developmental and skill-enhancement training, and
 - 2. Reports relating to firearms training.

020.040 On-the-Job Training and the Mentoring Program

- A. The on-the-job training program is an individualized program designed to ensure that the new employee understands the history, organization, duties, and responsibilities of the SSA and the OIG. This program begins immediately upon the first day the employee reports for duty. The SAC will evaluate the employee's knowledge of the Social Security system and background in criminal investigations, and decide the best method of introducing the agent to the position he/she has been hired to fill.

- B. The SAC will explain the OIG training requirements to the new employee, including the OI New Agent/Mentoring Checklist in the On-the-Job Training Guide (*see [Exhibit 20-2](#)*).

- C. The mentoring program is one in which the new agent works with one or more experienced SSA OIG agents to learn the nuances of the investigative and administrative duties they are expected to perform. The new employee should be assigned to work with an experienced agent for a minimum of 30 days. Additional mentoring periods may be assigned at the discretion of the SAC.

020.050 Individual Development Plan (IDP)

- A. An IDP is a document in which the employee lists his or her professional development goals, both short and long term, and outlines the work activities and training programs needed to help achieve the stated goals.

- B. Each OI employee is required to complete or review an existing IDP as part of the [annual certifications](#) process. Employees can use The Career Development and Training Plan; it identifies key competencies and abilities to assist with identifying training needs to further enhance individual development.

- C. To ensure it remains relevant and current, both the employee and management should perform an annual review of the IDP. This discussion should coincide with annual performance plan reviews. At the conclusion of the discussion, the employee and the supervisor must sign the document to attest to the review of the plan.

- D. The mere existence of an IDP does not mean that the employee will attain the stated goals nor be able to attend all of the identified training programs. The IDP is simply a planning document to assist the employee and supervisor in seeing that the employee gains the experience and training needed to perform at a higher level or with greater proficiency.

020.060 Field Division In-Service Training

- A. SACs may request to hold periodic in-service training for all employees within their FD. This training can address mandated training requirements, local issues, new policies and procedures, or other work-related topics.

- B.** The SAC must notify HQ when a FD in-service training is being planned. The Deputy Assistant Inspector General for Investigations for Field Operations and the OI TPM must approve the training agenda. A representative from HQ may wish to attend the training to discuss national issues and future plans.

Chapter 20 — **EXHIBITS**

[20-1 — Training Nomination and Authorization \(SSA-352, formerly HHS-350\)](#)

[20-2 — On-the-Job Training Guide](#)

[20-3 — Statement of Experience and Training](#)

DEPARTMENT OF HEALTH AND HUMAN SERVICES TRAINING NOMINATION AND AUTHORIZATION	IMPORTANT NOTICE 1. Form is to be typed or printed clearly. 2. Guidance for completion and code definitions are contained on reverse of Parts 7 thru 10. 3. Note Continued Service Agreement on back of this page; sign if applicable.	1. Transaction Number (z-7) <div style="font-size: 24pt; font-weight: bold;">233921 A</div>
--	--	--

SECTION A TRAINEE DATA					
2. Social Sec. No. (8-16)	3. Last Name (17-32)	First (33-42)	Initial (43)	4. Organization (Agency, Bureau, Off., Div., Br.)	
5. Pay Plan-Series-Grade	6. Type Appointment	7. Position Title		8. Continuous Service	
				YEARS	MONTHS
10. Home Address:				9. Hrs. of Prior Non-Gov't Training	
				11. Office Phone ()	

SECTION B COURSE DATA						
12. Training Hours:		A. Duty		B. Non Duty		
(82-85)	(86-89)					
14. Costs (\$ only)			13. Training Period: MMDDYY			
			From: (80-83) To: (86-71)			
A. Tuition & Fees (72)		B. Books & Other (76)	C. Travel (80)	D. Per Diem (84)	E. Other Trans. (88)	F. Total (92)
HEW (72-96)						
Employee (97-121)	(97)	(104)	(105)	(109)	(113)	(117)
15. Training Course Title (Do not exceed 45 letters) (122-166)						
16. Describe employee's training need and relate to official duties						
17. Describe how course content relates to item 16 above:						

18. Name & Address to Send Payment (167-201)				Attn:	
Address				ZIP (202-206)	
19. Location of Training-Name (207-241)				ZIP (242-246)	
Address					
20. Coding (See Instructions. Insert appropriate number in box)		A. Purpose (247)	B. Type (248)	C. Source (249)	D. Special Int. Program (250)
		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
				21. Self-sponsored (See Inst.) (251)	22. Skill Code (252-256)
				<input type="checkbox"/>	<input type="checkbox"/>

SECTION C FISCAL DATA			
23. Accounting Data (Appropriation, Allotment, CAN, Class)		24. SIBAC	25. Funds are available
			SIGNATURE
			Date

SECTION D CLEARANCE ACTION				
TYPED NAME & TITLE	(PHONE)	SIGNATURE	DATE	COMMENTS
26. Initiating Supervisor				
27. Concurring Official				
28. Concurring Official				
29. Approving Official				
30. Reviewing Emp. Dev. Spec.				
31. Authorizing Official				
				32. SPO CODE (258-261) (TYPED)

SECTION E PROCUREMENT DATA

Reference your catalogue, please furnish the services mentioned in item 15 above on the terms specified on both sides of the Vendor's Copy of this order, and on the attached sheets if any, including delivery as indicated. This purchase is negotiated under authority of 41 USC 252 (c) (3) or (5).

33. Send Invoice To:	34. Address Correspondence Regarding This Order To:		
	Name	Title	Phone
	Address		
	35. Signature of Purchasing Official		



On-the-Job Training Guide

The purpose of this On-the-Job Training (OJT) Guide is to establish On-the-Job Training/Mentor Programs that will standardize procedures for training newly hired Special Agents (SA) working under Special Agents-in-Charge (SAC) in the Office of Investigations (OI). This program will accomplish the following:

1. Improve the professionalism and competence of SA personnel.
2. Ensure that SAs receive training in all aspects of OI.
3. Supplement formal basic training received at the Federal Law Enforcement Training Center (FLETC), Glynco, Georgia, and the Social Security Administration (SSA) Training Center, Baltimore, Maryland.

The provisions of this guide are applicable to all managers, supervisors, mentors, and SAs during the first year an SA is employed by OI. This includes experienced 1811 criminal investigators who transfer to SSA Office of the Inspector General (OIG) from other Federal agencies.

The overall objective of the OJT Program is to produce self-sustaining, competent, professional SAs. Successful attainment of this objective is directly related to the efforts put forth by the SA, mentor, supervisor, and the support provided by higher-level management.

An SA will begin formalized training at FLETC as soon as possible after entry on duty. Trainees must successfully complete basic formal training during the first year. The OJT Program will continue for 12 calendar months from the date of entry on duty.

There is no specific order established for the type of training to be provided during the OJT Program. Priorities should be established that are consistent with the particular type of operation being conducted in the office.

SUPERVISOR'S RESPONSIBILITIES

At a minimum the mentor should be a journeyman GS-12 SA, and preferably a GS-13. Ideally, the mentor would have one trainee, although this may not always be possible.

Mentors may be rotated as necessary to provide adequate guidance to the employee and to assure the mentor maintains reasonable caseload production. The rotation will provide the trainee with exposure to different skills and expertise of various journeymen investigators within an office or division.

The program for training should be tailored to the experience level of the employee. The intent is to provide an avenue to strengthen areas of weakness in employees with other agency experience, as well as provide a broad base of instruction and experience for new hires

The supervisor will formulate plans with the mentor for further instruction of the trainee to correct deficiencies and weaknesses identified at file reviews.

Exhibit 20-2

MENTOR'S RESPONSIBILITIES

The primary responsibility of the mentor is to provide instruction to train the new SA to perform the tasks on the New Agent/Mentoring Checklist (attached). The training cycle, however, also entails evaluation and counseling if effective instruction is to take place.

Maintain frequent personal contact and communication with the trainee and supervisor.

Observe and evaluate the trainee's performance of each planned OJT task, and apprise the trainee of his or her strengths and weaknesses.

Regularly advise the supervisor of the trainee's progress and accomplishments.

Guide the trainee through the OJT task standards. Some employees will progress faster than others. The program is intended to be a learning experience.

TRAINEE'S RESPONSIBILITIES (FOR NEW 1811s)

Become thoroughly familiar with the OJT Guide and the New Agent/Mentoring Checklist.

Follow instructions of the supervisor and mentor and ask for clarification of any directions not fully understood.

Apply the knowledge gained in formal training to on-the-job situations.

Accept the constructive criticism and suggestions for improvement given during the OJT Program.

Flexibility is necessary as OJT assignments may vary. Training assignments will depend upon the caseload and the needs of the Field Division.

GUIDELINES FOR TRAINEES

Flexibility and initiative are the keys to quality OJT, which must be tailored to the needs of the trainee. Each trainee has an individual background of experiences and abilities. Some will need a great deal of guidance, while others will require only minimal guidance. This program is designed with every intention of allowing the trainee's immediate supervisor a free hand in developing the trainee to the full professional level of performance.

In order to assist the trainee in reaching the full level of performance, the supervisor and mentor will use the OJT Task Guide. The OJT Task Guide defines the tasks and objectives expected to be performed before an SA reaches the full professional level. OI recognizes that some offices may not have the varied day-to-day investigative activity that others have. Thus, some tasks may be impossible to perform either directly or indirectly. In such cases, management will take this into consideration and will attempt to include the trainee in those tasks as the investigative activity occurs.

Exhibit 20-2

GUIDELINES FOR 1811s WHO TRANSFER TO SSA OIG

SSA OIG recognizes and values the knowledge and skills that experienced 1811 criminal investigators bring with them when they transfer to OI. The OJT/Mentoring Program is also designed to build on investigative knowledge and acquired skills.

It is essential that all agents become familiar with the policies and procedures listed in Part I of the New Agent/Mentoring Checklist. Experienced agents will see that many of the policies are consistent with those of their previous agency. However, OI procedures may vary from those practiced by other Federal agencies. It is incumbent on the new agent to learn where to find OI policies and to review OI procedures. The checklist is used to record this activity, just as it is for an agent trainee.

The activities listed in Part II of the checklist will include activities in which experienced 1811 criminal investigators will have participated during their past employment. The new agent and SAC or other supervisor will review the activities. Together, they will decide which activities the agent will not have to complete based on prior experience; for instance, Observe an Interview, Visit an Office of a United States Attorney, or Present a Case to a Grand Jury. A notation should be made on the checklist to indicate that the activity has been completed based on previous employment.

RECORD KEEPING

The OJT Task Guide is kept in the possession of the new SA, who is responsible for ensuring that each task accomplished is properly recorded. The agent's mentor and SAC can ask to review the guide at any time. The guide must be presented to the mentor or SAC upon request.

SAs who transfer to SSA OIG from other Federal agencies are required to maintain the log for their first year of employment with the OIG. New agents who have not met the requirements for a "career" appointment status must keep possession of the guide until they are no longer considered "career conditional" employees.

The guide may be destroyed one year after becoming employed by the OIG, or when "career" status is achieved, in the case of "career conditional" employees. At a minimum, the guide must be maintained for a one-year period.



Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

NEW AGENT/MENTORING CHECKLIST

Name of Agent: _____

Field Division (and Office): _____

GS Level: _____

- Check One:**
- Entered on Duty as a New Federal Criminal Investigator**
 - Transferred to the SSA OIG from Another Federal Agency as a Trained Criminal Investigator**

Number of Years of Prior Federal Law Enforcement Experience: _____

Agent Mentor: _____

Agent Supervisor: _____

Agent Mentor OJT Plan Term: (From) _____ (To) _____
(1 Year Period)

Exhibit 20-2

PART I (Supervisory Oversight)

DESCRIPTION OF ACTIVITY PART I – POLICY COVERAGE (To be Conducted by Supervisor)	DATE OF OCCURRENCE	AGENT’S INITIALS	SUPERVISOR’S INITIALS
<i>Special Agent Handbook Certification (SAH Chapter 1)</i>			
Employee Conduct (APPM Chapter 7)			
Ethical Conduct (SAH Chapter 2)			
Use of Government Vehicles (SAH Chapter 2) & (APPM 7-40)			
Home-to-Work Driving Authority (SAH Chapter 2)			
Use of Sirens/Lights (SAH Chapter 2 – 060-J-5)			
Reporting of Accidents (APPM 4-50 & APPM 7-40)			
Physical Fitness (SAH Chapter 22.0-10)			
Use of Force Policy (SAH – Chapter 21)			
Firearms Policy (SAH Chapter 21)			
Firearms Qualifications (SAH Chapter 21)			
Report of Shooting Incident (SAH Chapter 21)			
Undercover Operations/Informants (SAH Chapters 7, 9, 17.05)			
A G Guidelines – Informants (Search ERC – “Confidential Informants”)			
Electronic Surveillance (SAH Chapter 8)			
Investigative Reports Review (SAH Chapter 11 – See Investigative Checklist)			
Interviewing Policy (SAH Chapter 10)			
Protecting Identity of Complainants (SAH Chapter 4)			
External Speeches (APPM 8-00-20)			
Congressional Inquiries (SAH Chapter 2)			
News Media Policy (SAH Chapter 2)			
Outside Activities (SAH Chapter 2)			
Local and Temporary Travel (APPM 03-80 & 06-00)			

Exhibit 20-2

PART I (Continued)	DATE OF OCCURRENCE	AGENT'S INITIALS	SUPERVISOR'S INITIALS
Disclosure of Information <i>(SAH Chapter 2 & APPM 13)</i>			
SSA Record Access and Disclosure <i>(SAH Chapter 6)</i>			
Grand Jury Information <i>(SAH Chapter 14)</i>			
Case Reviews <i>(SAH Chapter 3)</i>			
Acquisition, Preservation & Management of Evidence <i>(SAH Chapter 14)</i>			
General Office Security <i>(APPM 12)</i>			
Loss of Property <i>(APPM 4-50)</i>			
Use of Privately Owned Software <i>(APPM 12-00-07)</i>			
Law Enforcement Availability Pay <i>(SAH Chapter 2)</i>			
24 Hour Availability <i>(SAH Chapter 2-080)</i>			
Confidential Financial Disclosure <i>(APPM 09-00-20-30)</i>			
Use of Government Issued Travel Cards <i>(APPM 7-70)</i>			
Leave Advances <i>(APPM Future)</i>			
Use of Government Issued Phone Cards <i>(APPM Future)</i>			
Use of GSA Gasoline Cards <i>(APPM Future)</i>			

Note: Blank Rows Provided for Inclusion of Additional and/or Specialized Training Items.

* SAH References the SSA OIG OI *Special Agent Handbook*

**APPM References the SSA OIG OI *Administrative Policies and Procedures Manual*

Exhibit 20-2

DESCRIPTION OF ACTIVITY PART II – ON-THE-JOB TRAINING THROUGH MENTOR FACILITATION (To be completed by Mentor and reviewed by Supervisor)	DATE OF OCCURRENCE	AGENT'S INITIALS	SUPERVISOR'S INITIALS
Review of OI Case Files (to familiarize)			
Review Allegation Process (to familiarize)			
Visit SSA Local Field Office			

Review an SSA Claims Folder for Evidence			
Obtain an SSA/MCS AACT or FACT Query for an Investigation (Title II)			
Obtain an SSA/MCS SSID Query for an Investigation (Title XVI)			
Obtain an SSA/MCS Numident Query for an Investigation			
Obtain an SSA/MCS Alphadent for an Investigation			
Obtain an SSA/MCS SEQY or DEQY Query for an Investigation			
Obtain a Consolidated Query in SSA/MCS for an Investigation			
Run a Misc Query in SSA/MCS to Identify Bank Routing Information			
Obtain an SSA/MCS PHUS Query for an Investigation			
Process Title II and XVI Check Photocopy Request			
Submit a Request for a Form SS-5			
Process SRAD IT Request			

Demonstrate Proper Usage of OI Radio Equipment			
Become Familiar with Technical Investigative Equipment			
Draft a Request to Conduct a Consensual Monitoring			
Record a Consensual Telephone Call			
Participate in a Surveillance			
Participate in the Execution of a Search Warrant			
Participate in the Execution of an Arrest Warrant			



Office of the Inspector General

SOCIAL SECURITY ADMINISTRATION

STATEMENT OF EXPERIENCE AND TRAINING

Experience

1. **Employer/Agency:** _____
Position Held: _____
Dates of Employment: _____

Describe how you gained experience in each of these areas and give examples if applicable.

Interviewing:

Report Writing:

Conducting Investigations:

Legal Training:

Firearms:

Defensive Tactics/Arrest Techniques:

2. **Employer/Agency:** _____
Position Held: _____
Dates of Employment: _____

Describe how you gained experience in each of these areas and give examples if applicable.

Interviewing:

Report Writing:

Conducting Investigations:

Legal Training:

Firearms:

Defensive Tactics/Arrest Techniques:

Exhibit 20-3

3. **Employer/Agency:** _____
Position Held: _____
Dates of Employment: _____

Describe how you gained experience in each of these areas and give examples if applicable.

Interviewing:

Report Writing:

Conducting Investigations:

Legal Training:

Firearms:

Defensive Tactics/Arrest Techniques:

Training

	Course/Program Name	Dates/Location	# Hours	Degree/Certification
Interviewing				
Report Writing				
Conducting Investigations				
Legal Training				
Firearms				
Defensive Tactics/Arrest Techniques				

FIREARMS POLICY AND TRAINING

021.000 Authority to Carry Firearms

- A.** The Homeland Security Act of 2002 provides in part that the Attorney General may grant certain law enforcement authority to the various Federal Offices of Inspectors General (OIGs), including SSA OIG. Under this authority, agents of the Office of Investigations (OI) may, under prescribed conditions, carry firearms, make arrests without warrants, and execute arrest or search warrants (*see [Chapter 1](#) for more information*).
- B.** The OIG Training Program Manager (TPM) at OI Headquarters (HQ) serves as the program manager to ensure that firearms, fitness, and use-of-force training is accomplished in accordance with OI policy and the requirements listed in the Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority.

021.010 General Conduct

- A.** SAs are responsible for the safe handling and use of OI-issued firearms, personally owned firearms carried as back-up weapons, less-than-lethal weapons, and other safety-related equipment at all times. In addition, SAs are responsible for the safe handling, storage, and disposition of any firearm or other weapon seized or otherwise acquired by them while they are engaged in the performance of their official duties.
- B.** The Transportation Security Administration (TSA) enforces a strict regulation, [49 CFR § 1544.219](#), concerning the transportation of firearms on commercial aircraft. That portion of the regulation that applies to Federal law enforcement officers/agents requires that such officers/agents authorized to carry firearms while traveling on official business properly identify themselves to appropriate airline personnel and file the necessary forms. It is mandatory that all SAs comply with this regulation and that they understand that they may be denied access to the scheduled flight at the discretion of the flight commander or captain. Therefore, in situations that require the time-sensitive presence of the traveling SA, such as assistance with the service/execution of search and/or arrest warrants, travel should be planned to allow for such unanticipated events.
- C.** Subject to the authorized exceptions cited in Section [002.050G](#), SAs are prohibited from consuming alcoholic beverages while carrying firearms.
- D.** For each law enforcement officer traveling armed, the air carrier will review the law enforcement officer's badge and credential to ensure that the badge and credential are issued by the same

agency, and the name on the credential matches the name on the travel authorization. **NOTE:** Agents are reminded to carry a copy of their travel authorization.

021.020 **Carrying Issued Weapons**

- A.** SAs will carry issued handguns on their person, in agency-issued or SAC-approved holsters. Extra ammunition (at least one fully loaded magazine) and other approved equipment (including but not limited to handcuffs, baton, Oleoresin Capsicum (OC) aerosol, and radio) will be carried as appropriate. Except when involved in an approved undercover work assignment, the SA is required to have his/her badge and credentials on his/her person when carrying a firearm.
1. Agents may request permission to use a non-agency-issued holster for duty-carry. Agents must prepare a memorandum requesting approval to deviate from agency-issued equipment. The memorandum must include a detailed description and photograph of the holster that the agent is requesting to use for duty carry. The memorandum must be approved by the SAC and forwarded to the OIG Training Program Manager (TMP) at OIG Headquarters.
 2. Additionally, agents must successfully qualify with their holster prior to use for duty-carry.
 3. Holsters that utilize a trigger finger lock are not approved for duty-carry.
- B.** The current Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority grants the authority to an Inspector General to allow off-duty agents to carry firearms for either operational or safety reasons. SSA OIG agents were granted the authority to carry their issued firearm off duty by their Inspector General. **Personally owned firearms cannot be carried under this authority.** Should agents elect to carry a firearm other than the issued firearm while off duty, they would do so outside of the authorities granted by the Attorney General and Inspector General. Instead, they would be acting as private citizens under relevant Federal, State, and local law, including the Law Enforcement Officers Safety Act of 2004 (LEOSA). The responsibility of deciding the reason why an issued firearm should be carried off duty rests with the agent. If the agent elects to carry an issued firearm while in an off-duty status, all laws, regulations, and OIG policies governing the use and handling of a firearm while on duty shall apply, including the following:
1. Special Agents are personally responsible for the security of their OIG-issued firearm.
 2. Special Agents must carry OIG official credentials at all times when they carry issued firearms.
 3. Special Agents may not consume or be under the influence of alcoholic beverages when carrying a firearm off duty.
 4. Except while traveling aboard a commercial airline, Special Agents must carry their issued firearm in a holster on their person. The carrying of an issued firearm in a briefcase, backpack, or other like container is contrary to OIG policy.
 5. Special Agents shall adhere to TSA regulations regarding the carrying, checking, and stowing of a firearm while traveling on a commercial airline.
 6. Special Agents must exercise discretion when putting on, carrying, and removing firearms to ensure that there is no unnecessary display to the public.

7. Avoid unnecessary references to the fact that a Special Agent is carrying a firearm.
 8. Special Agents are required to utilize OIG-issued locking devices when they are not in immediate control of their firearm, such as instances when their issued weapon is stored at home.
 9. Special Agents must not leave firearms unattended in a hotel room or automobile. (See 021.030 for exceptions for shotguns.)
 10. Issued firearms must be secured with a locking device in the agent's home while not on his or her person.
- C. The duty-related use of any OI-issued weapon shall be in accordance with the guidelines issued by the Department of Justice (DOJ) dated July 1, 2004 (*see Special Agent Handbook - Appendix III*). General Principles of the Department of Justice Use of Deadly Force Policy are found in chapter 24 of this Handbook.
- D. SAs are not authorized to carry weapons outside of the United States on official business unless approved in advance by the Assistant Inspector General for Investigations (AIGI), the State Department, and the host country.
- E. Each SA is responsible for the general care and maintenance of his/her issued firearm. No modifications may be made to any firearm. The Field Division (FD) Firearms Coordinator should return any weapon in need of repair to the manufacturer.
- F. Firearms and ammunition requiring storage will be stored in a secure room or in a GSA-approved Class 5 security container. In small offices, a file cabinet with a lock-bar security system and a combination lock will suffice. Each SA assigned a firearm is responsible for exercising the highest degree of care to prevent its theft or loss.
- G. Agents may request permission to change the stock pistol grips on their issued SIG Sauer duty weapon to improve proficiency. Agents must prepare an office memorandum delineating their reason for the request. The office memorandum must be approved by your SAC then forwarded to the Training Program at Headquarters (HQ) for final approval.

Once approval is received, the change must be made on an empty weapon at the range prior to firing the pistol. An Agency qualified firearm instructor must check the pistol prior to firing to assure that the grip adapter does not interfere with the safe and efficient operation of the pistol in any way.

Slip-on grip adapters are not considered a modification and, therefore, do not require HQ approval; however, care should be taken to assure that the adapter does not interfere with the safe and efficient operation of the weapon.

021.025 Carrying of Backup Weapons

- A. The purpose of a backup firearm is for the agent to have access to a second firearm to use in case the agent's issued firearm malfunctions or becomes inaccessible to the agent. A back-up weapon is to be used primarily for close in protection.

- B. Backup firearms can be either a semiautomatic pistol or a revolver manufactured by Beretta, Browning, Colt, Glock, Heckler and Koch, Kahr, Ruger, Sigarms, Smith and Wesson, Taurus, Walther, Bersa Thunder or Rossi; in .380 caliber or larger.
- C. Agents may request permission to carry a back-up handgun while on official duty by submitting a memorandum to their Special Agent-in-Charge providing the following:
1. Detailed information describing the particular firearm the agent is requesting to carry - make, model, serial number, and caliber.
 2. State how the firearm will be carried (ankle holster, belt holster, under the arm holster, etc.)
 3. Certify that he/she has qualified with the firearm on OI's prescribed course for back-up weapons. The date the agent qualified must be in the request. *Note: Qualification training must be conducted by an OI firearms instructor.*
 4. Indicate that the agent understands that if he/she fails to qualify with the firearm, the agent must immediately stop carrying the firearm on duty until he/she qualifies with the firearm.
 5. Acknowledge that the agent accepts all responsibility for maintenance of the firearm and purchasing of ammunition for training and carrying. The OIG will be absolved of any liability if the agent's personally owned weapon fails to fire when the agent attempts to use it or if the agent is injured while shooting the firearm while attempting to qualify with the weapon.
 6. A statement that the agent will not carry the back-up firearm in lieu of his/her issued firearm and will only use the back-up firearm when his/her issued firearm malfunctions or is inaccessible.
- D. The agent's Special Agent-in-Charge (SAC) has the option of approving or disapproving the request. If the request is approved, file the memorandum bearing the SAC's signature in the agent's 7B extension file, and forward a scanned copy of the memorandum to the OIG TPM at OIG Headquarters. The agent should be given a copy of the approval for his/her records.

021.030 Use of Shotguns

- A. Shotguns are assigned for use on a case-by-case basis. Agents seeking to carry shotguns during any operational activity must obtain permission from their SAC, ASAC, or RAC. Agents must be current in their training with a shotgun in order to carry the weapon for operational purposes. To be current, the agent must have qualified with the weapon during the current quarter or the quarter immediately preceding the current quarter. The shotgun course is found in the OI Trainers' Handbook. A score of 70% is required in order to qualify.
- B. Shotgun familiarization is mandatory and this training must be conducted twice each fiscal year. Targets are not scored during the familiarization training. Those seeking familiarization only are required to fire ten rounds.

- C. Each office shall maintain a sign-out log for shotguns ([Exhibit 21-1](#)). The log must include the date; name of the agent requesting to use the shotgun; serial number of the shotgun; type and number of rounds taken; name of the supervisor authorizing the use of the weapon; and the reason for the use (case number, training, etc.). The log should be annotated to show the date and time the shotgun is returned to the office.
- D. Shotguns shall be stored unloaded in an office safe or gun locker when they are not being used for operational or training purposes.
- E. Ordinarily, shotguns will not be left unattended in a vehicle. If circumstances arise that require SAs to temporarily store the weapon in a vehicle used for official use, the shotgun may be locked in the trunk or storage area of an SUV.
- F. Temporary storage would include securing the shotgun in the trunk of a government vehicle during a search warrant or other official operation. The shotgun must be removed from the trunk as soon as possible and secured at the office. Temporary storage does not include storing the shotgun in the trunk of a vehicle overnight.

021.040 Firearms Inventory Control and Safekeeping

- A. The complete inventory of OI-issued firearms is included in the OIG’s Property Management System. Each SAC will maintain a local record of all firearms assigned to his/her division. The SAC will conduct a yearly inventory of all firearms and other accountable law enforcement equipment.
- B. Firearms shall not be left unattended unless secured. Each SA to whom a firearm is issued or has been approved to carry a back-up firearm will maintain control and custody of that firearm(s) at all times
 - 1. Firearms and/or ammunition shall not be stored in any unlocked desk or cabinet.
 - 2. Firearms will be loaded and/or unloaded only in designated safe areas, with the muzzle pointed in a safe direction. A safe direction is one which, in the event of an accidental discharge, would preclude the loss of life or serious injury and minimize damage to property.
 - 3. When an SA is transferred to another FD or other assignment within SSA OIG, his/her issued firearm will be transferred with him/her.
- C. All Office of Investigations firearms will be purchased centrally by OIG HQ.
- D. Procedures for reporting lost firearms are found in Section [021.090](#) D.

021.050 Types of Firearms and Ammunition

- A. Standards
 - 1. The standard OI-issued handgun for SAs is the SIG-Sauer, .357 caliber semi-automatic pistol, Model P229 or P239.

2. No secondary or back-up firearm(s) may be carried at any time unless use of the firearm has been approved (see section [021.025](#)).
 3. Any exception to the handgun standards set forth in this policy must be requested in writing to the AIGI. Approvals will be in writing and will only be valid for a specific period of time. This includes undercover operations.
- B.** No personally owned handguns shall be carried while on duty unless authorized for use during an approved undercover operation or approved as a back-up firearm (in such instances, the SA shall have demonstrated the ability to qualify with that firearm on an OI-approved course of fire).
- C.** No automatic weapons of any type are authorized.
- D.** Ammunition
1. With the exception of ammunition for back-up weapons, all ammunition will be purchased by PAD in HQ. The amount purchased will be determined by the Training Program Manager (TPM) and will be dependent upon:
 - a. Current inventory for each type of ammunition;
 - b. Duty, qualification, and training needs for the current and following fiscal year; and
 - c. Individual range requirements (e.g. requirement to use frangible ammunition).
 2. Generally, ammunition used for qualification will be service ammunition. An exception will be made for ranges that only permit the use of lead-free and/or frangible ammunition
 3. The duty ammunition carried by the SA will be expended at the time of qualification and/or training, if permitted by the range, and fresh ammunition will be issued.
 4. The Firearms Instructors (FI) are responsible for assuring that the amount of ammunition issued for training is commensurate with the amount of ammunition required to complete that session's training and for fresh duty carry.
 5. Hand-loaded, reloaded, or remanufactured ammunition is not authorized. The only ammunition authorized for use is the ammunition purchased, provided by and/or approved by OI HQ.
 6. SAs are responsible for purchasing ammunition for non-OI issued firearms approved as back-up weapons. The use of official funds to purchase ammunition for any non-OI issued firearms is prohibited.
 7. On an annual basis, PAD will distribute or coordinate the distribution to the Field Divisions the amount of ammunition necessary to cover their duty, qualification, and training needs for the remainder of the current and following fiscal years.

- a. The amount dispersed will be determined by the TPM and based upon the requirements in 021.050.1 above.
 - b. If additional ammunition is needed at any time, the Field Division will provide a written request, including a justification for the request, to the TPM. This request must be received by the TPM at least two weeks prior to the event causing the additional need for ammunition.
8. Each office will maintain an inventory of its ammunition by completing the ammunition inventory screen in MetaStorm.
 - a. Use of the Ammunition Inventory System in MetaStorm is mandatory; no other forms are acceptable.
 - b. An individual, separate entry is required on the ammunition inventory screen each time ammunition is removed from inventory and each time ammunition is placed into inventory.
9. Each Field Division is responsible for designating one ammunition Point of Contact (POC), as well as a Point of Contact for every Field Office that maintains an ammunition inventory. The POCs (both at the Field Division and Office level) will certify the amount of ammunition maintained in their Field Divisions on a quarterly basis by performing a physical count of all ammunition and reconciling that count with the Ammunition Inventory System in Metastorm.
 - a. Field Office Point of Contact – this role allows the designated individual to enter ammunition information into the inventory system for their office
 - b. Field Division Point of Contact – this role allows the designated individual to enter information into the inventory system for the entire field division
 - c. On a quarterly basis, the TPM will perform a national review of the ammunition inventory. If the TPM determines that an office possesses more ammunition than needed, that office will be directed to either return the excess ammunition to PAD or transfer it to an office in need of additional ammunition.
 - d. On a semi-annual basis, the SAC will verify to the DAIGI, in writing, the amount of ammunition that exists in his/her field division and that a physical accounting of all ammunition has been completed and that the physical count has been reconciled with the Ammunition Inventory System. This verification will be completed in April and October, at the same time as the semi-annual property verification.

E. Emergency Situations

In emergency or life-threatening situations where prior approval is not practical, the SA is authorized to use any firearm or ammunition that is immediately available.

021.060 **Basic Firearms Training**

- A. Newly appointed SAs, or those transferred into positions requiring the use of firearms, shall not be issued firearms until they have successfully completed basic firearms and other use-of-force training.
- B. Basic firearms training shall consist of that provided during the Criminal Investigator Training Program at FLETC, or comparable training provided or approved by the AIGI or his/her designee.
- C. Firearms training requirements are found in the *OI Trainers' Handbook*.

021.070 **Firearms Instructors**

- A. OI SAs will serve as firearms instructors. The instructors will successfully complete firearms instructor training at FLETC or other firearms instructor training course(s) approved by the AIGI or his/her designee.
- B. Firearms instructors must be recertified every three to five years. Recertification standards are developed by OI and coordinated by the TPM.
- C. The firearms instructor will maintain a file of quarterly firearms qualification scores and any applicable certifications attained by the SAs whom he/she monitors. The firearms instructor will ensure that those scores are entered into the Training database.
- D. Firearms instructors will inspect the weapon of any agent who experiences a malfunction during firearms training. Any weapon determined by a firearms instructor to be unserviceable must be withdrawn from service and returned to the manufacturer for repair. Replacement firearms will be issued from FD inventories.
- F. Instructors are encouraged to enroll in professional organizations (e.g., the International Association of Law Enforcement Firearms Instructors [IALEFI]) and to attend available regional and/or national conferences offered by those organizations.
- G. Instructors are appointed or removed at the discretion of the SAC, DAIGI, or AIGI.
- H. Instructors are responsible for keeping track of the inventory of ammunition assigned to their office by completing form OI-74 when ammunition is issued or used for training.

021.080 **Firearms Qualification Standards**

- A. Supervisors must afford SAs authorized to carry firearms the opportunity to shoot during work hours in order to maintain their proficiency. All shooting using issued firearms and ammunition on Government time must be supervised by a qualified firearms instructor from OI or another Federal law enforcement agency.
- B. Each SA is required to qualify quarterly with his/her issued firearm and to successfully participate in practical judgmental and/or tactical exercises including but not limited to yearly qualification

on an approved, reduced light course of fire. Courses of fire used by OI will be selected from a listing of training materials/courses of fire approved by the TPM, with the concurrence of the AIGI and DAIGI. (Detailed instructions are found in the *OI Trainers' Handbook*.)

- C.** Each SA will be given a maximum of three attempts to fire a qualifying score on an OI-approved practical pistol course (PPC). Intervening practice may be allowed, but must be identified as such and will not mirror the qualification course of fire selected for the exercise. The minimum qualification score on any OI-approved course of fire will be 70 percent. No course of fire will be graded on a pass/fail basis for qualification purposes.
- D.** The Field Division firearms instructor will report all failures to qualify to the SAC as soon as possible following the close of the scheduled training session. Any SA who fails to achieve a qualifying score as required will not be authorized to carry a firearm. As soon as possible, special and/or remedial training will be provided to assist any shooter unable to qualify. After the completion of this training, the SA will distinguish further attempts to qualify from subsequent “practices.”
- E.** Any SA who is unable to qualify because of medical and/or physical limitations will be prohibited from carrying firearms and from engaging in any hazardous duty that might require the use of firearms.
- F.** SAs are required to use issued or approved holsters at all times for issued firearms. For normal duty, only strong-side hip holsters are permitted. No ankle, shoulder, cross-draw, or fanny-pack holsters are permitted under normal duty conditions. On a case-by-case basis, the SAC may authorize the use of another holster to fit a specific mission requirement. The SA authorized to carry an alternative holster must demonstrate the ability to use it safely and proficiently.
- G.** Every SA who is authorized to carry a firearm must participate in a scheduled firearms training session at least once per quarter. Any SA who fails to comply with this requirement shall provide a memorandum of explanation to his/her SAC detailing such failure to comply. Unjustified absences from scheduled firearms training for two consecutive quarters, or failure to qualify for two consecutive quarters shall result in the SA’s surrender of his/her agency-issued weapon as well as potential suspension of or removal from law enforcement availability pay status, until such time as the SA is able to requalify with his/her issued firearm. An agent who has surrendered his/her agency-issued weapon is prohibited from carrying a back-up weapon until reinstated.
- H.** Every SA who has been authorized to carry an approved back-up firearm shall complete the official agency back-up qualification course before carrying that firearm on official duty. Once the initial qualification has been completed, the SA shall be required to qualify at a minimum of one quarter each year and complete the back-up familiarization course of fire the other three quarters within the same year. Any SA who fails to comply with this requirements shall provide a memorandum of explanation to his/her SAC detailing such failure to comply and will not be approved to carry their back-up firearm until they complete the required qualification.
- I.** If the SA is unable to participate in the back-up familiarization course for one quarter, that SA shall be require to provide a memorandum of explanation to his/her SAC detailing the reason they were unable to participate in the back-up familiarization. Failure to participate in the back-up firearm familiarization course for two consecutive quarters shall result in the SA’s authority to carry the back-up firearm being rescinded until such time the SA completes the full back-up weapons qualification course.

- J.** If the SA decides to no longer carry a back-up firearm, that SA shall provide a memorandum to his/her SAC documenting that they will no longer carry a back-up firearm. If that SA wishes to carry a back-up firearm in the future, that SA must submit a new memorandum to his/her SAC requesting approval to carry a back-up firearm and complete the back-up firearms qualification course prior to carrying the back-up firearm while on duty.
- K.** If the SA decides to carry a different firearm other than from the approved list of authorized back-up firearms, he/she must submit the appropriate memorandum and complete the back-up firearms qualification prior to carrying that firearm while on duty.

021.090 Weapons Issuance and Security

- A.** FDs issue and assign firearms, handcuffs, ammunition, and related protective equipment such as expandable batons and OC aerosols.
- B.** The SAC will ensure that all unassigned firearms and ammunition are stored in a locked and secure area.
- C.** The SAC must immediately inform a DAIGI or AIGI when a firearm is missing or otherwise unaccounted for during any announced or unannounced weapons inventory.
- D.** SAs shall report immediately the loss or theft of an issued firearm or other weapon to their supervisor, who in turn reports to the AIGI or DAIGI through the SAC. This oral report shall be followed by a written report within 24 hours. The supervisor will forward the original report via the chain-of-command to the AIGI, with a copy to the SAC, who will ensure that the loss is reported to the National Crime Information Center (NCIC).
- E.** Under the direction of the AIGI, an administrative inquiry will be conducted to determine the circumstances of the theft/loss of the firearm or other weapon. The AIGI, or his designee, will select the individuals to conduct the inquiry.

021.100 Permits to Carry Firearms

SAs who possess state, county, and/or local police department permits to carry firearms are advised that such permits will not be recognized, in any way, as authorization to carry weapons while performing their official duties. Further, SAs are not authorized to carry agency-issued firearms off duty under the color of a state, county, or local “permit to carry.”

021.110 Report of Shooting Incident

- A.** SAs must immediately report any shooting incident involving OI personnel to the SAC or, in his/her absence, the ranking supervisor.
- B.** Instructions on the reporting of shooting incidents are found in chapter 24 of this Handbook.

Chapter 21 — **EXHIBITS**

[21-1 — Shotgun Sign-Out Log](#)

OCCUPATIONAL HEALTH AND WELLNESS

022.000 **General Policy**

- A. The occupational health and health enhancement programs for agents of the Social Security Administration (SSA) Office of the Inspector General (OIG) have three distinct elements: (1) the Mandatory Physical Examination Program, (2) the Exposure Control Plan (ECP), and (3) the Health Enhancement Program (HEP). The Training Program Manager (TPM) oversees the OIG occupational health and health enhancement programs.
1. **Mandatory Physical Examination:** The Mandatory Physical Examination is a medical/physical evaluation performed under contract with the Division of Federal Occupational Health (DFOH). The first step of the process is a medical examination performed at a U.S. Public Health Service (PHS) facility. The results of the examination and the reports from the laboratory tests are reviewed by a Medical Reviewing Officer (MRO). The MRO prepares a written statement based on the medical findings, which addresses the employee's ability to meet the medical requirements for the position held by the employee. (Physical requirements for OIG Agents are found in [Exhibit 22-1](#))
 2. **Exposure Control Plan:** ECP is a written plan designed to identify such things as: employees at risk to occupational exposure to bloodborne pathogen (BBP) hazards, the method of implementation of the Occupational Safety and Health Administration (OSHA) Bloodborne Pathogens Standard ([29 C.F.R. § 1910.1030](#)), and the procedures to be followed in the event of an exposure incident. (NOTE: A [copy of the ECP](#) can be found on the **(b) (7)(E)** Video on Demand (VOD) training pertaining to bloodborne pathogens is available through the video lending library at www.osha.gov.)
 3. **Health Enhancement Program:** Physical conditioning under the HEP is a process by which the employee performs certain activities in order to maintain or improve one's strength, stamina, agility, and overall wellness qualities. This program is voluntary, and participants may use up to three duty hours per week for participation in approved fitness activities. The physical fitness levels achieved, or maintained by the employee are measured by a process known as an assessment. The assessment provides a tool for the individual agent to compare his or her level of fitness against established sets of standards. The assessment must be performed prior to beginning the HEP and periodically thereafter. It is mandatory for participation in the HEP.

- B. All elements of the Occupational Health and the HEP require active participation by the employee and the employee's supervisor.

022.010 Physical Requirements and Medical Standards

- A. The SSA OIG has adopted the physical requirements and medical standards that were developed for criminal investigators based on the recommendations of the President's Council on Integrity and Efficiency (*Exhibit 22-1*). The council recommended the establishment of mandatory physical requirements and medical standards for applicants and incumbents in the criminal investigator job series for the Offices of Inspector General throughout the Federal Government.

The published report is referred to as the Model OIG Directive.

- B. The physical requirements listed in the Model OIG Directive should be considered during the review of the medical history and physical examination. They are not intended to be all encompassing nor are they meant to establish absolute requirements for criminal investigators. Rather, they are provided to aid the examining physician and SSA OIG management officials in determining what medical problems may hinder the ability of incumbents of the criminal investigator positions to satisfactorily perform the actual work without causing undue risk to themselves or others. They are also provided to ensure consistency in the application of these standards for applicants for employment as well as for current employees considered for assignment to criminal investigator positions.

022.020 Pre-Employment Physical Examinations

The SSA OIG requires that all criminal investigator applicants meet specific physical requirements and medical standards prior to being hired.

022.030 Informing Applicants of the Mandatory Physical Examination Program

- A. All applicants for the position of criminal investigator (Special Agent) positions are made aware of the conditions of employment in the form of the vacancy announcement. The announcement lists the medical and physical requirements for the series 1811 employee.
- B. All applicants selected will be required to undergo a pre-employment medical examination by an Agency-designated physician to determine if they are physically and mentally qualified to perform the full range of duties of the position. In addition, applicants must be informed that, if hired, they will be subject to periodic medical examinations for the purposes of assessing their fitness to retain the position.
- C. Any selectee who refuses to submit to the required examinations will not be considered for employment as a criminal investigator. SSA OIG personnel involved in the candidate interview process should make certain that these requirements are discussed with the candidate at the time of initial interview.

- D. Tentative selectee(s) will be required to submit to urinalysis to screen for illegal drug use prior to appointment unless currently an SSA employee occupying a position already in a random drug testing program. Appointment to the position is contingent upon a negative test result. After appointment, the employee will be included in the agency's random drug test program.

022.040 Scheduling Pre-Employment Physicals

After tentative selection, the applicant is scheduled for a pre-employment physical by the Office of Communications and Resource Management (OCRM). OCRM arranges for the PHS, Health and Human Services (HHS) to send the results of the completed examination to them.

022.050 Review by Public Health Service Medical Officer

The medical officer will review the results of the physical examination. Based on the review, the medical officer will make a recommendation and will submit a written memorandum to OCRM containing the results of the review and the recommendation of the medical officer.

022.060 Mandatory Periodic Physical Examinations

- A. SSA OIG agents will take mandatory periodic physical examinations to determine fitness for duty. The frequency of these examinations will be based solely on age and date of last physical. The general rules to follow for age are:

- Under 45 – Physical examinations will be taken every 3 years
 - 45 Plus – Physical examinations will be taken every 2 years

- B. Employees who refuse to submit to required periodic examinations will be subject to reassignment or appropriate disciplinary action.

022.070 Scheduling of Periodic Physical Examinations

OCRM will administer a national contract with the PHS, Federal Occupational Health (FOH) that provides physical examinations to SSA OIG agents. At the beginning of each fiscal year, OCRM will provide the Assistant Inspector General for Investigations (AIGI) with a list of all personnel required to complete a physical examination during the year. **PHYSICALS CANNOT BE SCHEDULED WITHOUT THE CONCURRENCE FROM OCRM.** The Office of Investigations (OI) will designate one staff person in Headquarters (HQ) and in each field division (FD) to contact PHS to schedule the examinations as required. Every effort will be made for an examination to be conducted at a PHS facility convenient to either an agent's work or home location. No examination should be scheduled during the fourth quarter of any fiscal year. Employees whose birthdays are in July, August, or September should be scheduled either the quarter immediately preceding or immediately following their birthday.

022.080

Reporting the Results of Periodic Physical Examinations

The contract health unit will forward the results of the physical examination to the PHS medical officer as stated in the contract. The medical officer will forward the results of the examination to the Personnel Officer, OIG, who will file the report in the employee's medical folder. Any recommendations for additional testing or follow-up will be brought to the attention of the AIGI.

022.090

Exposure Control Plan

- A. The Exposure Control Plan for Occupational Exposure to Bloodborne Pathogens has been developed for OIG in accordance with the Centers for Disease Control (CDC) guidelines and the OSHA BBPs Standard. (*A copy of the Exposure Control Plan is found on the OIG's* (b) (7)(E) *.)* The plan is designed to protect all OIG OI employees from occupational exposure to blood and other potentially infectious materials.
- B. The Special Agent-in-Charge (SAC) of the Criminal Investigations Division (CID) is responsible for ensuring that the Exposure Control Plan is available to all personnel and for the administration of the Plan for OI HQ. FD SACs are responsible for modifying the Plan to fit the local needs of personnel assigned to the FD.
- C. All employees who have been designated by the plan as at risk to possible exposure to BBPs and other potentially infectious materials are required to receive annual training to review the Exposure Control Plan for their office. Employees must be familiar with the following terms:
1. Bloodborne Pathogens – Bloodborne Pathogens (BBP) are defined as pathogenic microorganisms present in human blood that can cause disease in humans.
 2. Other Potentially Infectious Materials – Other potentially infectious materials are defined as other types of body fluids and tissues besides blood which are potentially infectious materials. The PHS considers it prudent to consider all bodily fluids as potentially infectious and recommends that care and appropriate protection be used when in contact with all bodily secretions.
 3. Engineering Controls – Engineering controls mean control measures that isolate or remove the BBPs from the workplace. These might include such things as special containers for disposal of contaminated needles or other products that may have come into contact with human blood.
 4. Exposure Incident – Exposure incident is defined as a specific contact of blood or other potentially infectious materials with an emphasis on eye, mouth, or other mucous membrane, non-intact skin, or by parenteral contact (i.e., by a puncture wound or cut with a contaminated object such as a hypodermic needle).
 5. Personal Protective Equipment – Personal protective equipment (PPE) are items the employee may use to prevent contamination by potentially infectious material. In the case

of BBPs, such PPE may include gloves, eye protection or face shields, masks covering the mouth, and protective clothing.

6. Universal Precautions – Universal precautions refer to both a mental attitude that all blood or bodily fluids are potentially hazardous along with safe work practices which minimize the risk of exposure to potentially infectious material.
- D. OIG shall make the hepatitis B vaccine and vaccination series available to all employees who face possible occupational exposure. These shots will be provided at no cost to the employee.

022.100 Office of the Inspector General Health Enhancement Program

- A. The primary goal of the SSA OIG Health Enhancement Program (HEP) and the Mandatory Fitness Assessment is to promote healthy behaviors, of which physical exercise is an integral component. Ideally, the Program benefits would include improved employee health, productivity, and decreased employee absenteeism, disability, and health care costs. The HEP and Mandatory Fitness Assessment Program is available to all employees in positions covered by Law Enforcement Officer retirement provisions as stated in Title 5, United States Code, Sections 8336(c) and 8412(d) (hereinafter referred to as 6c/12d employees).
- B. Mandatory Fitness Assessment results are not directly related to the Mandatory Physical Examination Program and the “fitness for duty” issue. However, significant health problems that arise in connection with HEP activities, the mandatory fitness assessment, or at any time (regardless of whether they are observed by other OIG officials), must be reported through proper channels to the AIGI.
- C. The Mandatory Fitness Assessment is a part of the HEP and is managed by the Training Program Manager (TPM) in HQ. The SSA OIG HEP is administered by the area Fitness Coordinators at the field level and nationally through the DFOH and private medical providers contracted by the SSA OIG.
- D. While accomplishing this process, the SSA OIG HEP and DFOH will take every measure possible to ensure that participant medical information is properly protected. Actual results of the medical testing are confidential and maintained by the DFOH. Only the SSA OIG Office of Communications and Resource Management (OCRM) receives Medical Certification/Exemption Forms specifying each participant’s authorized level of fitness program participation, and these forms are securely safeguarded. OCRM will notify the TPM in the event an agent is not authorized to participate in the Mandatory Fitness Assessment Program.
- E. The TPM periodically evaluates the Mandatory Fitness Assessment Program, taking note of those elements of the Program that “work,” and reconsidering others that prove less functional. Coupled with feedback from participants and SSA OIG HEP coordinators in the field, this enables SSA OIG to modify certain aspects of the Program in an effort to better accommodate the needs of the participants.
- F. In an effort to provide quality medical services at a reasonable cost to SSA OIG, and mindful of the reality that an individual’s fitness lifestyle, and not necessarily their age, contributes to their level of health, a medical certification process has been devised which takes into account these and other important considerations.

- G. The certification process, Risk Stratification Protocol, is based on American College of Sports Medicine (ACSM) guidelines. Unlike previous medical clearance processes in which a person's age dictated the frequency of medical exams, the new protocol specifies that the individual's health status shall determine the extent of medical testing. Accordingly, resources for medical clearance are focused on the smallest percentage of employees that have the greatest need; i.e., those at the highest risk. (A more detailed explanation can be found in the [Office of Investigations Trainers' Handbook](#)).

022.110 Physical Conditioning Under the Office of the Inspector General Health Enhancement Program

- A. Agents are authorized to participate in physical conditioning activities during the workday up to 3 hours per week. These activities should focus on the functional requirements stated in the Medical - Physical Evaluation packet prepared by DFOH for the OIG. These requirements include: ability to run 1.5 miles, moderate calisthenics warm-up and cool down, moderate lifting (15-45 pounds), flexibility in extremities and lower back, agility, rapid muscular coordination, etc.
- B. In order to determine the level of fitness of the agent, it is essential that periodic assessments be given under the supervision of trained fitness coordinators. (See Section [022.130B](#))
- C. All OIG 1811 series personnel, regardless of grade, are required to participate in the assessment process, unless excused according to procedures described in this chapter.
- D. Special agents may participate, on a voluntary basis, in a regular on-duty fitness maintenance/improvement activity. The Training Program Manager (TPM) will manage the overall Health Enhancement and Mandatory Fitness Program. The program will be coordinated in each field division office by the division Physical Fitness Coordinators selected by each SAC.
- E. It is the responsibility of the special agent to inform his/her supervisor and Physical Fitness Coordinator immediately of any condition arising during the interim period between medical examinations that may affect the agent's ability to participate safely in the wellness program. Participation in the fitness program during duty hours will be suspended, in whole or part, until the medical condition is corrected or satisfactorily improved based on the medical opinion of a qualified physician.

022.120 Requesting Approval for Workday Conditioning Activities

- A. OIG agents who wish to participate in physical conditioning activities during the workday must complete the mandatory assessment process and submit the Request for Workday Conditioning Activities [Form OI-48](#) to their SAC. In the request, agents will specify the fitness activities, location, and approximate times for the workouts. Certain activities such as bowling, golf, or organized team activities such as softball or basketball will not be considered as authorized fitness activities. Inherently dangerous sports and physical activities also will not be authorized. The SAC can grant agents 3 hours per week for conditioning activities. This written request shall be updated at the beginning of each fiscal year and whenever there is a change in the

location at which the fitness activities will occur. The original request will be kept on file in the local office. A signed copy will be returned to the agent.

- B. SACs are encouraged to ensure that all agents participate in physical conditioning activities since this is one area specifically addressed in the Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority.
- C. OIG will not reimburse agents for memberships in health or fitness facilities.

022.130 Administration of the Fitness Assessment

- A. The fitness assessment must be taken once each fiscal year. The local fitness coordinators are responsible for conducting the fitness assessment test. The assessment, patterned after the standards from the Center for Aerobic Research (Cooper Clinic), is designed to measure strength, endurance, and flexibility.

The Fitness Assessment consists of four events: push-ups, sit-ups, sit and reach, and a 1.5-mile run.

- B. Each FD shall have a Fitness Coordinator whom has received training as a fitness instructor. The Fitness Coordinator will administer the fitness assessments. Physical Fitness Coordinators will receive appropriate training prior to serving in that capacity. (Federal Law Enforcement Training Center (FLETC) training or a suitable substitute, such as the Cooper Aerobic Clinic training program, will be the standard.)
- C. Prior to the assessment, the agent must have undergone a health/medical screening and received a medical certification for participation in the program. As part of the assessment, the agent must provide a signed statement stating that they know of no medical reason why he or she should not participate in the assessment. A copy of the statement must be kept on file in the office to record the reason why the assessment was not given.
- D. The fitness coordinator records the raw score on the SSA OIG Fitness Evaluation Report ([Exhibit 22-3](#)). The raw scores are compared against the SSA OIG Fitness Norms and given a rating by category: Excellent, Very Good, Good, Fair, or Poor.
- E. The OCRM database has a screen for notification of agent participation. It is not necessary to send the scores to HQ. All fitness assessment related forms must be secure and retained locally by the Fitness Coordinator.
- F. Special Agents-in-Charge may excuse an agent from participating in a particular segment(s), or the entire fitness assessment, due to temporary physical or medical problems (e.g. broken bones, sprains, flu, pregnancy, etc.). Such waivers are temporary in nature and the agent will be expected to complete the test when the temporary condition no longer exists.
- G. It is the responsibility of the special agent to inform his/her supervisor and Physical Fitness Coordinator immediately of any condition arising during the interim period between medical examinations that may affect the agent's ability to participate safely in the wellness program. Participation in the fitness program during duty hours will be suspended in whole or part until

the medical condition is corrected or satisfactorily improved based on the medical opinion of a qualified physician.

- H.** An agent may be excused from segments, or the entire fitness assessment, due to a chronic medical condition. The condition must be documented in the agent's medical file and brought to the attention of the examining physician during the agent's required physical examination. Advise your DAIGI in writing of all waivers and their basis.
- I.** The AIGI or the DAIGI may grant a permanent waiver from participation in this program to any agent who has a medical condition that precludes them from participating in related physical activities. This authority may not be delegated below the DAIGI level.

Chapter 22

—

EXHIBITS

[22-1 — Physical Requirements for SSA OIG Criminal Investigators](#)

[22-2 — SSA OIG Fitness Evaluation Report](#)

[22-3 — SSA OIG Fitness Norms](#)

PHYSICAL REQUIREMENTS FOR SSA OIG CRIMINAL INVESTIGATORS

I. INTRODUCTION

The duties of a criminal investigator, job series GS-1811, in the Social Security Administration (SSA), include Federal criminal law enforcement activities, which can be physically demanding and dangerous. Accordingly, the SSA Office of the Inspector General (OIG) is responsible for ensuring that criminal investigators are physically and medically qualified for the position they hold.

II. POLICY

All applicants for OIG criminal investigator positions covered under the law enforcement provisions of either the Federal Employees Retirement System (FERS) or the Civil Service Retirement System (CSRS) will be required to undergo a pre-employment medical examination by agency-designated physicians to determine if they are physically and medically qualified to perform the full range of duties of that position. In addition, incumbent OIG criminal investigators will be subject to periodic medical examinations by agency-designated physicians for the purpose of assessing their fitness to retain the position.

- A. Any physical condition that would hinder an individual's full, efficient, and safe performance of his/her duties as a criminal investigator or failure to meet any of the required physical qualifications will usually be considered disqualifying for employment. Exception is made when convincing evidence is presented that the individual can perform the essential functions of the job efficiently and without hazard to himself/herself or others. (See item F below.)
- B. When ordering applicants/employees to undergo required medical examinations or requesting medical documentation, a representative of SSA OIG will notify the applicant/employee, in writing, of the reasons for the examination; the consequences of failure to report for an examination; and, the individual's right to submit medical information from his/her own source.
- C. Applicants who refuse to submit to the required examinations will not be considered for employment as a criminal investigator. Employees who refuse to submit to required periodic examinations will be subject to reassignment or appropriate disciplinary action.
- D. The Office of Investigations (OI) may also require a physical examination whenever there is a direct question about an employee's continued capacity to meet the physical or medical requirements of a position (5 C.F.R. 339.301(b)(3)).
- E. In certain situations, OI may order a psychiatric examination (including a psychological assessment). For instance, OI may order a psychiatric examination if a current general medical examination indicates no physical explanation for behavior or actions that may affect the safe and efficient performance of your duties (5 C.F.R. 339.301(e)).
- F. If a current employee fails to meet our physical requirements for any reason, he or she will have the opportunity to demonstrate that the essential duties of the job can be performed without endangering the health and safety of the individual or others (5 C.F.R. 339.204). Any history of a particular medical problem may result in medical disqualification only if the condition at issue is itself disqualifying, recurrence cannot medically be ruled out, and the duties of the position are such that a recurrence would pose a reasonable probability of substantial harm (5 C.F.R. 339.206).

III. BACKGROUND

Under FERS and CSRS, a law enforcement officer is defined as an employee whose primary duties are the investigation, apprehension, or detention of individuals suspected or convicted of offenses against the criminal laws of the United States. Also included in this definition are employees who move to a supervisory or administrative position (secondary position).

- A. The Government's authority to order medical examinations of employees is found at 5 U.S.C. 3301 and 5 C.F.R. Part 339, which authorizes agencies to determine the medical qualifications of applicants and to order examinations as necessary.
- B. The Office of Personnel Management (OPM) regulations under FERS (5 C.F.R. 842.802) limit law enforcement officer employment opportunities to young and physically vigorous individuals. Moreover, official documentation for the position must establish that the agency does not allow individuals to enter the position if they fail to meet physical qualifications as determined by the agency.

IV. PURPOSE

The purposes of adopting Medical/Physical Qualification Standards are:

- A. To meet OPM's requirements that agencies establish physical requirements for individuals entering criminal investigator positions;
- B. To provide realistic standards to ensure applicants/employees are physically capable of performing the duties that are expected of the position;
- C. To orient examining physicians to the medical disorders and physical conditions that would render an applicant/employee unable to meet the functional requirements for the position of criminal investigator or that would place the employee or others at risk; and
- D. To provide a consistent basis for examining and reviewing physicians to evaluate an applicant's/employee's fitness for duty.

V. SCOPE (COVERAGE)

These physical requirements cover all SSA OIG positions classified in the GS-1811 criminal investigator series. Therefore, any employee who occupies such a position may be periodically subject to a physical examination, by a licensed physician, to determine the individual's ability to perform the duties of the position.

- A. Primary positions which generally consist of SSA OIG criminal investigators performing the operational details of criminal investigations such as interviewing witnesses; interrogating suspects; reviewing, collecting, and analyzing records, facts, and evidence; performing undercover assignments; obtaining and serving warrants; using firearms; and carrying out arrests, searches, and seizures.
- B. Secondary positions which generally consist of SSA OIG managerial, supervisory, technical, or administrative positions (some with policy making and oversight responsibilities) which clearly require the first-hand knowledge, skills, abilities, and experience gained in the performance of primary law enforcement positions. The grade levels of the positions vary with the scope, complexity, and importance of investigations, involvement with other jurisdictions, and the degree of individual responsibility that progressively increases at higher levels.

VI. REFERENCES

- A. OPM Qualifications Standards for Positions under the General Schedule, GS-1810/1811 (Supersedes OPM X-118 Handbook);
- B. 5 U.S.C. § 8401(17)
- C. 5 U.S.C. § 3301
- D. 5 C.F.R. Part 339
- E. 5 C.F.R. 831.901-911; (CSRS – Law Enforcement Officers);
- F. 5 C.F.R. 842.801-809; (FERS – Law Enforcement Officers);
- G. Federal Law Enforcement Training Center (FLETC), Directive Number 91-01.E, entitled “Practical Exercise Performance Requirements.” (See Appendix 4 of the Model OIG Directive.)

VII. PHYSICAL REQUIREMENTS

- A. The duties of the OIG criminal investigator position require moderate to arduous physical exertion involving walking and standing, use of firearms, and exposure to inclement weather. Applicants/employees must be in good health, physically fit, and possess the following general attributes in order that they may satisfactorily perform the duties of the position of criminal investigator:
 - full range of motion of limbs and trunk;
 - average manual dexterity and hand-eye coordination;
 - average strength for age and build;
 - acceptable eyesight and hearing;
 - normal vocal abilities; and
 - emotional and mental stability.
- B. Manual dexterity with comparatively free motion of all joints is required. Arms, hands, legs, and feet must be sufficiently intact and functioning, and the applicant/employee must possess sufficiently good vision. The ability to hear the conversational voice and whispered speech with or without the use of a hearing aid is required. Since the duties of the position are exacting and responsible, and activities involve working under trying conditions, applicants/employees must possess emotional and mental stability.
- C. In general, the applicant/employee must be physically fit and have no physical impairments that would prevent the performance of law enforcement tasks such as using firearms, making searches, and/or carrying out arrests.
- D. The applicant/employee must have no physical impairments that inhibit performance of required practical exercises and tasks while in mandatory training programs either at FLETC and/or other training facilities approved by the SSA OIG. Specific information regarding FLETC practical exercise performance requirements for the 8-week basic Criminal Investigator Training Program can be found in Appendix 4 of the Model OIG Directive.

VIII. MEDICAL STANDARDS

- A. Eyesight

The occupational significance of this area concerns the ability to see and be free of visual problems. Any condition that may interfere with visual acuity or put the eye at risk may render an individual unable to meet the functional requirements for the position of criminal investigator. The individual must possess the following:

Near Vision corrected or uncorrected must be sufficient to read Jaeger Type 1 to 4 at 13 to 16 inches. Normal depth perception and peripheral vision are required.

Normal contrast sensitivity is required to rule out problems with night vision.

Far Vision uncorrected no worse than 20/200 (Snellen) in each eye, with correction to 20/20 in one eye and at least 20/40 in the other eye.

Color Vision sufficient to distinguish basic colors.

The following are examples of impairments that may affect the individual's ability to perform required criminal investigator functions:

- Current Cataracts
- Glaucoma
- Proliferative Retinopathy
- Retinal Detachment
- Refractive Keratoplasty

B. Ears and Hearing

The occupational significance of this area concerns the ability to hear and to maintain body equilibrium adequate on standard test vestibular function. Ability to hear is acceptable if the individual meets the standard by audiometer test with or without a hearing aid, where there is auditory discrimination at 35 decibels at 1000, 2000, and 3000 Hz level in each ear.

The applicant/employee must be retested after a noise-free period of at least 15 hours before he/she can be disqualified for hearing loss.

C. Nose, Mouth, and Throat

The occupational significance of this area is that distinct speech, odor detection, and free breathing are required. The presence of any serious acute or chronic disease or condition affecting the respiratory system and/or functional abnormality of the ears, nose, mouth, or throat which interferes with the applicant's ability to perform required criminal investigator functions are to be considered.

D. Peripheral Vascular System

The occupational significance of this area concerns the efficiency of the vascular system for maintaining adequate blood flow. Any condition that may interfere with the peripheral vascular system's normal functioning could render the individual unable to meet the functional requirements for the position of criminal investigator. The following are examples of impairments that may affect the individual's ability to perform required duties:

- Chronic Venous Insufficiency
- Peripheral Vascular Disease
- Thrombophlebitis

E. Heart and Cardiovascular System

The occupational significance of this area concerns the ability of the heart to provide the functional work capacity to meet the oxygen demands of physical work tasks. Any condition that would interfere with heart function could render an individual unable to meet the functional requirements for the position of criminal investigator. The following are examples of impairments that may affect the individual's ability to perform required duties:

- Angina
- Cardiomyopathy
- Congestive Heart Failure
- Coronary Artery Disease
- ECG Abnormalities (associated with disease; including arrhythmia incompatible with functional work capacity)
- Hypertension (with repeated readings which exceed 150 systolic and 90 diastolic without medication)
- Organic Heart Disease
- Mild Controlled Hypertension (less than 140 over 90 with limited medication may be acceptable)

F. Chest and Respiratory System

The occupational significance of this area concerns lung function, breathing capacity, and freedom from airway obstruction. This is a key area for job performance in terms of the respiration needed to perform physical tasks and to be free to move about in various environments. Any condition that may significantly interfere with breathing capacity could render the individual unable to meet the functional requirements for the position of criminal investigator. The following are examples of impairments that may affect the individual's ability to perform required duties:

- Asthma (associated with reduced pulmonary function)
- Chronic Bronchitis
- Chronic Obstructive Pulmonary Disease
- Bronchiectasis
- Pneumonectomy
- Pneumothorax
- Pulmonary Tuberculosis (active or with significant lung destruction)
- Reduced Pulmonary Function (if FEV1 is less than 65 percent of vital capacity)

G. Abdomen and Gastrointestinal System

The occupational significance of this area concerns a variety of gastrointestinal disorders that can affect performance of job tasks by imposing severe individual discomfort. Any functional disorders rendering the applicant incapable of sustained attention to work tasks; i.e., chronic diarrhea and discomfort secondary to such disorders, could render an individual unable to meet the functional requirements for the position of criminal investigator. The following are examples of impairments that may affect the individual's ability to perform duties:

- Active Hepatitis
- Active Peptic Ulcer Disease (not adequately controlled on medication)
- Cirrhosis of the Liver
- Chronic Inflammatory Bowel Disease
- G.I. Bleeding
- Femoral Hernia (not surgically repaired)
- Inguinal Hernia (not surgically repaired)

H. Genitourinary and Reproductive System

The occupational significance of this area concerns renal failure and genitourinary dysfunction. Any condition affecting the genitourinary tract rendering an individual unable to meet the functional requirements for the position of criminal investigator should be considered.

Pregnancy will not disqualify the individual for the position. However, some training and law enforcement assignments will be deferred until termination of pregnancy.

The following are examples of impairments that may affect the individual's ability to perform required duties:

- Acute and Chronic Nephritis
- Nephrosis
- Obstructive Uropathy
- Polycystic Kidney Disease
- Pyelonephritis
- Recurrent Renal (or other urinary calculi)
- Renal Failure
- Symptomatic Prostatic Hypertrophy
- Severe Dysmenorrhea or Symptomatic Endometriosis

I. Endocrine and Metabolic Systems

The occupational significance of this area concerns any abnormality of the endocrine system that may affect job performance. Any excess or deficiency in hormonal production can produce metabolic disturbances affecting weight, stress adaptation, energy production, and a variety of symptoms such as elevated blood pressure, weakness, fatigue, and collapse. Any such disturbance of maintenance of body functions may affect ability to meet the functional requirements for the position of criminal investigator. The following are examples of impairments that may affect the individual's ability to perform required duties:

- Adrenal Dysfunction
- Thyroid Disease (not controlled and stable)
- Pituitary Dysfunction
- Symptomatic Hypoglycemia
- Diabetes Mellitus*

* A diabetic condition is not usually disqualifying if there have been no significant complications (e.g., Cardiovascular, Visual, Renal, Neurological, Alteration of Consciousness) and the condition is controlled by diet and/or exercise, or oral medication, **or if the condition is insulin requiring, there has been no evidence of severe hypoglycemic insulin reactions (e.g., alteration of consciousness) during the past year.**

J. Musculoskeletal System

The occupational significance of this area concerns the mobility, stability, flexibility, and strength to perform physical job tasks efficiently with minimum risk of injury. Disorders affecting the musculoskeletal system are acceptable if the individual meets the basic movement, strength, flexibility, and coordinated balance criteria in the functional requirements for the position of criminal investigator. The following are examples of impairments that may affect the individual's ability to perform required duties:

- Disease or Deformity of:
 - Bones or Joints;
 - Intervertebral Disk; and Muscles and Tendons
 - Previous Injury (impairing performance)

Cervical Spine or Lumbosacral Fusion (affecting performance)
Herniated Disk
Loss in Motor Ability from Tendon or Nerve Injury
Major Extremity Amputation
Digit Loss (incompatible with function)

K. Hematopoietic and Lymphatic Systems

The occupational significance of this area concerns chronic disorders that may affect overall health in a disabling manner. Any disorder in this area can lead to reduced capability to perform intense physical exertion, or place the applicant at undue risk and affect the applicant's ability to meet the functional requirements for the position of criminal investigator. The following are examples of impairments that may affect the individual's ability to perform required duties:

Leukemia
Severe Anemia
Thrombocytopenia or Clotting Disorders

L. Nervous System

The occupational significance of this area concerns the functioning of the central and peripheral nervous system. Dysfunction in this area can increase the probability of accidents and/or potential inability to perform a variety of physical tasks, as exemplified in the functional requirements for the position of criminal investigator. The following are examples of impairments that may affect the individual's ability to perform required duties:

Epilepsy (not controlled)
Multiple Sclerosis
Cerebrovascular Disease (including aneurysms and vascular malfunctions)
Other Disease or Disorder of the Nervous System (producing loss of strength, coordination, or other dysfunction impairing full performance, including sequelae of previous injury, infection, or other disease)

M. Malignant Diseases

The occupational significance of the disease must be related to the individual's ability to adequately function and to perform the physical work tasks as exemplified in the requirements for the position of criminal investigator.

N. Psychiatric Conditions

The occupational significance of this area is concerned with the presence of serious mental disease, which can adversely affect critical judgment and perceptive patterns necessary for safe performance of required law enforcement tasks, as exemplified in the functional requirements and environmental factors for the position of criminal investigator.

IX. ORIENTATION FOR EXAMINING PHYSICIAN

A proper examination of applicants/employees requires the physician to relate the physical examination and medical history to the demands of the job, as exemplified in the functional requirements for the position of criminal investigator. Accordingly, the examining physician should be provided with the following (all of these are found in the Model OIG Directive):

- Physical Requirements for Criminal Investigator (Appendix 1)

- Medical Standards (Pages 5 through 10)
- Functional Requirements and Environmental Factors (Appendix 2)
- Abridged Position Description for Criminal Investigator (Appendix 3)
- Training Requirements for Criminal Investigator (Appendix 4)

It is important that the examining physician be aware that the position of criminal investigator requires the individual to be physically fit in order to perform required law enforcement tasks, which may include surveillance, searches, arrests, and the use of firearms.

The criminal investigator must possess the ability to analyze records, documents, and other evidence related to suspected criminal activity. Proper vision is required in order to conduct searches and review physical evidence. A reasonable degree of physical strength is also required in order to carry or move bulk materials and/or boxes of records that are made available through searches.

To perform surveillance, a criminal investigator must stand for long periods of time and/or be mobile at a moment's notice. Inability to remain stationary for long periods of time, as a result of chronic diarrhea or urinary frequency, could also interfere with the performance of this activity. Sensory deficits also may render the individual unable to perform surveillance.

Physical confrontation may occur when search warrants are being served or arrests are being made by a criminal investigator. The inability to carry out these tasks, due to loss of a limb or weakness secondary to local or systemic disease, could place the individual or co-workers at risk.

Judgments must be made concerning an applicant's previous history of mental illness or its symptoms since the carrying of firearms implies that reasonable judgment and mental stability must be present. Adequate visual acuity and motor coordination are also required for the proper use of firearms and for the training activities related to the position of criminal investigator.

It may be found that an individual has two or more medical conditions where each one in and of itself is not sufficiently disabling to disqualify the person for employment. However, the combination of medical or physical conditions may collectively hinder the individual's functional capacity to perform activities relating to law enforcement functions. This could place the individual at personal risk to himself/herself or others. If so, the examining physician should so indicate in his/her medical findings.

X. MEDICAL FORMS

A. Report of Medical Examination

The results of the medical examination should be reported by the examining physician on the agency approved medical examination form (SF-78, SF-88, or revisions thereto).

B. Report of Medical History

The approved agency medical history form (SF-83, SF-93, or revisions thereto) should be completed by the applicant/employee and provided to the examining physician for his/her information and assistance in conducting the examination.

XI. EXAMINING PHYSICIAN'S CONCLUSIONS

After the examining physician has completed the physical examination and has reviewed all of the laboratory results, his/her findings should be recorded on the approved medical examination form using one of the following statements:

- A. No Significant Findings – All medical requirements for the position of criminal investigator have been satisfied.
- B. Significant Medical Findings – The medical findings are noted and it is the opinion of the examining physician that the individual cannot perform the essential functional requirements efficiently and without hazard to himself/herself or others.
- C. Additional Testing Requirements – Final assessment cannot be made until specific tests are conducted or repeated.

The tests recommended are:

XII. REPORTS ON MEDICAL FINDINGS

All completed medical reports on examinations, along with all laboratory results, should be sealed in an envelope and forwarded to Social Security Administration, Office of the Inspector General, Office of Technology and Resource Management, 2ME3 Meadows East, 6401 Security Boulevard, Baltimore, Maryland 21235-6401.

XIII. EMPLOYABILITY DETERMINATION

Employment related decisions involving health status are fundamentally management, not medical, decisions. Medical information may be relevant, indeed dominant, in the outcome, but OIG management has both the obligation to consider issues which are not strictly medical (e.g., reasonable accommodation or undue hardship on agency operations) and the authority to hold medical information to a standard of relevance and veracity. Accordingly, the medical examination cannot determine an individual's ability to perform the essential duties of a criminal investigator. This responsibility rests solely with the OIG appointing official or his/her designee. (Medical consultant services will be obtained if necessary.)

- A. OIG must obtain OPM approval of any agency decision to medically disqualify a certified preference eligible candidate.
- B. If the applicant/employee requests the opportunity to submit supplementary medical documentation from his/her personal physician, such documentation must be reviewed and considered by the deciding OIG official(s). Supplementary physical examinations from a personal physician will be paid for by the applicant/employee.
- C. OIG deciding officials must comply with applicable OPM guidelines for specific medical conditions.

XIV. RECONSIDERATION

Should an applicant/employee be found to have a significant impairment that precludes him/her from selection or retention as a criminal investigator (and the impairment is correctable), he/she will be given the opportunity to take corrective action. If the individual can present medical documentation within 90 days that the impairment has been corrected, the individual will then be eligible for reconsideration. The SSA OIG reserves the right to have such individuals re-examined by an agency-designated physician.

XV. WAIVER OF MEDICAL STANDARDS/PHYSICAL REQUIREMENTS

All requests for waivers of criminal investigator medical standards and/or physical requirements will be forwarded for decision to the Inspector General (IG) or the Deputy Inspector General (DIG). The IG/DIG may also call upon medical consultant services if deemed necessary.

- A. Failure to meet the established medical standards or physical requirements means that the individual is not qualified for the position unless there is sufficient evidence that he/she can perform the duties of the position safely and efficiently despite a condition that would normally be disqualifying. The SSA OIG must waive any physical requirement for a person who is able to demonstrate the capacity to perform safely and efficiently. Factors that will be considered in deciding whether or not to waive a standard or requirement for OIG employment/retention include:
- health and safety considerations;
 - recent satisfactory performance in the same or similar positions (any unsatisfactory performance appraisal not due to physical or mental condition should not be considered in this context);
 - successful performance of other life activities with similar physical and environmental demands;
 - successful performance of a real or simulated work sample; and
 - a determination that the condition may be reasonably accommodated (without undue hardship on the agency) to permit effective performance.
- B. The decision as to whether or not an applicant/employee can perform safely and efficiently rests with the OIG deciding official(s) or appropriate designee(s).
- C. An agency's decision to separate an employee for reasons of medical disqualification does not control, preempt, or otherwise supersede an OPM determination of entitlement or non-entitlement to disability retirement under section 8337 or 8451 of title 5, United States Code.
- D. A history of a medical condition may be considered disqualifying only if the condition itself is normally disqualifying, a recurrence cannot medically be ruled out, and the duties of the position are such that a recurrence would pose a reasonable probability of substantial harm.

For example, while an early history of epilepsy, by itself, would not ordinarily be disqualifying for any position, a particular history of epilepsy may, depending upon the specific nature of the condition, be disqualifying. Each case must be decided on its own merits. Generally speaking, as long as the candidate is presently able to do the job, he/she is qualified unless the possibility that the condition might recur would present a substantial health and safety risk.

XVI. REASONABLE ACCOMMODATION

In accordance with the Rehabilitation Act of 1973, as amended, the SSA OIG will make reasonable accommodation to the known physical or mental limitations of qualified handicapped applicants/employees if the accommodation will permit the handicapped applicant/employee to perform the essential functions of the position in question without endangering the health and safety of the individual or others, unless the accommodation would impose an undue hardship on the OIG.

Individuals seeking such accommodation must, as determined by the OIG, submit to the medical examination required by the OIG and/or produce medical documentation to support the request.

XVII. COST OF EXAMINATION AND TESTING

Costs of the medical examination, including specified tests and reasonable travel expenses (for employees), will be paid by the SSA OIG. Additional tests, corrective action, follow-up treatment, and/or additional medical examination recommended by the examining physician to determine the applicant's ability to meet the standards will be the responsibility of the individual applicant/employee.

XVIII. FREQUENCY OF MEDICAL EXAMINATIONS

Unless waived, all new criminal investigators will undergo a medical examination before entering on duty. Periodic medical examinations will be administered at least every 36 months thereafter, until the criminal investigator's 45th birth date. All criminal investigators over the age of 45 will undergo a periodic medical examination at least every 24 months. All criminal investigators will be subject to a medical examination whenever there is a question about the employee's continued ability to meet the physical or medical requirements of the position.

XIX. RECORDS

When the physical examination process has been completed, the Office of Communications and Resource Management (OCRM) will establish an employee medical folder for each applicant/employee. All medical documentation will be maintained in the employee medical folder. This folder is maintained separately from the Official Personnel Folder, and the information is covered under the provisions of the Privacy Act. This folder will be physically located in a secured area of OCRM.

Access to the information contained in this folder will be available only to the applicant, employee, the representative of the employee (who has been designated in writing), servicing personnel specialist(s), medical consultants, and OIG management officials who are involved in making employment/retention determinations.

The medical folder will be maintained for the length of the individual's employment with SSA. If an employee transfers to another Federal agency, the employee medical folder will be transferred to the gaining agency. When the employee leaves Federal service, the medical folder will be retired to the Federal Records Center.

SSA OIG FITNESS EVALUATION REPORT

Name: _____ Title: _____

Division: _____ DOB: _____

Fitness Assessment Date: _____

	Sit Ups	Push Ups	Sit & Reach	1.5-mile Run	% Body Fat
Raw Score					
Fitness Level					

Overall Numerical Score: _____ Average: _____

Fitness Assessment Date: _____

	Sit Ups	Push Ups	Sit & Reach	1.5-mile Run	% Body Fat
Raw Score					
Fitness Level					

Overall Numerical Score: _____ Average: _____

Fitness Assessment Date: _____

	Sit Ups	Push Ups	Sit & Reach	1.5-mile Run	% Body Fat
Raw Score					
Fitness Level					

Overall Numerical Score: _____ Average: _____

SSA OIG FITNESS NORMS

SIT UPS Females

Fitness Category *****Age Categories*****

AGE LEVEL	20-29	30-39	40-49	50+
(5) Excellent	(b) (2)			
(4) Very Good				
(3) Good				
(2) Fair				
(1) Poor				

SIT UPS Males

Fitness Category *****Age Categories*****

AGE LEVEL	20-29	30-39	40-49	50+
(5) Excellent	(b) (2)			
(4) Very Good				
(3) Good				
(2) Fair				
(1) Poor				

PUSH UPS Females

Fitness Category *****Age Categories*****

AGE LEVEL	20-29	30-39	40-49	50+
(5) Excellent	(b) (2)			
(4) Very Good				
(3) Good				
(2) Fair				
(1) Poor				

PUSH UPS Males

Fitness Category *****Age Categories*****

AGE LEVEL	20-29	30-39	40-49	50+
(5) Excellent	(b) (2)			
(4) Very Good				
(3) Good				
(2) Fair				
(1) Poor				

MODIFIED SIT & REACH

FEMALES

Level Age	20-29	30-39	40-49	50-59	60+
(5) Excellent 95%					
(4) Very Good 90%					
(3) Good 80%					
(2) Fair 70%					
(1) Poor 60%					

MALES

Level Age	20-29	30-39	40-49	50-59	60+
(5) Excellent 95%					
(4) Very Good 90%					
(3) Good 80%					
(2) Fair 70%					
(1) Poor 60%					

****All measurements are made in inches**

1.5-MILE RUN **Females**

Fitness Category *****Age Categories*****

AGE LEVEL	20-29	30-39	40-49	50+
(5) Excellent	(b) (2)			
(4) Very Good				
(3) Good				
(2) Fair				
(1) Poor				

1.5-MILE RUN **Males**

Fitness Category *****Age Categories*****

AGE LEVEL	20-29	30-39	40-49	50+
(5) Excellent	(b) (2)			
(4) Very Good				
(3) Good				
(2) Fair				
(1) Poor				

PERCENT BODY FAT (Optional) **Females**

Fitness Category *****Age Categories*****

AGE LEVEL	20-29	30-39	40-49	50+
(5) Excellent	(b) (2)			
(4) Very Good				
(3) Good				
(2) Fair				
(1) Poor				

PERCENT BODY FAT (Optional) **Males**

Fitness Category *****Age Categories*****

AGE LEVEL	20-29	30-39	40-49	50+
(5) Excellent	(b) (2)			
(4) Very Good				
(3) Good				
(2) Fair				
(1) Poor				

ADMINISTRATIVE SUPPORT FUNCTIONS

023.000 General

Administrative functions and policies not covered in the Office of the Inspector General *Administrative Policies and Procedures Manual* are discussed in this chapter.

023.010 Property Management

A. Policy

[Chapter 4 of the *Administrative Policies and Procedures Manual*](#) (APPM) is the official source of information on general property management for the Office of the Inspector General. That chapter contains information regarding the duties and responsibilities of the property management officers, custodial officers, supervisors, and employees.

B. Property for New Employees

Property for new employees shall be issued from a Field Division's (FD) inventory, including weapon, handcuffs, holster, extra magazines, extendible baton, and other related items. Additional items can be requested through the Regional ASAC, or purchased locally if they are not available at the FD, when the new employee reports for duty. The receipt of property/equipment must be acknowledged/documented in the Property Management System (Metastorm).

C. Badges and Credentials

1. OI HQ issues badges and credentials.
2. The FD requests these through their Criminal Investigations Division (CID) regional desk officer.
3. The request must include two passport-size photographs of the person to whom the credentials will be issued.
4. The credential is forwarded to the FD for the new employee to sign.
5. After signing the credential, the credential must be returned to HQ in order to obtain the signature of the Inspector General.

6. The completed credential and badge is returned to the employee.
7. Instructions for reporting lost or stolen badges or credentials is found in APPM, Chapter 4.
8. An employee whom the OIG has hired as a Special Agent, and who has not attended the Criminal Investigator Training Program (CITP) at the Federal Law Enforcement Training Center (FLETC), may be issued a temporary credential bearing the title “Investigator.” This credential will allow the OI employee to engage in non-criminal investigative functions that requires a government credential (i.e. making a request for court records). This credential will not convey law enforcement authority to the receiving employee and will not authorize the individual to carry a firearm. Prior to reporting to FLETC’s CITP the employee will return the “Investigator” credential to PAD/OI Headquarters (HQs) and PAD/OI HQs will issue the “Special Agent” credential upon completion of CITP.

D. Body Armor

1. Each SA is issued a protective vest. The vests are made to fit the specific measurements of the employee. The FD is responsible for the actual ordering of the vest. The vest should be purchased using the Visa International Merchant Purchase Authorization Card (IMPAC). Vests may be purchased from any vendor listed on the General Services Administration (GSA) schedule of approved vendors.
2. The level of the vests must be checked. OI’s requirement is that the vests must be rated as Level IIIA.
3. The life expectancy of body armor varies depending on its frequency of use and how it is maintained. The body armor should be replaced as needed.

023.020 Administrative Filing System

- A. All documents created or received by OIG/OI must be filed according to a common system. The filing system to be used by all organizational elements of OI is based on the *Special Agent Handbook (SAH)* and the *OIG Administrative Policies and Procedures Manual (APPM)*.
- B. Each file will have an eight character numeric code that will indicate the year, chapter number, and section. For example, to create a file for information regarding new policies and procedures, one would use the file code 001.130. SAH [001.130](#) of the *SAH* addresses “Establishing Policy and Procedure.” All documents relating to the new policies or procedures would be filed under the general administrative file code 001.130.
- C. The file number must contain eight digits. The first two numbers identify the fiscal year, the third through fifth numbers identify the chapter, and the sixth through eighth numbers identify the section. Chapters 1 through 9 will be designated as 001, 002, 003, etc. Chapter 10 and above will be designated as 010, 011, 012, etc. Incoming documents may be marked with a three-letter code for filing purposes. This code is shown after the chapter title, for example, documents for filing under Chapter 1, Authority and Organization may be marked as AOP.
- D. In order to include information relating to topics in the *OIG APPM* (awards, budgets, property management, records retention, work schedules, etc.), a zero will be added before chapters

numbered 3-9 and a one for the chapters 10 and beyond. Since Chapter 1 of the *APPM* contains information similar to that of Chapter 1 of the *SAH*, no additional file codes are needed for this chapter. Chapter 2 of the *APPM*, *Delegation of Authority*, will not have its own chapter number. All material related to that topic may be filed in the AOP or PER file. All other chapters will be given a three-digit designation. For example, Chapter 3 becomes 030, 4 becomes 040, 11 becomes 110, etc. If an office established a file to track "Awards" for FY 2012, file number 12-117.000 would be assigned since chapter 17 in the *APPM* addresses awards.

- E. While it is essential to create a file system that facilitates the easy storage and retrieval of documents, it is not necessary to create a file for every section or paragraph listed in the *SAH* and the *OIG APPM*. Offices are encouraged only to create files as needed.
- F. The creation of a uniform system for information management will ensure that each division handles documents uniformly, and that historical information is readily obtainable.

023.030 Files to be Considered for Establishing Each Fiscal Year

AUTHORITY AND ORGANIZATION (AOP)

- 001.130– Establishing Policy and Procedure (POL)
- 001.140– Certification of *Special Agent Handbook (SAH)*
- 001.150– Liaison (LIA)

RESPONSIBILITIES AND CONDUCT (CON)

- 002.000– Standards of Ethical Conduct (ETH)
- 002.060– Official Vehicles (VEH)
- 002.080– LEAP (LEP)
- 002.150– Media Relations (MED)
- 002.170– Congressional Inquiries (INQ)

CASE MANAGEMENT (INV)

- 003.000– General
- 003.100– Case Reviews

INVESTIGATIVE GUIDELINES AND PROCEDURES (IPE)

- 004.270– Investigations in Foreign Countries
- 004.280– Audit Assistance (AUD)

INVESTIGATIVE PROJECT MANAGEMENT (IPM)

- 005.000– Investigative Projects
- 005.030– Cooperative Disability Investigations Program (CDI)
- 005.040– Fugitive Felon Program (FFP)
- 005.050– SSN Misuse and Identity Theft (IDT)
- 005.060– Deceased Auxiliary Beneficiary Project (BIC)
- 005.070– Residency Projects (RES)
- 005.080– Homeland Security Projects (HOM)

ACCESS TO SOCIAL SECURITY INFORMATION (SSD)

- 006.010– Policy Statement
- 006.020– SSA Records Access and Disclosure

INVESTIGATIVE OPERATIONS AND SUPPORT (OPS)

007.040– Use of SSA Employees in Field/Undercover Operations
007.140– Technical Investigative Equipment and Support

INTERCEPTION OF COMMUNICATIONS (INT)

008.000– Consensual and Non-consensual Monitoring
008.020– Accounting for Interception Devices

CONFIDENTIAL EXPENDITURES (CEX)

009.010– Confidential Funds

INTERVIEWS AND STATEMENTS (STA)

010.050– Legal Issues

INVESTIGATIVE REPORTS (REP)

011.000– General
011.040– SSA/OIG Fact Sheets

INSPECTOR GENERAL SUBPOENAS (SUB)

012.010– Subpoena Requests

SEARCH AND SEIZURE (SRH)

013.000– Policy

ACQUISITION, PRESERVATION, AND MANAGEMENT OF EVIDENCE (EVD)

014.090– Evidence Management Procedures

CRIMINAL PROCEDURE (CRM)

015.120– Declinations of Prosecution

CIVIL MONETARY PENALTY (CMP)

016.000– Section 1129 – False Statements and Representations

VICTIM AND WITNESS ASSISTANCE PROGRAM (VIC)

017.000– General

GENERAL LEGAL MATTERS (LEG)

018.000– General Legal Matters

FREEDOM OF INFORMATION AND PRIVACY ACTS (FOI)

019.000– The Freedom of Information Act
019.060– Privacy Act of 1974

TRAINING (TRN)

020.000– General Policy
020.060– Field Division In-Service Training

FIREARMS AND USE OF FORCE POLICY (FIR)

021.000– General

OCCUPATIONAL HEALTH AND WELLNESS PROGRAM (WEL)

022.000– General

022.120– Requesting Approval of Workday Conditioning Activities

ADMINISTRATIVE SUPPORT FUNCTIONS (ADM)

023.000– General

023.060– Personnel Management

NOTE: Chapters 24 through 28 are reserved for future use.

ADMINISTRATIVE POLICIES AND PROCEDURES (File under code PER (Personnel) unless otherwise noted)

BUDGET and FINANCIAL MANAGEMENT (BUD)

030.000– General

PROPERTY MANAGEMENT (PRO)

040.000–

RECORDS RETENTION and DISPOSITION)

050.000– General

WORK SCHEDULES and HOURS OF WORK

060.000– General

EMPLOYEE CONDUCT (CON)

070.000– General

REQUIREMENTS FOR OUTSIDE ACTIVITIES

080.00– General

FINANCIAL DISCLOSURE REPORTING

090.000– General

RESERVED (Chapter 10)

100.000– General

TELEWORK PROGRAM

111.000– General

RESERVED (Chapter 12)

112.000– General

RESERVED (Chapter 13)

113.000– General

RESERVED (Chapter 14)

114.000– General

RESERVED (Chapter 15)

115.000– General

RESERVED (Chapter 16)

116.000– General

AWARDS PROGRAMS (AWD)

117.000– General

RESERVED (Chapter 18)

118.000– General

SEXUAL HARASSMENT

119.000– General

RESERVED (Chapter 20)

120.000– General

CRITICAL INCIDENTS

121.000– General

023.040 Records Disposition Schedules

- A. The OIG’s records management program is found in [Chapter 5 of the Administrative Policy and Procedures Manual](#). Chapter 5 addresses policy, scope, definitions, responsibilities, record retention, records disposal, and procedures to follow when recalling records from storage.
- B. Records are maintained according to either a General Records Schedule (GRS) established by the National Archives and Records Administration (NARA) or by individual agency retention schedules approved by NARA.

023.050 Personnel Management Information and Procedures Guidance

- A. The Human Resources Division of the OIG’s Office of Communication and Resource Management (OCRM) serves as the official source of information relating to personnel matters. This includes issues relating to employee conduct, pay, processing personnel actions, issuing vacancy announcements, recruiting, etc.
- B. OI employees who require information on personnel matters should consult the OIG Administrative Policies and Procedures Manual. If the information is not available in that manual, employees should contact the Policy and Administration Division for guidance or go directly to the human resource specialist in OCRM assigned to cover their division.

023.060 Employee Transfers and Relocations

- A. Employees selected for transfer will receive notification from OI headquarters.
- B. The Policy and Administration Division coordinates relocations by OI employees.

Government Vehicle Fleet Management**A. General**

The Office of Investigations recognizes the need for a well-maintained and functional fleet of vehicles to carry out its investigative and support duties. All employees who drive a government leased vehicle, on either a regular or temporary basis, have a responsibility to ensure that the vehicle is used only for official purposes and is driven in a manner consistent with existing laws and government regulations.

B. The Policy and Administration Division oversees the general management of the fleet of vehicles assigned to the Office of Investigations (OI) by:

1. Establishing policy regarding the types of vehicles that comprise OI's fleet,
2. Tracking the approval, acquisition, and use of fleet vehicles, and
3. Preparing required reports regarding vehicle type, fuel usage, and mileage as requested by SSA or other government agencies.

C. The Special Agent-in-Charge (SAC) of the Field Division (FD) to which the vehicle is assigned is responsible for:

1. Ensuring that the FD has the appropriate number and type of vehicles necessary to carry out the duties and responsibilities of OI. The number of special purpose vehicles, such as SUVs, cannot exceed 20% of the FD's total fleet. Any exception to this rule must be approved in writing by the Deputy Assistant Inspector General (DAIGI) prior to initiating discussions to lease a vehicle other than a sedan.
2. Assigning vehicles to employees,
3. Monitoring the submission of required reports and memoranda to track vehicle usage and to account for any or all damage to a vehicle, and
4. Overseeing the return of vehicles to the lessor when the number of vehicles assigned to an office exceeds the number of agents actually assigned to the office. For example, if an agent retires or resigns and the process to select a replacement has not begun, the vehicle should be turned in.

D. Assistant Special Agents-in-Charge (ASACs) and Resident Agents-in-Charge (RACs) are responsible for ensuring that employees are aware of the requirements for users of government leased vehicles and shall assist the SAC in carrying out the duties listed previously in section C.**E. All users of government vehicles are responsible for knowing the requirements section 002.060 of this handbook.**

[23-1 — Personal Custody Property Record/Hand Receipt \(OI-52\)](#)

Exhibit 1

Personal Custody Property Record/Hand Receipt

Property Issued To:	OPDIV/STAFFDIV	Division/Branch	Location: Rm./Bldg.
Name: (Last) (First) (MI)			

Statement of Responsibility

I have received the item(s) listed below on the date indicated. I accept personal responsibility for the property and will surrender it upon demand, transfer, or separation from the Government. I further understand that failure on my part to exercise responsibility for the care and protection of the item(s) listed below could result in pecuniary liability established in accordance with SSA Administrative Instructions Manual System 04.02.04.

Description-Including Make, Model, Serial Number and Accessories	
	Name or Person Receiving Property Telephone #
	Signature Date
	Returned Date
	Received-Signature of Custodial Officer
	Items Are to be Returned To:
Name of Issuing Property Representative	Issuing Office Location Telephone #
Signature	

USE OF FORCE

024.000 **Consideration for Use of Force**

- A.** The primary considerations for the use of force are the timely and effective application of the appropriate level of force required to establish and maintain lawful control, preserve life, and prevent serious physical injury. (Force can range from minimal or no force to verbal direction, weaponless control techniques, intermediate force, and finally, deadly force.) The use of force, including deadly force, is governed by the totality of the circumstances known by a special agent (SA) at the moment he/she decides force is required.
1. Use of force by an SA upon a person will be based on the “objective reasonableness” standard. This means the use of force must be objectively reasonable under all the circumstances known to the SA at the time. The degree of force authorized is limited to that which is necessary to establish lawful order and control in a timely manner. **IF FORCE, OTHER THAN DEADLY FORCE, REASONABLY APPEARS TO BE SUFFICIENT TO ACCOMPLISH AN ARREST OR OTHERWISE ACCOMPLISH THE LAW ENFORCEMENT PURPOSE, DEADLY FORCE IS NOT JUSTIFIABLE.**
 2. It should be recognized that SAs frequently find themselves in unpredictable and rapidly evolving situations, and are often forced to make split-second decisions concerning the level of force that is appropriate and necessary in a particular circumstance.
- B.** The duty-related use of any OI-issued weapon shall be in accordance with the guidelines issued by the Department of Justice (DOJ) dated July 1, 2004 (*see Special Agent Handbook - [Appendix III](#)*) General Principles of the Department of Justice Use of Deadly Force Policy (*see Special Agent Handbook - [Appendix III](#)*).
1. As law enforcement officers, SAs may use deadly force only when necessary, that is, when the officer has reasonable belief that the subject of such force poses an imminent danger of death or serious physical injury to the SA or to another person.
 - a. Deadly force may not be used solely to prevent the escape of a fleeing suspect.
 - b. Firearms may not be fired solely to disable moving vehicles.

- c. If feasible, and if to do so would not increase the danger to the SA or others, a verbal warning to submit to the lawful authority of the agent **shall** be given prior to the use of deadly force.
- d. Warning shots are not permitted outside of the prison context.
- e. SAs will be trained in alternative methods and tactics for handling resisting subjects, which must be used when the use of deadly force is not authorized by this policy.

C. DOJ Policy in Custodial Situations

1. Unless force other than deadly force appears to be sufficient, deadly force may be used to prevent the escape of a prisoner committed to the custody of the Attorney General or the Bureau of Prisons.
 - a. if the prisoner is effecting his or her escape in a manner that poses an imminent danger to the safety of the officer or another person; or
 - b. if the prisoner is escaping from a secure facility or is escaping while in transit to or from a secure facility.
2. If the subject is in a non-secure facility, deadly force may be used only when the subject poses an imminent danger of death or serious physical injury to the officer or another person.
3. If the subject is in transit to or from a non-secure facility and is not accompanied by a person who is in transit to or from a secure facility, deadly force may be used only when the subject poses an imminent danger of death or serious physical injury to the officer or to another person.
4. After an escape from a facility or vehicle and its immediate environs has been affected, officers attempting to apprehend the escaped prisoner may use deadly force only when the escaped prisoner poses an imminent danger of death or serious physical injury to the officer or another person.
5. Deadly force may be used to maintain or restore control of a prison or correctional facility when the officer reasonably believes that the intended subject of the deadly force is participating in a disturbance in a manner that threatens the safety of the officer or another person.

In the prison context, warning shots may be fired within or in the immediate environs of a secure facility if there is no apparent danger to innocent persons:

- a. if reasonably necessary to deter or prevent the subject from escaping from a secure facility; or
- b. if reasonably necessary to deter or prevent the subject's use of deadly force or force likely to cause serious physical injury.

D. Application of the DOJ Policy - This policy is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the

United States, its departments, agencies, or other entities, its officers or employees, or any other person.

- E.** Deadly force may be directed against vicious dogs or other animals when necessary for self-defense or in the defense of others.
- F.** Weapon(s), to include a firearm, may be drawn before the situation escalates to one requiring the use of force, if so dictated by circumstances and/or reasonable judgment.
- G.** Using Less-Than-Lethal Devices
 - 1. OI agents are authorized to use only those less-than-lethal devices (expandable batons or pepper spray) provided by the SSA OIG and that they are trained to use, absent exigent circumstances.
 - 2. OI agents are authorized to use less-than-lethal devices only in those situations where reasonable force, based on the totality of the circumstances at the time of the incident, is necessary to effectuate an arrest, obtain lawful compliance from a subject, or protect any person from physical harm. Use of less-than-lethal devices must cease when it is no longer necessary to achieve the law enforcement objective.
 - 3. OI agents are not authorized to use less-than-lethal devices if voice commands or physical control achieves the law enforcement objective. OI agents are prohibited from using less-than-lethal devices to punish, harass, or abuse any person.
 - 4. Less-than-lethal devices are used with a reasonable expectation that death or serious bodily injury will not result. They are, however, recognized as having the potential to cause death or serious bodily injury, and OI agents may use less-than-lethal devices as deadly weapons only when authorized under OI's use of force policy as found in this chapter.
 - 5. OI agents must make necessary medical assistance available to subjects of less-than-lethal device use as soon as practicable.

024.010 Liability

- A.** SAs should be aware that liability issues arising from on-duty and off-duty actions involving the use of agency issued equipment are identical; however, employment and Department of Justice representation determinations can be more complex in off-duty carriage situations. Questions regarding liability issues associated with off-duty carriage should be addressed to the Office of the Counsel to the Inspector General (OCIG).

024.020 Basic Use of Force Training

- A.** Newly appointed SAs, or those transferred into positions requiring the use of firearms, shall not be issued firearms or other less-than-lethal weapons (e.g., expandable batons and/or OC aerosol sprays) until they have successfully completed basic firearms and other use of force training.

- B.** Basic use of force training shall consist of that provided during the Criminal Investigator Training Program at FLETC, or comparable training provided or approved by the DAIGI and the AIGI.
- C.** Firearms training requirements are found in chapter 21 of the Special Agent Handbook.

024.030 Use of Force Instructors

- A.** OI SAs will serve as use of force instructors. The instructors will successfully complete use of force instructor training at FLETC or other use of force instructor training course(s) approved by a DAIGI and the AIGI.
- B.** Use of force instructors must be recertified every three to five years. Recertification standards are developed by OI and coordinated by the TPM.
- C.** The use of force instructor will maintain a file of the training provided to SAs for the application of less-than-lethal force techniques, including baton and OC aerosol training. The use of force instructor will ensure that those scores and/or certifications and/or description(s) of less-than-lethal force training are entered into the Training database.
- D.** During periodic use of force training, each SA will ensure that his/her issued expandable baton functions properly and that any issued OC dispenser is leak free and is in generally good condition. Any weapon determined by an instructor to be unserviceable must be withdrawn from service and replaced from FD inventories.
- F.** Instructors are encouraged to enroll in professional organizations (e.g., the International Association of Law Enforcement Firearms Instructors [IALEFI]) and to attend available regional and/or national conferences offered by those organizations.
- G.** Instructors are appointed or removed at the discretion of the SAC, DAIGI, or AIGI.

024.040 Reporting Use of Force Incidents (Shooting Incidents)

- A.** SAs must immediately report any shooting incident involving OI personnel to the SAC or, in his/her absence, the ranking supervisor.
- B.** The SAC or, in his/her absence, the senior supervisor present, will notify the AIGI by telephone of any OI-involved shooting incident as soon as possible. This oral notification will be followed by a written report to the AIGI, with a copy to the appropriate DAIGI, by the fastest means possible. In all cases, a preliminary report of the shooting incident must be sent within 24 hours. This report must include, but is not limited to, the following facts:
 - 1.** The time, date, and location where the incident occurred.
 - 2.** The names of all persons involved in the incident, and their affiliations.

3. The names and affiliations of any news media representative present.
4. The name(s) of any person(s) injured; a description of the injuries; and the name, location, and telephone number of all medical facilities used to treat the injured.
5. A description and estimate (if possible) of any property damage.
6. A narrative synopsis of the incident, including case number.
7. The name(s) of any person(s) arrested and a description of the offenses charged.
8. The name of the lead investigative agency, including the title and telephone number of the lead investigator(s).
9. The make and type of any and all weapons used, the total number of rounds expended, and the condition of the weapon after the shooting (slide back, magazine empty, round chambered, etc.).
10. A detailed summary of all statements made to any news media representative since the event occurred.
11. A detailed summary of statements (including copies, if in writing) made to other law enforcement agencies by witnesses to, or participants in, the incident.
12. A complete explanation of the involvement (if any) of the United States Attorney's Office, the Office of the Counsel to the Inspector General, or the SSA regional Office of the General Counsel.
13. The identity of the OI supervisor responsible for the initial report of the incident.

024. 050 Incidents Involving Less-Than-Lethal Force

- A. Any SA who witnesses or participates in the use of less-than-lethal force involving OI personnel must report the incident to his/her OI supervisor.
- B. The SAC or, in his/her absence, the senior supervisor present, will notify the AIGI by telephone of any injuries, actual or alleged, resulting from the incident. The oral notification will be followed within 24 hours by a written report to the AIGI, with a copy to the DAIGI, and will include elements similar to those outlined in Section 021.120 B.

024. 060 Post-Incident Procedures

- A. SAs have the responsibility to render assistance and protection to any person(s) involved in a use of force incident.
 1. SAs involved in any use of force incident will ensure that all injured persons receive necessary medical care. This responsibility includes care for any injured suspect(s).

2. Medical and other law enforcement authorities on the scene must be advised of the status of any suspect/defendant who has been injured and requires medical assistance.
3. SAs will ensure that the agent(s) directly involved in the shooting incident is removed from the scene as soon as practical. An on-scene supervisor (or the senior agent) will accomplish this after coordinating this action with local authorities or state investigating authorities.
4. SAs will not discuss the incident with anyone other than supervisory personnel conducting the initial inquiry, or entities having formal investigative jurisdiction. All agents may exercise their right to legal counsel, as appropriate.

Questions agents are expected to answer are:

1. Are you injured?
2. If you know of anyone who was injured, what is his or her location?
3. In what direction did you fire your weapon(s)?
4. If any suspects are at large, what are their descriptions?
5. What was their direction of travel?
6. How long ago did they flee?
7. For what crimes are they wanted?
8. With what weapons are they armed?
9. Does any evidence need to be preserved?
10. Where is it located?
11. Did you observe any witnesses?
12. Where are they?

B. Actions at the scene of a shooting include:

1. Ensure aid is being rendered and notifications are made.
2. Request assistance from local police.
3. Preserve the scene and any evidence.
4. Secure the scene and initiate an entry/exit log.
5. Secure weapons and note their condition before making safe.
6. Establish a Command Post and lines of communication.
7. Identify witnesses and record license plate numbers.
8. Designate a radio frequency for responding agents.
9. Identify individuals with the most knowledge of the incident and have them provide a summary.

10. Agents involved in the shooting may be asked by local authorities to turn over their weapons. This should be done out of the view of the public or press and a receipt or inventory must be obtained.
 11. Determine if additional assistance is needed at secondary locations (e.g., hospital, police station, employee residence).
 12. Separate agents who took part in or are involved in the shooting.
 13. Remove all employees who fired shots from the immediate scene to a neutral law enforcement facility.
 14. Brief local authorities when they arrive.
 15. Provide a briefing to the SAC or appropriate OI supervisor. The SAC or appropriate OI supervisor is responsible for notifying OI HQ (AIGI or DAIGI and the Office of Quality Assurance and Professional Responsibility), the U.S. Attorney's Office, and the FBI.
 16. Establish which agency will take the lead. (This decision is best made during joint operations prior to any occurrence of an incident.) The lead agency will
 - a. be responsible for the other agencies at the scene;
 - b. complete the processing of the crime scene; and
 - c. direct the course of the investigation.
 17. Provide general assistance to the local agency in collecting any firearms that were discharged. Preservation of the scene includes securing all discharged OIG weapons for later ballistic comparison and technical examination. This should be accomplished by a supervisor and coordinated with local officials. The chain of custody must be documented.
- C. The SAC or his/her designee will personally supervise the initial investigation.
1. Statements will not be solicited from any SA involved in, or present during, a shooting until such time as the SA has regained his/her composure and, if appropriate, been given an opportunity to consult with an attorney or medical physician.
 2. INITIAL STATEMENTS CONCERNING THE INCIDENT WILL ONLY BE GIVEN TO THE SAC OR HIS/HER DESIGNEE.
 3. The SAC or his/her designee will be responsible for preparing the written report.
- D. If an SA has been injured, a designated OI employee will transport members of his/her immediate family to the appropriate medical facility and remain with them until released by the SAC, DAIGI, or AIGI. FD personnel should be informed about the ongoing situation, but cautioned against discussing it outside OI. No information concerning a

shooting or other injury shall be released to **anyone** outside SSA OIG without the express approval of the SAC.

- E.** OIG/OI policy is not to disclose to the media or otherwise make public the identity of SAs involved in shootings or other less-than-lethal force incidents. All media inquiries must be directed to the OIG Public Affairs Officer.
- F.** Post-trauma-stress counseling and/or intervention, including but not limited to that provided by the SSA Employee Assistance Program (EAP), shall be made available to all SAs involved in shooting incidents. Depending on the circumstances of the shooting, participation in such counseling may be mandatory or discretionary. Participation in a post-trauma-stress treatment program will be:
 - 1.** mandatory, if the use of force incident resulted in a fatality or serious physical injury to anyone, or if the SA requests such assistance.
 - 2.** discretionary, if the use of force incident did not result in a fatality or serious physical injury to anyone involved.

If counseling, including that provided by or through EAP, is mandatory, the SA should initiate appropriate contact within 72 hours of the shooting incident unless medically unable to do so. Information about how to obtain counseling is found in the [*OIG Administrative Policy and Procedures Manual \(See Chapter 21, Critical Incidents\)*](#).

- G.** No SA present during, or involved in, the use of force incident should be actively involved in the follow-up investigation.
- H.** Handling and Reporting of Injuries
 - 1.** Injured suspects: At least one armed SSA OIG agent and one other armed officer should accompany an injured suspect to the hospital. Assign personnel to the hospital if it has not already been done. Any statement or admissions should be recorded and later made part of the agent's report.
 - 2.** Injured Employees: Encourage any injured employee to personally call their family if they are able to do so. An agent should accompany injured employees to the hospital. Transportation to the hospital should be provided to family members as soon as possible. Assign an agent to the hospital if it has not already been done. If the injured employee is unable to call his family, someone should be assigned to notify the family in person. If possible, this notification should be made by someone who personally knows the family, and a **supervisor** should accompany them. The role of this employee will be to assist the family in any way they can.
- I.** Procedures in the event of a fatal shooting.
 - 1.** If an employee is deceased, the supervisor should not give the family false hope that they may be alive. **DO NOT** make this notification over the phone. **DO NOT** leave family members alone after making a death notification.

2. The notifying supervisor and agent should encourage a family member or friend to come to the location where the death notification is made. Depending on the situation, this could occur at the hospital.
3. The family should be transported in a government vehicle. If they refuse, they should be encouraged to follow the agents to the hospital.
4. Protect the family from the news media. The hospital agent should coordinate with security to have a private room or similar location available in which the family can wait.
5. An employee should remain with the family until the situation stabilizes. Family members should be offered transportation from the hospital back to their residence.

J. Discussion of the event

1. The SAC should conduct interviews in cooperation with local authorities.
2. DO NOT allow compelled statements to be taken from involved employees without approval from the U.S. Attorney's Office.
3. AUSAs and OIG/OC attorneys are not authorized to provide on-the-scene legal advice to employees concerning their potential personal liability as a result of a critical incident.
4. AUSAs are not authorized to enter into attorney-client relationships with government employees unless or until representation has been approved by an official of the Civil Division. Prior to authorization, the AUSAs are permitted to represent only the interests of the U.S. Government. Therefore, any statements made by an employee to an AUSA are not considered privileged communication and may be subject to disclosure.
5. Employees should be afforded reasonable time to regain their composure and understand their rights before any attempt is made to interview them.

IT IS OIG POLICY THAT NO STATEMENTS WILL BE PROVIDED TO OUTSIDE AGENCIES UNTIL THE EMPLOYEES INVOLVED HAVE HAD AN OPPORTUNITY TO CONSULT WITH COUNSEL.

6. Employees must cooperate with other agencies if circumstances pose a threat to public safety.
7. Upon arrival at a neutral location, the SAC should encourage the involved employee(s) to personally call their families to assure them that they are not injured.

K. SAs directly involved in any use of force incident that results in injury or death may take five days of administrative leave with the concurrence of the SAC.

Administrative Inquiry

- A.** The Office of Quality Assurance and Professional Responsibility (OQAPR) is responsible for conducting administrative inquiries of OI agents in use of force incidents, discharge of firearms in a non-training setting, and shooting accidents during a training activity. However, the Deputy Inspector General (DIG), at his discretion, may refer the investigation of certain incidents to the Assistant Inspector General for Investigations (AIGI). The AIGI will select someone to lead the inquiry. Regardless of whether the team is from OQAPR or OI, the team will conduct a thorough, objective, and timely inquiry. The report of this inquiry is separate and distinct from any report submitted at the time of the incident, or any official investigation done by outside law enforcement authorities.
- B.** The OQAPR or OI inquiry team leader will prepare a comprehensive report of its findings and deliver it to the AIGI. The content and format of the report will be in accordance with OQAPR or OI policy.
- C.** The AIGI will convene the SSA OIG Use of Force/Shooting Review Board (UFSRB) to review all SSA OIG use of force incidents and discharges of a firearm investigated by OQAPR or assigned by the DIG to OI to investigate. The UFSRB will meet within 30 days after receipt of the OQAPR or OI report of investigation.
- 1.** The UFSRB is comprised of the following persons: DAIGI (outside the agent's chain-of-command, will chair the UFRB); SAC Criminal Investigations Division; SAC Policy and Administration Division; Deputy Chief Counsel to the Inspector General; and one other person selected by the DIG.
 - 2.** The UFSRB will review each incident to determine the following:
 - a. If the facts and circumstances surrounding each event have been accurately and completely reported;
 - b. If the SSA OIG agent was acting within the scope of his/her authority;
 - c. If the agent's actions were reasonable, legal, and within OI's policy on the use of deadly force; and,
 - d. If the use of force was justified.
 - 3.** If the UFSRB finds all of the above to be true, the UFSRB can administratively close the inquiry. If the UFSRB determines there was misconduct or malfeasance by an SSA OIG agent, it will provide its findings to the appropriate management official for administrative adjudication. The UFSRB will also make recommendations, as appropriate, relating to training, equipment, procedures, etc.
 - 4.** The SAC Policy and Administration Division will review the incident to revise training curricula and incorporate "lessons learned," as warranted.

Emergency, Interim Legal Representation of Federal Law Enforcement Officials Involved in “Critical Incidents”

- B.** Under the policies and guidelines found in 28 C.F.R. sections [50.15](#) and [50.16](#), the Department of Justice (DOJ) may provide direct representation or retain private counsel at Government expense, as appropriate, to present and former employees who are sued, charged or otherwise the subject of judicial or administrative proceedings for acts done in the course of their official duties. These policies and guidelines apply to a line-of-duty discharge of a weapon or use of force resulting in death or serious bodily injury, following which a Federal law enforcement official needs representation because he/she has become the subject of a Federal, State, county or municipal criminal investigation related to the incident.
- C.** As a general matter, DOJ representation is provided to Federal employees after it is determined that they were acting within the scope of employment and it is in the interest of the United States to provide representation. However, in the immediate aftermath of this type of critical incident, emergency, the affected employee may need interim legal representation until the DOJ has had the necessary opportunity to consider the representation issue.
- C.** The term “critical incident” should be strictly defined as one in which there has been the use of force by a Federal employee in the line of duty which results in death or serious bodily injury. The phrase “serious bodily injury” generally means an injury that requires the hospitalization of the alleged victim.
- D.** At the time of the critical incident, personnel designated by the involved agency will contact the Torts Branch Deputy Assistant Attorney General or the Constitutional Torts Staff Director or Duty Attorney. The Constitutional Torts Staff will make an initial determination of scope of employment based upon the facts presented by the agency. In addition, the Constitutional Torts Staff will consider whether a Federal civil rights investigation has developed evidence, in the opinion of the Civil Rights Division, indicating there is potential prosecutive merit. If emergency representation is approved, the agency will contact a previously approved private attorney to coordinate representation.
- E.** Emergency representation by private counsel will be provided for a limited period until the Constitutional Torts Staff has an opportunity to consider the representation issue. In any event, however, such representation will be provided for no longer than one week, unless otherwise authorized by the Constitutional Torts Staff under exceptional circumstances. An investigating agency and/or the Civil Rights Division will have the continuing responsibility of advising the Constitutional Torts Staff of the initiation of an investigation, as well as its potential merit, to inform the consideration of whether emergency representation should continue during the one-week period.

In the event that the Constitution Torts Staff is unable to make a representation decision or declines to provide representation, the employee may, at his or her own expense, continue to be represented by the same private attorney. Current DOJ regulations pertaining to requests for reimbursement for the expenses of private counsel will then apply.

- F.** A private attorney will be provided on an emergency basis for a Federal, State, county or municipal criminal proceeding that arises out of the critical incident. However, a private attorney will not be provided for representation in an internal agency investigation arising out the critical incident. Such determination will be made by the Constitutional Torts Staff. Prior to accepting such representation, the employee will agree to turn over all non-testimonial evidence connected with the incident to the appropriate agency representative, including the employee's weapon, if appropriate.

- G.** The Constitutional Torts Staff will compile a listing of attorneys who agree to provide representation to Federal employees on this limited emergency basis. Such listing will be provided to all agencies for distribution to field offices. This list will be re-certified by the United States Attorney's Office in each district on a semiannual basis. Each United States Attorney's Office will establish a point of contact with the attorneys on the list.

At the time that emergency representation by private counsel is approved, the Constitutional Torts Staff will complete all necessary arrangement for payment of such legal services. All record-keeping tasks will be performed by the Constitutional Torts Staff.

GLOSSARY

A

ACSM	American College of Sports Medicine
AG	Attorney General
AIDS	Acquired Immune Deficiency Syndrome
AIGA	Assistant Inspector General for Audits
AIGER	Assistant Inspector General for Employee Relations
AIGRM	Assistant Inspector General for Resource Management
AIGI	Assistant Inspector General for Investigations
ALJ	Administrative Law Judge
AMFED	Allegation Management and Fugitive Enforcement Division
AMS	Allegation Management System
ASAC	Assistant Special Agent-in-Charge
AST	Administrative Support Team
AT	Analytics Team
AUSA	Assistant United States Attorney

B

BBP	Bloodborne Pathogen
-----	---------------------

C

CAN	Common Accounting Number
CBP	Customs and Border Protection
CD	Certificate of Deposit
CDC	Centers for Disease Control
CIG	Counsel to the Inspector General
CDI	Cooperative Disability Investigations
C.F.R.	Code of Federal Regulations
CI	Confidential Informant
CID	Criminal Investigations Division
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CISS	Center for Integrity and Security Support
CITP	Criminal Investigator Training Program
CMP	Civil Monetary Penalty
COOP	Continuity of Operations Plan
CPR	Cardiopulmonary Resuscitation
CSRS	Civil Service Retirement System

D

DAIGA	Deputy Assistant Inspector General for Audit
DAIGI	Deputy Assistant Inspector General for Investigations
DAIGRM	Deputy Assistant Inspector General for Resource Management
DCIG	Deputy Counsel to the Inspector General
DDS	Disability Determination Services
DFOH	Division of Federal Occupational Health
DHS	Department of Homeland Security
DIG	Deputy Inspector General
DFT	Digital Forensics Team
DO	District Office
DOB	Date of Birth
DODPI	Department of Defense Polygraph Institute
DOJ	Department of Justice
DTO	Divisional Training Officer

E

EAP	Employee Assistance Program
ECD	Electronic Crimes Division (renamed 1/13 now DFT)
EFT	Electronic Funds Transfer
EIC	Electronic Intelligence Center

F

FAA	Federal Aviation Administration
FBI	Federal Bureau of Investigation
FCRA	Fair Credit Reporting Act
FD	Field Division
FECA	Federal Employees Compensation Act
FEMA	Federal Emergency Management Agency
FERS	Federal Employees Retirement System
IAD	Intelligence and Analysis Division
FLETC	Federal Law Enforcement Training Center
FOH	Federal Occupational Health
FOIA	Freedom of Information Act
FOT	Field Operations Team
FPS	Federal Protective Service
FRC	Federal Records Center
FRE	Federal Rules of Evidence
FST	Field Support Team
FTCA	Federal Tort Claims Act
FY	Fiscal Year

G

GLPSC	Great Lakes Program Service Center
GOV	Government Vehicle
GRS	General Records Schedules
GSA	General Services Administration

H

HBV	Hepatitis B Virus
HEP	Health Enhancement Program
HHS	Health and Human Services
HIV	Human Immunodeficiency Virus
HQ	Headquarters

I

IAA	Inter-Agency Agreement
IALEFI	International Association of Law Enforcement Firearms Instructors
IG	Inspector General
IGCIA	Inspector General Criminal Investigator Academy
IGITP	Inspector General Investigator Training Program
IGTTP	Inspector General Transitional Training Program
IM	Investigative Memorandum
IMPAC	International Merchant Purchase Authorization Card
IRA	Individual Retirement Account
IRS	Internal Revenue Service
IRT	Investigative Response Team
ISCT	Investigative Support and Compliance Team

J

J&C	Judgment and Commitment Order
-----	-------------------------------

L

LE	Law Enforcement
LEAP	Law Enforcement Availability Pay
LEMUSE	Law Enforcement Methods Used

M

MAD	Manpower and Administration Division (renamed 1/13 PAD)
MAMPSC	Mid-America Program Service Center
MAR	Management Advisory Report

MATPSC	Mid-Atlantic Program Service Center
MBR	Master Benefits Record
MCS	Modernized Claims System
MGQT	Modified General Question Test
MOU	Memorandum of Understanding
MRO	Medical Reviewing Officer

N

NARA	National Archives and Records Administration
NCIC	National Crime Information Center
NEPSC	Northeastern Program Service Center

O

OA	Office of Audit
OC	Oleoresin Capsicum
OCIG	Office of the Counsel to the Inspector General
OCO	Office of Central Operations
ODAR	Office of Disability Adjudication and Review
ODP	Office of Disclosure Policy
OER	Office of External Relations
OGC	Office of General Counsel
OGE	Office of Government Ethics
OI	Office of Investigations
OIG	Office of the Inspector General
OJT	On-the-Job Training
OMB	Office of Management and Budget
OPAC	On-line Payment and Collection System
OPM	Office of Personnel Management
ORC	Operations Review Committee
ORM	Office of Resource Management
OSC	Office of Special Counsel
OSHA	Occupational Safety and Health Administration

P

PA	Privacy Act
PAD	Policy and Administration Division
PAO	Public Affairs Officer
PDD	Psychophysiological Detection of Deception
PHS	Public Health Service
PIN	Personal Identification Number
POMS	Program Operations Manual System
PPC	Practical Pistol Course

PPE Personal Protective Equipment
PSC Program Service Center
PT Policy Team

R

RA Resident Agent
RAC Resident Agent-in-Charge
RFPA Right to Financial Privacy Act
RLRO Regional Labor Relations Officer
ROI Report of Investigation
ROIA Report of Investigative Activity
RPAO Regional Public Affairs Officer

S

SA Special Agent
SAC Special Agent-in-Charge
SAH Special Agent Handbook
SCERS Seized Computer and Evidence Recovery Specialist
SEPSC Southeastern Program Service Center
SES Senior Executive Service
SGA Substantial Gainful Activity
SOP Standard Operating Procedure
SRAD Strategic Research and Analysis Division (renamed 1/13 FIAD)
SSA Social Security Administration
SSADO Social Security District/Branch Office
SSI Supplemental Security Income
SSN Social Security Number
SST Special Services Team

T

TPM Training Program Manager

U

USAO United States Attorney's Office
U.S.C. United States Code
USPIS United States Postal Inspection Service
USSS United States Secret Service

V

VWC Victim/Witness Coordinator
VWPA Victim and Witness Protection Act

W

WPSC

Western Program Service Center

Revised 07/14/09, 1/23/13

Index

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#)
[P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)



Abandoned Property	013.090
Abbreviated Account Query (AACT)	Exhibit 6-16
Access Documentation	006.030
Access To Social Security Information	Chapter 6
Access	
Documentation	006.030
EIF, by EIN (AEQY)	Exhibit 6-36A
EIF, by Name (AEQY).....	Exhibit 6-36
Employer Identification System, Alpha Access (AEQY)	006.130
Financial Records, Customer Consent & Authorization to (OI-59)	Exhibit 18-3
Initial, SSA Mainframe	006.120
Records.....	018.020
SSA Record Disclosure	006.010
Accountability Report	009.070
Accountability Report (OI-28C).....	Exhibit 9-5
Accounting for Interception Devices	008.010
Achievements, Monetary	003.130
Acquisition, Preservation, & Management of Evidence	Chapter 14
Action Memorandum (OI-42)	Exhibit 7-4
Actual Recoveries.....	003.130
Additional Subjects/Victims/Alias Data.....	Exhibit 3-2
Administration of the Fitness Assessment.....	022.130
Administrative Filing System	023.020
Administrative Inquiry	021.090
Administrative Law Judge.....	004.065
Administrative Policies & Procedures Manual.....	002.040
Administrative Sanctions.....	016.090
Administrative Support Functions - General	023.000
Admissibility, Relevancy & Competency of Evidence	014.020
Advice of Rights.....	010.050
Advice of Rights (OI-13).....	Exhibit 10-3
Advice of Rights - Non-Custodial (OI-13 NC)	Exhibit 10-4
Advice of Rights -Spanish (OI- I3 S)	Exhibit 10-5
Affirmation or Oath.....	010.100
Agreement Between SSA OIG & SSA Special Project Staff (OI-55).....	Exhibit 7-6
Agreement to Provide Information (OI-27A)	Exhibit 4-13
AIGI Policy Message	Exhibit 1-3
Allegations of Child Abuse	003.010
Allegations of Misuse of Official Time by Union Officials	004.140
Alpha Access to the Employer Identification System (AEQY).....	006.130

Alpha-Index Query (ALPH).....	Exhibit 6-20
Alphabet, International Phonetic.....	Exhibit 7-16
Alphident.....	006.130
Annual Certifications Checklist (Form OI-41).....	Exhibit 1-7
Annual Certification of Availability Hours (OI-50).....	Exhibit 2-4
Annual Training Requirements (Form OI-41A).....	Exhibit 1-8
Appearance, Initial	015.070
Approval of Undercover Operations	007.030
Approving Amounts by Officials	009.050
Arrestment	015.090
Arrests, Documenting of	003.140
Arrest Warrant.....	Exhibit 15-2
Arrest Warrants - Execution.....	015.040
Arrest Warrants - General	015.020
Arrest Without a Warrant.....	015.060
Assaults, investigation of	004.190
ATM Withdrawals, Disposition of Excess	009.020
Attorney General Guidelines for OIGs with Statutory Law Enforcement Authority	Exhibit 1-2
Attorney Representation, Employee.....	004.110
Audit Assistance in Criminal Investigations	004.280
Audit and Financial Forensic Assistance, Request for	Exhibit 3-14, Exhibit 4-20
Authority & Organization	Chapter 1
Authority	012.000, 017.010
Authority for LEAP.....	002.090
Authority to Carry Firearms	021.000
Availability Pay Certification (OI-49)	Exhibit 2-2
Avoidance of Informal Agreements	004.230

B	B	B	B	B	B	B	B	B
----------	----------	----------	----------	----------	----------	----------	----------	----------

Background Investigations.....	004.170
Education (Non-Criminal)	Exhibit 4-9
Employment (Non-Criminal)	Exhibit 4-10
Neighborhood (Non-Criminal).....	Exhibit 4-11
Back-up Weapons, Carrying	021.025
(b) (7)(E)	
Basic Firearms Training	021.060
Best Evidence Rule	014.040
BIC "D"	005.060
Blanket Declination	015.120
Bribes	004.070
Burden of Proof	014.030

C	C	C	C	C	C	C	C	C
----------	----------	----------	----------	----------	----------	----------	----------	----------

Carrying Back-up Weapons	021.025
--------------------------------	-------------------------

Carrying Issued Weapons.....	021.020
Case File Arrangement and Closing Checklist (OI-31).....	Exhibit 3-4
Case File Organization.....	003.110
Case File Arrangement and Closing Checklist.....	003.120
Case Management	Chapter 3
Case Numbering System.....	003.080
Case Opening Guidelines.....	003.070
Case Opening Guidelines for SSA Employee Investigations.....	004.050
Case Opening Priorities.....	003.060
Case Opening Procedures.....	003.050
Case Reviews.....	003.100
CDI Program and MOU.....	005.030
CDI Savings.....	003.130
CDR Query Screen (QCDR).....	Exhibit 6-12
CDR Selection Menu (MCDR).....	Exhibit 6-11
Center for Security and Integrity (CSI).....	004.030 , 006.050
Certification of Compliance with the Lautenberg Amendment (OI-82A).....	001.140
Certificate of Compliance with the Right to Financial Privacy Act of 1978 (OI-57).....	Exhibit 18-1
Certification	
Annual, Availability Hours (OI-50).....	Exhibit 2-4
Availability Pay (OI-49).....	Exhibit 2-2
General.....	006.040
Home-to-Work Use of Government Vehicles (OI-46).....	Exhibit 2-1
Review of the <i>Special Agent Handbook</i>	Exhibit 1-4 , 001.140
Certifications.....	006.040
Chain of Custody.....	Exhibit 14-3
Child Abuse	
Defined.....	017.030
Hotline and Field Division Responsibilities.....	003.040
Policy.....	003.010
CID Quarterly Case Reviews.....	003.210
CJIS Fingerprinting Supply Requisition Form.....	Exhibit 3-13 , 003.140
CIGIE.....	001.090 , 011.010
Civil Monetary Penalties & Administrative Sanctions.....	Chapter 16
Civil Monetary Penalty Authorities under Section 1129.....	Exhibit 16-1
Civil Monetary Penalty Investigative Referrals.....	016.050
Civil Monetary Penalty Reports of Investigation.....	016.060
Closing/Disposition of Investigative Files.....	003.170
Collateral Investigation.....	003.150
Collectability.....	016.030
Collections.....	016.080
Commonly Investigated Statutes.....	001.100
Communication(s)	
Interception of Wire or Oral.....	008.040
Radio.....	007.150
Comprehensive Integrity Review Program (CIRP).....	005.050
Computer Assistance in Employee Investigations.....	004.075
Computer Based Evidence.....	014.050
Computer Data Matches.....	006.070
Computer Generated Consent to Search (OI-26).....	Exhibit 13-6
Computer Research and Inquiries Team.....	004.075 , 005.090
Conduct While on Official Duty.....	002.030

Confidential Expenditures	009.030
Confidential Expenditures	Chapter 9
Confidential Informants	004.240
Contact Record (OI-27B)	Exhibit 4-14
Data (OI-27)	Exhibit 4-12
Deactivation	004.240
Expenditures	009.040
Implementation with Respect to,	017.050
Confidential Source Registration Card (OI-27C)	Exhibit 4-15
Confidential Sources	004.250
Congressional Inquires	002.170
Consensual Non-Telephone Monitoring	008.070
Consensual Telephone Monitoring	008.050
Consent to Monitor Non-Telephone Conversations	Exhibit 7-3
Consent to Monitor Non-Telephone Conversations (OI-25AL)	Exhibit 8-4
Consent to Monitor Telephone Conversations	Exhibit 7-5
Consent to Monitor Telephone Conversations (OI-25L)	Exhibit 8-2
Consent to Search Computers/Electronic Media (OI-91)	Exhibit 4-19
Consent to Search - Computer Generated (OI-26)	Exhibit 13-6
Consent to Search - Handwritten (OI-26L)	Exhibit 13-7
Consolidated Query (CNQY)	Exhibit 6-38
Contact with Person Seeking Records Under the Freedom of Information Act	019.040
Conspiring to Fraudulently Secure Benefits	004.070
Control of SSA's Claims, Files, and Documents	006.050
Cooperative Disability Investigations Program	005.030
Council of Inspectors General on Integrity and Efficiency (CIGIE)	001.090
(b) (7)(E)	
Credentials, surrender of	002.070
Criminal Complaint	Exhibit 15-1
Criminal Investigations	
Audit Assistance in	004.280
Federal Employee Rights in	004.090
Criminal Investigations Division	001.040
Criminal Procedures	Chapter 15
Critical Incidents, Enforcement Officials Involved in	024.080
Custodian's Activity Log for Confidential Funds	Exhibit 9-5
Custody, Chain of	Exhibit 14-3
Customer Consent & Authorization for Access to Financial Records (OI-59)	Exhibit 18-3
Customer Notice	Exhibit 18-4



DAIGI Memorandum for Employee Misconduct Cases Involving OI SAS	Exhibit 11-10
Data	
Additional Subjects/Victims/Alias	Exhibit 3-2
Computer Matches	006.070
Confidential Informant (OI-27)	Exhibit 4-12
Data Exchange Query Menu (DXQM)	Exhibit 6-21
DDS (Disability Determination Services)	005.030
Deactivation of Confidential Informants	004.240

Deceased Auxiliary Beneficiary Project (BIC "D")	005.060
Deceased Payee Investigations	004.040
Declination of Prosecution	015.120
DECOR (decentralized correspondence)	006.150
Definitions	010.030 , 017.030
Delayed Notification	018.040
Delayed Notification	018.040
Description of Property Acquired	Exhibit 14-2
Detail Earnings Query (DEQY)	Exhibit 6-27
Detail Earning Report (DEQR)	Exhibit 6-28
Detailed Office/Organization System (DOORS)	Exhibit 6-7
Dialed Number Recorder	008.030
Digest of Standards of Ethical Conduct	002.010
Digital Forensics Team	004.075
Disability Determination Service (DDS).....	005.030
Disability Investigations.....	004.030
Disclosure (of)	
Employee Identity	004.210
Information	002.160
Information Protected from.....	019.030
SSA Record & Information Disclosure.....	006.010
Disposition of Excess ATM Withdrawals	009.020
Diversion of Government Funds	004.070
Diversion, Pretrial	015.130
Divisional Responsibilities	003.030
DNA Samples.....	003.140
Documentation	
Access	006.030
Of Arrests	003.140
Of Monetary Achievements	003.130
Video.....	013.060
Documenting Arrests.....	003.140
Documenting Monetary Achievements	003.130
Drug & Alcohol Use	002.050
Duty of Care While in Official Custody.....	018.100
Duty of Employee to Cooperate.....	004.080



EDCOR (educational correspondence).....	006.150
EIF Access by EIN (AEQY)	Exhibit 6-36A
EIF Access by Name (AEQY)	Exhibit 6-36
EIF Response to Query (AEQY).....	Exhibit 6-37
Electronic Device Forensic Examinations	007.120
Electronic Sources of Information	007.110
Electronic Tracking Devices	008.020
Eligibility for LEAP.....	002.100
Emergency Lights and Sirens.....	002.060

Enforcement Officials Involved in "Critical Incidents"	024.080
Employee Case Notifications at Conclusion of Investigation	004.065
Employee Case Notifications at Start of Investigation.....	004.055
Employee Misconduct with Prosecution Potential.....	004.085
Employee's Right to Representation.....	004.110
Entrapment	015.010
Enumeration	001.090 , 003.060
Establishing Policy & Procedure.....	001.130
Establishment of the Office of the Inspector General	001.000
Ethical Conduct	
Digest of Standards of.....	002.010
Standards.....	002.000
Evidence	
Admissibility, Relevancy & Competency	014.020
Best Evidence Rule	014.040
Computer Based.....	014.050
Evidence/Property Report (OI-21)	Exhibit 14-1
Federal Rules of	014.010
Management Procedures	014.060
Evidence/Property Report (OI-21)	Exhibit 14-1
Examination, Pre-Employment Physical.....	022.020
Exceptions	018.030
Exclusions & Limitations.....	018.010
Exculpatory & False Exculpatory Statements.....	004.120
Execution of Search Warrants	013.070
Expenditures	
Confidential.....	009.030
For Confidential Informants.....	009.040
Exposure Control Plan	022.090
Extracts, Payment.....	006.055



Fact Sheets, SSA/OIG (General).....	011.040
FBI LEO (Law Enforcement On-Line)	007.110
FBI Notification Letter	Exhibit 1-6
FBI Form R-84 (Final Disposition Report).....	003.140 , 003.170
Federal Employee Advice of Rights (Form OI-15).....	Exhibit 4-1 , 004.090
Federal Employee Advice of Rights - Spanish (Form OI- 15 S).....	Exhibit 4-2 , 004.090
Federal Employee Rights in Criminal Investigations.....	004.090
Federal Employee Rights in Non-Criminal Investigations.....	004.095
Federal Law Enforcement Training Center (FLETC)	020.000
Federal Officers, Liability of.....	018.090
Federal Rules of Evidence.....	014.010
Federal Tort Claims Act.....	018.080
Field Division In-Service Training.....	020.060
Field Divisions	001.080
Field Office Address & Phone Numbers (FOADDRESS).....	Exhibit 6-8
Final Financial Institution Listing (RTN1).....	Exhibit 6-35

FinCEN (Financial Crimes Enforcement Network)	007.110
FinCEN Request for Information	Exhibit 7-11
Firearms	
Authority to Carry	021.000
General Conduct	021.010
Inventory Control & Safekeeping	021.050
Qualification Standards	021.090
Types/Ammunition	021.050
Use of Shotguns	021.030
<i>Firearms Policy and Training</i>	Chapter 21
Firearms Instructors	021.070
Firearms Qualification Standards	021.080
Fitness Assessment	022.130
Folder Query (FQY1)	Exhibit 6-41
Forensic Examinations, Electronic Device	007.120
Forensic Intelligence and Analysis Division	001.060
Form(s)	
Consent to Search Computers/Electronic Media (OI-91)	Exhibit 4-19
NICMS Criminal & Administrative Disposition (OI-9)	Exhibit 11-7
NICMS Disposition	Exhibit 3-5
Application for Special Deputation (Form USM-3R)	Exhibit 1-2
FBI - R-84(Final Disposition Report)	003.140, 003.170
Federal Employee Advice of Rights (Form OI-15)	Exhibit 4-1
Federal Employee Advice of Rights - Spanish (Form OI- 15 S)	Exhibit 4-2
Inventory (Attachment) (OI-23A)	Exhibit 13-5
Inventory (OI-18)	Exhibit 13-4
Inventory (OI-23)	Exhibit 14-4
Inventory (Attachment) (OI-23A)	Exhibit 14-5
Kalkines (Form OI-14)	Exhibit 4-3, 004.050, 004.100
Kalkines - Spanish (Form 01- 14 S)	Exhibit 4-4
Personal History Information (OI- 19)	Exhibit 3-7
Radio Network User Registration	Exhibit 7-15
Request for Information or Assistance (Form 01-56)	Exhibit 4-7
Report of Court Ordered Restitution/Judgment (Form 01-68)	Exhibit 3-6
Union Representative Advisory to SSA Employee (Form OI-80)	Exhibit 4-8, 004.110
Fraud	
Alert, Sample	Exhibit 1-5
Alert, National & Regional	001.170
Program Fraud Investigations	004.010
Residency	005.070
Title II	004.010
Title XVI	004.010
Voucher	004.070
<i>Freedom Of Information & The Privacy Act</i>	Chapter 19
Freedom of Information Act	019.000
Contact with Person Seeking Records Under	019.040
Fugitive Felon Program	005.040
Fugitive Felon Savings	003.130
Full Miranda Statement (OI-16C)	Exhibit 10-8
Full Titles of Selected Acronyms	006.080
Funds Administration	009.060

G G G G G G G G G

General Legal Matters.....[Chapter 18](#)
 Giglio Policy [015.140](#)
 Government Property Searches [004.260](#), [013.110](#)
 Government Vehicle Fleet Management..... [023.070](#)
 Government Vehicles, use of official..... [002.060](#)
 Grand Jury Information [014.070](#)
 Guide to Third Party Facilitator Investigations [Exhibit 5-1](#)
 Guidelines
 Administratively Closing Referrals..... [003.090](#)
 Case Opening [003.070](#)
 Case Opening, Allegations for SSA Employee Investigations..... [004.050](#)
 Investigative Guidelines [Chapter 4](#)
 Photo Lineup Guidelines..... [Exhibit 7-7](#), [007.090](#)
 Suspected Child Pornography on Agency Networks [Exhibit 7-12](#), [007.120](#)

H H H H H H H H H

Handwriting Sample (OI-29A)..... [Exhibit 7-13](#)
 Handwriting Specimen (OI-29B) [Exhibit 7-14](#)
 Handwritten Consent to Search (OI-26L) [Exhibit 13-7](#)
 Hearings & Appeals [016.020](#)
 Hearing, Preliminary [015.080](#)
 High Risk Query System (VHRQ), SSA’s Visitor Intake Process (VIP)..... [004.190](#)
 High Risk Situations [007.000](#)
 Homeland Security Projects [005.080](#)
 Hotline & Field Division Responsibilities [003.040](#)
 How to Use NICMS to Submit OI-68s..... [Exhibit 3-6A](#)

I I I I I I I I I

IAD - Request for FST IT Support [Exhibit 5-2](#)
 IAD Field Support Team..... [004.075](#), [005.090](#)
 IG Academy at FLETC [020.000](#)
 IG Subpoena Transmittal Letter..... [Exhibit 12-2A](#)
 Implementation with Respect to Confidential Informants..... [017.050](#)
 Incidents Involving Less-Than-Lethal Force [024.050](#)
 Indictment & Information [015.030](#)
 Individual Developmental Plan (IDP)..... [Exhibit 20-3](#), [020.050](#)
 Informant, Confidential..... [004.240](#)
 Information
 Access To Social Security Information..... [Chapter 6](#)

Agreement to Provide (OI-27A)	Exhibit 4-13
Disclosure of	002.150
Electronic Sources of	007.110
FinCEN Request for	Exhibit 7-11
<i>Freedom Of Information & The Privacy Act</i>	Chapter 19
Freedom of Information Act	019.000
Grand Jury	014.070
Non-Immigrant & Alien Status Verification Display (NIIS)	Exhibit 6-24
Numident Query Sensitive (NUMI)	Exhibit 6-18
Personal History Information Form (OI- 19)	Exhibit 3-7
Request for Information or Assistance (Form OI-56)	Exhibit 4-7
Information for Victims & Witness of Crime	Exhibit 17-1
Information Protected from Disclosure	019.030
Informing Applicants of the Mandatory Physical Examination Program	022.030
Initial Access to the SSA Mainframe	006.120
Initial Appearance	015.070
Initiating Undercover Operations	007.020
Injunctions & Testimonial Subpoenas	016.040
<i>Inspector General Subpoenas</i>	Chapter 12
Interception of Wire or Oral Communications	008.040
International Phonetic Alphabet	Exhibit 7-16
Interview(s)	
Conducting	010.060
<i>Interviews, Investigative Notes & Statements</i>	Chapter 10
Juveniles (Interviewing of)	010.040
Purpose	010.010
Introduction to SSI	006.000
Instructions for Completing & Filing the Enclosed Motion & Sworn Statement (OI-61 A)	Exhibit 18-7
Inventory Form (Attachment) (OI-23A)	Exhibit 13-5
Inventory Form (OI-18)	Exhibit 13-4
Inventory Form (OI-23)	Exhibit 14-4
Inventory Form (Attachment) (OI-23A)	Exhibit 14-5
Investigation(s)	
Audit Assistance (in Criminal Investigations)	004.280
Background	004.170
Civil Monetary Penalty Reports of	016.060
Collateral	003.150
Cooperative Disability Program	005.030
Deceased Payee	004.040
Disability	004.030
Federal Employee Rights in Criminal	004.090
Federal Employee Rights in Non-Criminal	004.095
Foreign Countries	004.270
Guide to Third Party Facilitator Investigations	Exhibit 5-1
Nature of OI	001.090
Non-Criminal Background, Education	Exhibit 4-9
Non-Criminal Background, Employment	Exhibit 4-10
Non-Criminal Background, Neighborhood	Exhibit 4-11
Notification to SSA at the Conclusion of,	003.180
Office of,	001.020
Program Fraud	004.010
Quality Standards	Exhibit 1-1

Representative Payees	004.020
Report of, (OI-4)	Exhibit 10-2 , Exhibit 11-3
Social Security Number Misuse	004.160
Specialized Report of, (OI-5A)	Exhibit 11-4
Threats & Assaults	004.190
Types	004.000
Investigative Checklist (OI-34)	Exhibit 11-8
Investigative Guidelines & Procedures	Chapter 4
Investigative Notes	010.080
Investigative Operations.....	007.000
Investigative Operations & Support	Chapter 7
Investigative Plan (OI-2).....	Exhibit 11-2
Investigative Project Management	Chapter 5
Investigative Projects	005.000
Investigative Projects Originating in OI Headquarters.....	005.010
Investigative Reports	Chapter 11 , 011.030
Issuance & Security of Weapons	021.090
IT Support – Request for SED	Exhibit 5-2

J J J J J J J J J

Jurat.....	010.110
Juveniles (Interviewing of).....	010.040

K K K K K K K K K

Kalkines (Form OI-14).....	Exhibit 4-3 , 004.050 , 004.100
Kalkines - Spanish (Form OI- 14 S).....	Exhibit 4-4

L L L L L L L L L

Lautenberg Amendment (OI-82A), Certification of Compliance	001.140
Law Enforcement Availability Pay (LEAP).....	002.080
Law Enforcement Methods Used (LEMUSE)	011.060
LEAP	
Authority	002.090
Eligibility	002.100
General.....	002.080
Opting out	002.140
Reporting Requirements.....	002.120
Rules	002.110
Tracking Work Hours	002.130
Legal Considerations Regarding the Use of Text Messaging	018.130

Letter Opting out.....	002.140
IG Subpoena Transmittal	Exhibit 12-2
Model Referral (to SSA – action needed)	Exhibit 4-6A
Model Referral (to SSA – no action needed)	Exhibit 4-6B
Transmittal - Account Information Only Under Right to Financial Privacy Act.....	Exhibit 18-12
Transmittal - Customer	Exhibit 18-6
Transmittal - Right to Financial Privacy Act.....	Exhibit 18-5
Less-Than-Lethal Force Incidents.....	024.050
Liability of Federal Officers.....	018.090
Liaison.....	001.150
Lineups.....	007.090



MBR.....	003.020 , 005.060 , 006.110
Mail Covers.....	007.080
Mail Cover Requests – USPS Procedures.....	Exhibit 7-6A
Mail Cover Transmittal Letter (OI-71).....	Exhibit 7-6B
Mail Cover Request form, USPS version.....	Exhibit 7-6C
Mandatory Periodic Physical Examinations.....	022.060
Master File Query	006.130
Master File Query Menu	Exhibit 6-4
Master File Query Menu (MFQM)	Exhibit 6-15
Media Relations	002.150
Medical Standards & Physical Requirements	022.010
Memorandum	
Action.....	Exhibit 3-1
Action (OI-42).....	Exhibit 7-3
DAIGI, Employee Misconduct Cases Involving OI SAS	Exhibit 11-10
Sample Request (OI-24).....	Exhibit 8-3
Transmission (OI-7).....	Exhibit 11-6
Understanding (MOU)	001.110 (FBI)
(Review of MOU).....	001.130
Menu	
CDR Selection (MCDR)	Exhibit 6-11
Data Exchange Query (DXQM).....	Exhibit 6-21
Master File Query	Exhibit 6-4
Master File Query (MFQM).....	Exhibit 6-15
Miscellaneous (MISM)	Exhibit 6-33
National Directory New Hire, Wage, & Unemployment (NDNH).....	Exhibit 6-22
Prison Systems	Exhibit 6-14
Representative Payee Main (RPM)	Exhibit 6-9
SSA Main (VTAM)	Exhibit 6-1
SSA (Main)	Exhibit 6-3
Title II (T2SM).....	Exhibit 6-5
Message, AIGI	Exhibit 1-3
Methodology	019.020
Methodology for Calculating Disability Program Savings in CDI Program.....	003.130
Miscellaneous Menu (MISM)	Exhibit 6-33

Misuse of SSA Data Bank Information/System Security Violation.....	004.070
Misuse of SSN.....	004.160
Mobile Device Inventory Worksheet (Form OI-94)	Exhibit 7-22
Model Referral Letter(s).....	004.065
Model Referral Letter to SSA - Action Needed	Exhibit 4-6A
Model Referral Letter to SSA – No Action Needed.....	Exhibit 4-6B
Modern Enumeration System (MES).....	005.050
Modernized Claim System (MCS)	006.020
Modernized System Operations Manual (MSOM)	006.100
Monetary Achievements	003.130
Monitoring	
Consensual Non-Telephone	008.070
Consensual Telephone	008.050
Consent, Non-Telephone Conversations.....	Exhibit 7-5
Consent, Non-Telephone Conversations (OI-25AL)	Exhibit 8-4
Consent, Telephone Conversations.....	Exhibit 7-4
Consent, Telephone Conversations (OI-25L)	Exhibit 8-2
Field or Undercover Operations.....	007.050
Nonconsensual	008.000
Request for Approval of Consensual Telephone.....	008.060
Monthly Verification of Statistics	003.190
Motion for Order Pursuant to Customer Challenge Provisions of the Right to Financial Privacy Act of 1978 (OI-61)	Exhibit 18-8
Motor Vehicles.....	018.110
Mutual Assistance Agreement.....	001.180



National & Regional Fraud Alerts.....	001.170
National Directory New Hire, Wage & Unemployment Menu (NDNH).....	Exhibit 6-22
Nature of OI Investigations	001.090
NCIC (National Crime Information Center)	007.110
NICMS Case Opening Report.....	Exhibit 3-1
NICMS Case Opening Report (OI- 1).....	Exhibit 11-1
NICMS Criminal & Administrative Disposition Form (OI-9).....	Exhibit 11-7
NICMS Disposition Form	Exhibit 3-6
NICMS Entries for Administrative Sanctions Referrals	016.110
NICMS, Updating of the Status of Employee Cases	004.150
NLETS (National Law Enforcement Telecommunications System)	007.110
No Match Letters.....	006.150
Noncompliance	012.030
Nonconsensual Monitoring	008.000
Non-Criminal Background Investigation: Education.....	Exhibit 4-9
Non-Criminal Background Investigation: Employment.....	Exhibit 4-10
Non-Criminal Background Investigation: Neighborhood	Exhibit 4-11
Non-Custodial Advice of Rights Statement (OI-16B)	Exhibit 10-7
Non-Immigrant Information & Alien Status Verification Display (NIIS)	Exhibit 6-24
Notice, Customer.....	Exhibit 18-4
Notice to Customer for Transfer of Records	Exhibit 18-11

Notifications for OIG Employee Allegations of Misconduct.....	004.060
Notification to SSA at the Conclusion of an Investigation.....	003.180
Numident (NUMI)	Exhibit 6-19, 006.020
Numident Query Sensitive Information (NUMI)	Exhibit 6-18

O O O O O O O O O O

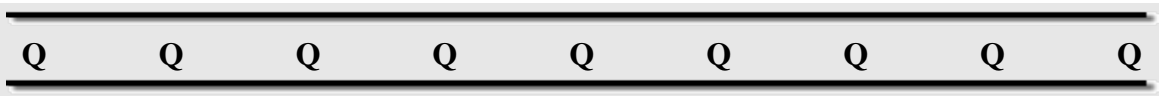
Oath or Affirmation.....	010.100
Oaths, Affirmations, & Law Enforcement Authority.....	001.110
Obtaining a Summons	015.050
Obtaining Confidential Funds	009.010
Obtaining Descriptive Factors.....	010.070
<i>Occupational Health & Wellness</i>	Chapter 22
Office of Central Operations (OCO)	004.030
Office of Disability Adjudication and Review (ODAR)	003.040, 004.065
Office of Government Ethics	004.055
Office of Investigations.....	001.020
Office of the Inspector General	
Actions After Receipt of Potential Sanction Referrals.....	016.100
Establishment	001.000
Health Enhancement Program.....	022.100
SSA Fact Sheets	011.040
Subpoena.....	Exhibit 12-1
Transmittal Register.....	Exhibit 9-7
Office of Public Disclosure (SSA)	019.040
Office of Quality Assurance and Professional Responsibility	004.060
Official Duty Conduct.....	002.030
Official Time, allegations of misuse	004.150
Official Vehicle Use.....	002.060
OI Polygraph Examination Request Worksheet.....	Exhibit 7-9
OI Standard Operating Procedure for Psychological Detection Of Deception.....	Exhibit 7-8
OIG Actions After Receipt of Potential Sanction Referrals	016.100
OIG Subpoena.....	Exhibit 12-1
OIG Transmittal Register	Exhibit 9-7
On-the-Job Training & the Mentoring Program.....	020.040
On-the-Job Training Guide	Exhibit 20-2
Opting Out of (LEAP).....	002.130
Organizational Structure	001.010
Organizational Representative Payee Cases	003.230
Other Forensic Examinations	007.130
Outside Activities.....	002.040

P P P P P P P P P

PACER (U.S. Treasury Checks)	007.110
------------------------------------	-------------------------

Payment.....	020.020
Payment History by BIC (PHU1).....	Exhibit 6-32
Payment History Update System Queries (PHUS).....	Exhibit 6-31
Payment Extracts.....	006.055
Payment Extract Request Letter.....	Exhibit 6-0
PCS (Program Service Center, SSA).....	004.030
Periodic Unannounced Audits of Unexpected Confidential Fund Balances	009.080
Permits to Carry Firearms	021.100
Personal History Information Form (OI-19)	Exhibit 3-8, Exhibit 10-1
Personally Identifiable Information Safeguarding Guidelines	006.160
Personally Identifiable Information Outside of OIG Security Space, Transportation of.....	Exhibit 6-45
Phonetic Alphabet, International.....	Exhibit 7-16
Photo Lineup Guidelines.....	Exhibit 7-7, 007.090
Photocopy Request (PEPH)	Exhibit 6-6
Physical Conditioning Under the Office of the Inspector General Health Enhancement Program	022.110
Physical Requirements & Medical Standards	022.010
Pledges of Confidence.....	004.220
Policy	003.010, 007.010, 011.020, 013.010, 017.020
Policy & Administration Division.....	001.050
Policy Directive.....	010.000
Policy Message, AIGI	Exhibit 1-3
Policy Regarding the Transportation of Personally Identifiable Information (PII) Outside of OIG Secure Space	006.160
Policy Regarding Notice to Executor or Administrator of Estate When Requesting Records of a Deceased Beneficiary.....	018.060
Policy Regarding the Disclosure to Federal Prosecutors of Potential Impeachment Information Concerning SSA Office Of the Inspector General Employees Who are/or Witness in Federal Criminal Cases (Giglio Policy)	015.140
Policy Statement.....	006.010, 019.010
Policy Statement of the Department of Justice Regarding the Use of Deadly Force	Exhibit 21-1
Polygraph	007.100
POMS	003.020, 006.020, 006.090
Pornography Guidelines for Suspected Child Pornography on Agency Networks.....	Exhibit 7-12
Post-Incident Procedures.....	024.060
Post Referral Activities	016.070
PowerPoint training – Quarterly Employee Case Report.....	004.150
Pre-Employment Physical Examinations	022.020
Preliminary Hearing	015.080
Preparatory Checklist for Search Warrant Affidavit (OI-35).....	Exhibit 13-1
Pretrial Diversion	015.130
Prison Systems/Fugitive Felon (PFSM).....	Exhibit 6-13
Prison Systems Menu.....	Exhibit 6-14
Privacy Act of 1974	019.050
Requests	019.060
Violations	019.070
Procedural Requirements Under Section 1129.....	016.010
Procedures	010.040
Administrative Policies & Procedures Manual	002.040

Case Opening	003.050
Evidence Management Procedures	014.060
<i>Investigative Guidelines & Procedures</i>	<i>Chapter 4</i>
OI Standard Operating, Psychological Detection Of Deception	Exhibit 7-8
Post-Incident	024.060
Processing Center Action Control System (PCACS)	006.130
Program(s)	
CDI and MOU	005.030
Comprehensive Integrity Review (CIRP)	005.050
Cooperative Disability Investigative	005.030
Fugitive Felon	005.040
Fraud Investigations	004.010
Informing Applicants of the Mandatory Physical Examination	022.030
Office of the Inspector General Health Enhancement	022.100
On-the-Job Training & the Mentoring Program	020.040
Operations Manual System (POMS)	006.090
Service Center, SSA (PCS)	004.030
Physical Conditioning Under the OIG Health Enhancement	022.110
<i>Victim & Witness Assistance</i>	<i>Chapter 17</i>
Program Service Center (PCS)	004.030
Project(s)	
Deceased Auxiliary Beneficiary (BIC "D")	005.060
Homeland Security	005.080
Investigative	005.000
<i>Investigative Project Management</i>	<i>Chapter 5</i>
Worksite Enforcement Operations	005.085
Prosecution	
Declination	Exhibit 15-3, 015.120
Report (OI-6)	Exhibit 11-4
Waiver of, to Obtain Employee Cooperation	004.100
Protecting the Identity of Employee Allegers	004.200
Protections Afforded by the U.S. Constitution	013.020
Property	
Abandoned	013.090
Badges and Credentials	023.010
Body Armor	023.010
Description of Acquired	Exhibit 14-2
Evidence/Property Report (OI-21)	Exhibit 14-1
Management	023.010
Policy	023.010
Property for New Employees	023.010
Searches of Government Owned	004.260, 013.110
Purpose (Confidential Expenditures, Search and Seizure)	009.000, 013.000
Purpose of Interviews	010.010



Quality Assurance	001.160
Quality Standards	011.010

Quality Standards for Investigations	Exhibit 1-1
- General Standards	Page 2
- Qualitative Standards	Page 8
- Appendices	Page 15
Quarterly Case Reviews by CID	003.210
Quarterly Employee Case Report (PowerPoint training)	004.150
Query	
Abbreviated Account (AACT).....	Exhibit 6-16
Alpha Index (ALPH)	Exhibit 6-20
CDR Screen	Exhibit 6-12
Consolidated (CNQY).....	Exhibit 6-38
Data Exchange Menu (DXQM)	Exhibit 6-21
Detail Earnings (DEQY)	Exhibit 6-27
EIF Response to (AEQY)	Exhibit 6-37
Folder (FQY1).....	Exhibit 6-41
Master File	006.130
Master File Menu (MFQM)	Exhibit 6-4 , Exhibit 6-15
Numident Sensitive Information (NUMI).....	Exhibit 6-18
RP Response Selection List (RQSL).....	Exhibit 6-10 , Exhibit 6-39
SSA Claims Control System (SSACCS).....	Exhibit 6-17
Standard (SQRY)	Exhibit 6-40A
Standard & Reply (SQRY).....	Exhibit 6-40B
Summary Earning (SEQY)	Exhibit 6-25
Query Master.....	006.110



Radio Communications	007.150
Radio Network User Registration Form.....	Exhibit 7-17
Receipt for Payment to Informant (OI-28B)	Exhibit 9-3
Receipt of Allegations from SSA.....	003.020
Regional Security Officer.....	003.020
Record(s)	
Access	018.020
Confidential Informant Contact Record (OI-27B)	Exhibit 4-14
Financial Records, Customer Consent & Authorization for Access (OI-59)	Exhibit 18-3
Request for NCIC/NLETS Records Checks	Exhibit 7-10
SSA, Access & Disclosure	006.020
SSI Complete (SSID)	Exhibit 6-30
Transfer	018.050
Transfer, Another Agency or Department	Exhibit 18-10
Transfer, Notice to Customer	Exhibit 18-11
Recoveries	
Actual	003.130
Scheduled	003.130
Regional Labor Relations Officer (RLRO)	004.105
Registration Card, Confidential Source (OI-27C).....	Exhibit 4-15
Removals (Rules of Criminal Procedure - Rule 40).....	015.110
Re-Opening of Previously Closed Cases.....	003.200
Report	

Accountability	009.070
Accountability (OI-28C)	Exhibit 9-6
Alleged SSA Employee Misconduct.....	Exhibit 4-5, 004.055
Biweekly Activity	002.110
Biweekly Activity (Special Agent) (OI-33)	Exhibit 2-3
Civil Monetary Penalty (CMP)	016.060
Court Ordered Restitution/Judgment (OI-68)	Exhibit 3-7
Detail Earning (DEQR).....	Exhibit 6-28
Employee Misconduct to Headquarters	011.050
Evidence/Property (OI-21).....	Exhibit 14-1
Intercept (OI-24A)	Exhibit 8-1
Investigation.....	Exhibit 3-9
Investigation (OI-4).....	Exhibit 10-2, Exhibit 11-3
Investigation - Disability (OI-4D).....	Exhibit 3-10
Investigation (OI-4D CDI format)	Exhibit 3-10
Investigation , Specialized (OI-5A)	Exhibit 11-6
Prosecution (OI-6).....	Exhibit 11-4
Shooting Incident	021.110
SSA OIG Fitness Evaluation.....	Exhibit 22-3
Summary Earning Report (SEQR).....	Exhibit 6-26
Reporting the Results of Undercover Operations.....	007.060
Reporting of Judgments & Court Ordered Restitution	003.160
Reporting the Results of Periodic Physical Examinations	022.080
Representation.....	018.120
Representative Payee Investigation.....	004.020
Representative Payee Main Menu (RPMM)	Exhibit 6-9
Reprisals Against SSA Employees.....	004.180
Request for Approval of Consensual Telephone Monitoring.....	008.060
Request for Approval of Special Investigative Operation.....	Exhibit 5-3
Request for Approval to Establish Investigative Project.....	Exhibit 5-0
Request for Audit and Financial Forensic Assistance	Exhibit 3-14, Exhibit 4-20
Request for Information or Assistance (Form 01-56)	Exhibit 4-7, 004.080
Request for NCIC/NLETS Records Checks.....	Exhibit 7-10
Request for IAD IT Support.....	Exhibit 5-2
Request for Testimony/Information/Records Needed from SSA for Prosecution	006.060
Request from Field Divisions to Establish Investigative Projects.....	005.020
Requesting Approval for Workday Conditioning Activities	022.120
Requesting Deputation	001.120
Requests for Investigative Activities	
by Another Division (Collateral Investigations)	003.150
Required for the 1811 Position.....	022.140
Residency Fraud.....	005.070
Response Letter for SSN Queries.....	Exhibit 6-42
Responsibilities	017.040, 020.010
Divisional	003.030
Hotline & Field Division.....	003.040
Responsibilities & Conduct	Chapter 2
Review by Public Health Service Medical Officer	022.050
Rights	
Advice of.....	010.050
Advice of (OI-13).....	Exhibit 10.3
Advice of, Non Custodial (OI-13 NC).....	Exhibit 10-4

Advice of, Spanish (OI-13 S).....	Exhibit 10-5
Federal Employee Advice of (OI-15).....	Exhibit 4-1
Federal Employee Advice of, Spanish (OI-15 S).....	Exhibit 4-2
Federal Employee, Criminal Investigations.....	004.090
Federal Employee, Non-Criminal Investigations.....	004.095
Non-Custodial Advice Statement (OI-16B).....	Exhibit 10-7
Statement of Consumer, Under Right to Financial Privacy Act (OI-58).....	Exhibit 18-2
Right to Financial Privacy Act of 1978.....	018.000
Right to Representation, Employee's.....	004.110
Routing Transit Number (RTND).....	Exhibit 6-34
RP Query Response Selection List (RQSL).....	Exhibit 6-10, Exhibit 6-39
Rules for LEAP.....	002.110
R-84 (FBI Form - Final Disposition Report).....	003.140, 003.170



Sale of Social Security Account Number Cards.....	004.070
Sample Fraud Alert.....	Exhibit 1-4
Sample Request Memorandum (OI-24).....	Exhibit 8-3
Savings, Calculation of.....	003.130
Scheduled Recoveries.....	003.130
Scheduling of Periodic Physical Examinations.....	022.070
Scheduling Pre-Employment Physicals.....	022.040
Search – Computers/Electronic Device.....	004.075, 007.120, 013.080
Search Incident to Arrest.....	013.080
Search & Seizure	Chapter 13
Search Warrants - General.....	013.030
Search Warrant Supplies Inventory/Raid Kit (OI-36).....	Exhibit 13-2
Searches of Government Property.....	004.260, 013.110
Section 1129 - False Statements & Representation.....	016.000
Security Officer, Regional.....	003.020
Shotgun Sign-Out Log.....	Exhibit 21-1
Shotguns, Use of.....	021.030
Sirens, Use of.....	002.060
Social Security Number (SSN) Misuse Investigations.....	004.160
Spanish Forms	
Advice of Rights -Spanish (OI- I3 S).....	Exhibit 10-3
Federal Employee Advice of Rights - Spanish (Form OI- 15 S).....	Exhibit 4-2
Kalkines - Spanish (Form 01- 14 S).....	Exhibit 4-4
Special Agent Handbook.....	001.130, 001.140
Special Agent Handbook (Clarification of).....	001.090
Special Indicator 7.....	005.050
Special Indicator 8.....	005.050
Special Interest Cases.....	003.220
Special Situations.....	010.120
Specialized Report of Investigation (OI-5A).....	Exhibit 11-4
SS-5 Requests.....	006.140
SSA Claims Control System Query (SSACCS).....	Exhibit 6-17
SSA Employee(s)	
Case Opening Guidelines for SSA Employee Investigations.....	004.050

Investigation of Threats & Assaults Against.....	004.190
Reprisals Against	004.180
Union Representative Advisory to (Form OI-80).....	Exhibit 4-8 , 004.110
Use of, in Field or Undercover Operations.....	007.040
SSA Main Menu (VTAM)	Exhibit 6-1
SSA Menu (Main).....	Exhibit 6-3
SSA Office of the Inspector General Fact Sheets.....	011.040
SSA OIG Fact Sheet (OI-12L).....	Exhibit 11-9
SSA OIG Fitness Evaluation Report.....	Exhibit 22-3
SSA OIG Fitness Norms	Exhibit 22-4
SSA Production.....	Exhibit 6-2
SSA Record Access & Disclosure.....	006.020
SSA Visitor Intake Process (VIP) High Risk Query System (VHRQ).....	004.190
SSI Complete Record (SSID).....	Exhibit 6-30
SSN Misuse & Identity Theft.....	005.050, 004.160
SSN Verification Policy	006.025
Standard Query (SQRY)	Exhibit 6-40A
Standard Query & Reply (SQRY).....	Exhibit 6-40B
Standards of Ethical Conduct.....	002.000
Statement Continuation (OI-16D).....	Exhibit 10-9
Statement of Consumer Rights Under Right to Financial Privacy Act of 1978 (OI-58)	Exhibit 18-2
Statement Signature Page (OI-16E)	Exhibit 10-10
Statements	010.090
Exculpatory & False Exculpatory	004.120
False Statements & Representation (Section 1129)	016.000
Full Miranda Statement (OI-16C).....	Exhibit 10-8
<i>Interviews, Investigative Notes & Statements</i>	Chapter 10
Non-Custodial Advice of Rights Statements (OI- 16B).....	Exhibit 10-7
Policy Statement	006.010, 019.010
Policy Statement of the DOJ Regarding the Use of Deadly Force.....	Exhibit 21-1
Witness (OI- 16A)	Exhibit 10-6
Written	004.130
Statutory Law Enforcement Authority, Attorney General Guidelines for OIG's.....	Exhibit 1-2
Structure, Organizational	001.010
Subpoena(s)	
IG Subpoena Transmittal Letter.....	Exhibit 12-2
Injunctions & Testimonial.....	016.040
<i>Inspector General Subpoenas</i>	Chapter 12
OIG Subpoena.....	Exhibit 12-1
Register	012.040
Request.....	012.010
Service.....	012.020
Summary Earning Query (SEQY).....	Exhibit 6-25
Summary Earning Report (SEQR)	Exhibit 6-26
Summons, Obtaining.....	015.050
Supervisory File Review Sheet (O1-20).....	Exhibit 3-3
Supplemental Agency Regulations on Conduct	002.020
Supplemental Security Income Queries (SSQM).....	Exhibit 6-29
Surrender of Equipment	002.070
Surveillance, Undercover & Arrest Tactical Plan (OI-17)	Exhibit 7-1
Sworn Statement of Movant.....	Exhibit 18-9

Systematic Alien Verification for Entitlement (SAVE) [Exhibit 6-23](#)



Tactical Plan.....	013.040
Tactical Plan for Search Warrants (OI-18).....	Exhibit 7-2, Exhibit 13-3
Tactical Plan: Surveillance, Undercover, Arrest (OI-17).....	Exhibit 7-1
Technical Investigative Equipment & Support	007.140
Text Messaging, Legal Considerations Regarding the Use of	018.130
The Arraignment	015.090
The Freedom of Information Act	019.000
The Privacy Act of 1974	019.050
The Right to Financial Privacy Act of 1978.....	018.000
Threats and Assaults, Category 1 – Threat Notification Report (Form OI-95)	Exhibit 4-21
Threats and Assaults – Interview Worksheet.....	Exhibit 4-16
Threats and Assaults, Investigation of	004.190
Title II Fraud	004.010
Title II Menu (T2SM)	Exhibit 6-5
Title XVI Fraud.....	004.010
Touhy Regulations	018.070
Tracking Work Hours.....	002.130
Trial Work Period	004.030
Training	
Basic Firearms.....	021.060
Database.....	020.030
Federal Law Enforcement Training Center (FLETC).....	001.120, 002.000
Field Division In-Service	020.060
Guide, On-the-Job.....	Exhibit 20-2
On-the-Job Training & the Mentoring Program.....	020.040
Nominations & Authorization (HHS-350).....	Exhibit 20-1
Training Policy	Chapter 20
Victim & Witness Awareness	017.060
Transmittal Letter (Account Information	
Only Under Right to Financial Privacy Act).....	Exhibit 18-12
Transmittal Letter (Right to Financial Privacy Act).....	Exhibit 18-5
Transmittal Letter to Customer.....	Exhibit 18-6
Transaction Record of Each Advance or	
Return of Confidential Funds (OI-28A)	Exhibit 9-4
Transfer from the District for Plea &	
Sentencing (Rules of Criminal Procedure - Rule 20).....	015.100
Transfer of Records	018.050
Transfer of Records to Another Agency or Department.....	Exhibit 18-10
Transportation of Personally Identifiable Information Outside of	
OIG Secure Space.....	Exhibit 6-45
Types of Employee Misconduct.....	004.070
Types of Firearms & Ammunition	021.050
Types of Investigations.....	004.000

U U U U U U U U

Updating the Status of Employee Cases in NICMS	004.150
Undercover Operations	007.000 , 007.060
Approval	007.030
Initiating.....	007.020
Monitoring	007.050
Use of SSA Employees in.....	007.040
Union Officials, Allegations of Misuse of Official Time	004.140
Union Representation, Employee.....	004.110
Union Representative Advisory to SSA Employee (Form OI-80)	Exhibit 4-8 , 004.110
U.S. Customs Service Radio Call System (10-Code)	Exhibit 7-15
<i>Use-of-Force</i>	Chapter 24
Administrative Inquiry	024.070
Basic Use-of-Force Training.....	024.020
Consideration for Use-of-Force	024.000
Emergency, Interim Legal Representation of Federal LEOs involved in Critical Incidents	024.080
Incidents Involving Less-Than-Lethal Force	024.050
Instructors	024.030
Liability.....	024.010
Post-Incident Procedures	024.060
Reporting Use-of-Force Incidents (Shooting Indicents)	024.040
Use of Official Vehicles	002.060
Use of SSA Employees in Field or Undercover Operations	007.040

V V V V V V V V

Vehicle (Government) Fleet Management	023.070
Vehicle Searches	013.100
Verification Policy for SSNs	006.020
Verification of Statistics, Monthly	003.190
<i>Victim & Witness Assistance Program</i>	Chapter 17
Victim & Witness Awareness Training.....	017.060
Victim & Witness of Crime, Information for	017.060
Video Documentation.....	013.060
Visitor Intake Process (VIP) High Risk Query System (VHRQ).....	004.190
Voucher Fraud.....	004.070

W W W W W W W W

Waiver of Disciplinary Action Against an Employee.....	004.105
Waiver of Prosecution to Obtain Cooperation of Employee.....	004.100
Warrant(s)	

Arrest.....	Exhibit 15-2
Arrest - Execution	015.040
Arrest - General.....	015.020
Arrest Without a Warrant.....	015.060
Execution of Search	013.070
Search - General.....	013.030
Search - Supplies Inventory/Raid Kit (OI-36)	Exhibit 13-2
Search - Tactical Plan (OI-18)	Exhibit 7-2, Exhibit 13-3
Warrantless Searches.....	013.080
Weapons	
Carrying & Using.....	021.020
Issuance & Security	021.090
Weingarten Rights.....	004.110
Wire or Oral Communications, Interception of.....	008.040
Witness Identification of Subjects	007.090
Witness Statement (OI-16A).....	Exhibit 10-6
Written Statements	004.130
Work Hours, tracking of.....	002.130
Worksite Enforcement Operations	005.085

LISTS OF EXHIBITS AND FORMS

The first table lists the numbers and titles of exhibits discussed in this *Handbook*. The second table is a numerical listing of all forms and the sections in which they are discussed.

List of Exhibits

Exhibit Number	Exhibit Title
1-1	Quality Standards for Investigations
1-2	Application for Special Deputation
1-3	Certification of Review of the <i>Special Agent Handbook</i>
1-4	Sample Fraud Alert
2-1	Certification for Home-to-Work Use of Official Government Vehicles (OI-46)
2-2	Availability Pay Certification (OI-49)
2-3	Biweekly Activity Report (Special Agent) (OI-33)
2-4	Annual Certification of Availability Hours (OI-50)
2-5	Special Agent Part-time Employment Program
3-1	Action Memorandum (OI-42)
3-2	NICMS Case Opening Report (OI-1)
3-3	Additional Subjects/Victims/Alias Data (OI-1A)
3-4	Supervisory File Review Sheet (OI-20)
3-5	Case File Table of Contents (OI-31)
3-6	NICMS Criminal & Administrative Disposition Form (OI-9)
3-7	Report of Court Ordered Restitution/Judgment (OI-68)
3-8	Report of Investigation (OI-4)
3-9	Personal History Information Form (OI-19)
4-1	Federal Employee Advice of Rights (OI-15)
4-2	Federal Employee Advice of Rights -- Spanish (OI-15S)
4-3	Kalkines Warning (OI-14)
4-4	Kalkines Warning -- Spanish (OI-14S)
4-5	DAIGI Memorandum to SAC
4-6	Model Referral Letter to SSA
4-7	Request for Information or Assistance (OI-56)
4-8	Union Representative Advisory to SSA Employee (Form OI-80)
4-9	Non-Criminal Background Investigation: Education
4-10	Non-Criminal Background Investigation: Employment
4-11	Non-Criminal Background Investigation: Neighborhood
4-12	Confidential Informant Data (OI-27)
4-13	Agreement to Provide Information (OI-27A)
4-14	Confidential Informant Contact Record (OI-27B)
4-15	Confidential Source Registration Card (OI-27C)
5-1	Cooperative Disability Investigative (CDI) Program MOU
5-2	Guide to Fugitive Felon Investigations

Exhibit Number	Exhibit Title
6-1	SSA Main Menu (VTAM)
6-2	SSA Production (Production)
6-3	SSA Menu (Main)
6-4	Master File Query Menu (MFQM)
6-5	Title II Menu (T2SM)
6-6	Photocopy Request (PEPH)
6-7	Detailed Office/Organization System (DOORS)
6-8	Field Office Address and Phone Numbers (FOADDRESS)
6-9	Representative Payee Main Menu (RPMM)
6-10	RP Query Response Selection List (RQSL)
6-11	CDR Selection Menu (MCDR)
6-12	CDR Query Screen (QCDR)
6-13	Prison Systems /Fugitive Felons (PFSM)
6-14	Prison Systems Menu (MFQM)
6-15	Master File Query Menu (MFQM)
6-16	Abbreviated Account Query Menu (MFQM)
6-17	SSA Claims Control System query (SSACCS)
6-18	Numident Query Sensitive Information (NUMI)
6-19	Numident (NUMI)
6-20	Alpha-Index Query (ALPH)
6-21	Data Exchange Query Menu (DXQM)
6-22	National Directory New Hire, Wage & Unemployment Menu (NDNH)
6-23	Systematic Alien Verification for Entitlement (SAVE)
6-24	Non-Immigrant Information and Alien Status Verification Display (NIIS)
6-25	Summary Earnings Query (SEQY)
6-26	Summary Earnings Report (SEQR)
6-27	Detail Earnings Query (DEQY)
6-28	Detail Earnings Report (DEQR)
6-29	Supplemental Security Income Queries (SSQM)
6-30	SSI Complete Record (SSID)
6-31	Payment History Update System Queries (PHUS)
6-32	Payment History by BIC (PHU1)
6-33	Miscellaneous Menu (MISM)
6-34	Routing Transit Number (RTND)
6-35	Final Financial Institution Listing (RTN)
6-36	EIF Access by Name (AEQY)
6-36A	EIF Access by EIN (AEQY)
6-37	EIF Response to Query (AEQY)
6-38	Consolidated Query (CNQY)
6-39	RP Query Response Selection List (RQSL)
6-40A	Standard Query (SQRY)
6-40B	Standard Query & Reply (SQRY)
6-41	Folder Query (FQY1)
6-42	Response Letter for SSN Queries
6-43	Annual Systems Security Certification
7-1	Tactical Plan: Surveillance, Undercover, Arrest (OI-17)
7-2	Tactical Plan for Search Warrants (OI-18)
7-3	Consent to Monitor Non-Telephone Conversations (OI-25AL)
7-4	Action Memorandum (OI-42)
7-5	Consent to Monitor Telephone Conversations (OI-25L)
7-6	Agreement Between SSA OIG and SSA Special Project Staff (OI-55)

Exhibit Number	Exhibit Title
7-7	Photo Lineup Guidelines
7-8	OI Standard Operating Procedures for Psychophysiological Detection of Deception
7-9	OI Polygraph Examination Request Worksheet
7-10	Request for NCIC/NLETS Records Check
7-11	FinCEN Request for Information
7-12	OI Standard Operating Procedures, Electronic Crime Team
7-13	Handwriting Sample (OI-29A)
7-14	Handwriting Specimen (OI-29B)
7-15	Radio Network User Registration Form
(b) (7)(E)	
8-1	Report of Intercept (OI-24A)
8-2	Consent to Monitor Telephone Conversations (OI-25L)
8-3	Sample Intercept Request Memorandum (OI-24)
8-4	Consent to Monitor Non-Telephone Conversations (OI-25AL)
9-1	Transaction Record of Each Advance or Return of Confidential Funds (OI-28A)
9-2	OIG Transmittal Register
9-3	Receipt for Payment to Informant (OI-28B)
9-4	Custodian's Activity Log for Confidential Funds (OI-28)
9-5	Accountability Report (OI-28C)
10-1	Personal History Information (OI-19)
10-2	Report of Investigative Activity (OI-3)
10-3	Advice of Rights (OI-13)
10-4	Advice of Rights - Non Custodial (OI-13NC)
10-5	Advice of Rights - Spanish (OI-13S)
10-6	Witness Statement (OI-16A)
10-7	Non-Custodial Advice of Rights Statement (OI-16B)
10-8	Full Miranda Statement (OI-16C)
10-9	Statement Continuation (OI-16D)
10-10	Statement Signature Page (OI-16E)
11-1	NICMS Case Opening Report (OI-1)
11-2	Investigative Plan (OI-2)
11-3	Report of Investigation (OI-4)
11-4	Specialized Report of Investigation (OI-5A)
11-5	Prosecution Report (OI-6)
11-6	Memorandum of Transmission (OI-7)
11-7	NICMS Criminal & Administrative Disposition Form (OI-9)
11-8	Investigative Checklist (OI-34)
11-9	SSA OIG Fact Sheet (OI-12L)
11-10	DAIGI Memorandum for Employee Misconduct Cases Involving OI SAs
12-1	OIG Subpoena
12-2	IG Subpoena Transmittal Letter
13-1	Preparatory Checklist for Search Warrant Affidavit (OI-35)
13-2	Search Warrant Supplies Inventory/Raid Kit (OI-36)
13-3	Tactical Plan for Search Warrants (OI-18)
13-4	Inventory Form (OI-23)

Exhibit Number	Exhibit Title
13-5	Inventory Form (Attachment) (OI-23A)
13-6	Consent to Search (OI-26)
13-7	Consent to Search (OI-26L)
14-1	Evidence/Property Report (OI-21)
14-2	Description of Property Acquired (OI-21A)
14-3	Chain of Custody (OI-21B)
14-4	Inventory Form (OI-23)
14-5	Inventory Form (Attachment) (OI-23A)
15-1	Criminal Complaint
15-2	Arrest Warrant
15-3	Declination of Prosecution (OI-77)
16-1	CMP / Administrative Sanctions Tracking Document
17-1	Information for Victims and Witnesses of Crime
18-1	Certificate of Compliance with the Right to Financial Privacy Act of 1978 (OI-57)
18-2	Statement of Customer Rights Under Right to Financial Privacy Act of 1978 (OI-58)
18-3	Customer Consent and Authorization for Access to Financial Records (OI-59)
18-4	Customer Notice (OI-60)
18-5	Transmittal Letter (Right to Financial Privacy Act)
18-6	Transmittal Letter to Customer
18-7	Instructions for Completing and Filing the Enclosed Motion and Sworn Statement (OI-61A)
18-8	Motion for Order Pursuant to Customer Challenge Provisions of the Right to Financial Privacy Act of 1978 (OI-61)
18-9	Sworn Statement of Movant
18-10	Transfer of Records to Another Agency or Department
18-11	Notice to Customer for Transfer of Records
18-12	Transmittal Letter (Account Information Only Under Right to Financial Privacy Act)
20-1	Training Nomination and Authorization (SSA 352, formerly HHS-350)
20-2	On-the-Job Training Guide
20-3	Individual Development Plan
21-1	Policy Statement of the Department of Justice Regarding the Use of Deadly Force
21-2	FLETC Use of Force Model
22-1	Physical Requirements for SSA OIG Criminal Investigators
22-2	SSA OIG Fitness Evaluation Report
22-3	SSA OIG Fitness Norms
23-1	Personal Custody Property Record/Hand Receipt (OI-52)

List of Forms

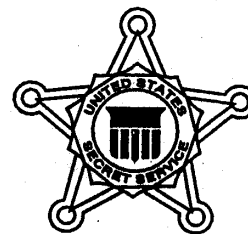
Number	Title	Chapter
SSA-352	Training Nomination and Authorization (formerly HHS-350)	20
OI-1	NICMS Case Opening Report	3, 11
OI-1A	Additional Subjects/Victims/Alias Data	3
OI-2	Investigative Plan	11
OI-3	Report of Investigative Activity	11
OI-4	Report of Investigation	10,11
OI-5A	Specialized Report of Investigation	11
OI-6	Prosecution Report	11
OI-7	Memorandum of Transmission	11
OI-9	NICMS Criminal & Administrative Disposition Form	11
OI-12L	SSA OIG Fact Sheet	11
OI-13	OI Advice of Rights/Waiver Form	4
OI-14	Kalkines Warning	4
OI-15	Federal Employee Advice of Rights	4
OI-16	Subject's Statement Form	10
OI-16A	Witness's Statement Form	10
OI-16B	Statement Form	10
OI-16C	Statement Continuation Form	10
OI-17	Tactical Plan: Surveillance, Undercover, Arrest	7
OI-18	Tactical Plan for Search Warrants	6, 13
OI-19	Personal History Information	3, 10
OI-20	Supervisory File Review Sheet	3
OI-21	Evidence/Property Report	14
OI-21A	Description of Property Acquired	14
OI-21B	Chain of Custody	14
OI-23	Inventory Form	13
OI-23A	Inventory Form (Attachment)	8
OI-24	Intercept Request	8
OI-24A	Report of Intercept	8
OI-25AL	Consent to Monitor Non-Telephone Conversations	8
OI-25L	Consent to Monitor Telephone Conversations	13
OI-26	Consent to Search	13
OI-26L	Consent to Search	13
OI-27	Confidential Informant Data	4
OI-27A	Agreement to Provide Information	4
OI-28	Custodian's Activity Log for Confidential Funds	9
OI-28A	Transaction Record of Each Advance or Return of Confidential Funds	9
OI-28B	Receipt for Payment to Informant	9
OI-28C	Accountability Report	9
OI-29A	Handwriting Sample	7
OI-29B	Handwriting Specimen	7
OI-31	Case File Table of Contents	3
OI-33	Biweekly Activity Report (Special Agent)	2
OI-34	Investigative Checklist	11
OI-35	Preparatory Checklist for Search Warrant Affidavit	13
OI-36	Search Warrant Supplies Inventory/Raid Kit	13
OI-42	Action Memorandum	3, 7
OI-46	Certification for Home-to-Work Use of Official Government Vehicles	2

Number	Title	Chapter
OI-49	Availability Pay Certification	2
OI-50	Annual Certification of Availability Hours	2
OI-52	Personal Custody Property Record/Hand Receipt	23
OI-54	Release Authority for Consumer Report Agency	5
OI-55	Agreement Between SSA OIG and SSA Special Project Staff	7
OI-56	Request for Information or Assistance	4
OI-57	Certificate of Compliance with the Right to Financial Privacy Act of 1978	18
OI-58	Statement of Customer Rights Under Right to Financial Privacy Act of 1978	18
OI-59	Customer Consent and Authorization for Access to Financial Records	18
OI-60	Customer Notice	18
OI-61	Motion for Order Pursuant to Customer Challenge Provisions of the Right to Financial Privacy Act of 1978	18
OI-61A	Instructions for Completing and Filing the Enclosed Motion and Sworn Statement	18
OI-68	Report of Court Ordered Restitution/Judgment	3
OI-77	Declination of Prosecution	15
OI-80	Office of the Inspector General, Social Security Administration Advisory to Employee	10
SF 1164	Claim for Reimbursement for Expenditures on Official Business	9
SSA-8551	Referral of Potential Violation	3

**Memorandum of Understanding Between the Social Security
Administration Office of the Inspector General and
the United States Secret Service**



Memorandum of Understanding
between
U. S. Secret Service Forensic Services Division
and the Social Security Administration
Office of the Inspector General
for Forensic Assistance



I. Introduction

A) The U.S. Secret Service (USSS) is offering the services of the Forensic Services Division (FSD) to the Social Security Administration, Office of the Inspector General (SSA, OIG), in areas of forensic support and expert testimony. The SSA, OIG is herein defined as the Office of Investigations (OI). This Memorandum of Understanding is in keeping with the philosophy of the work completed by Vice President Gore and the "National Performance Review".

II. Mission Statement

A) The FSD mission is to provide forensic/technical support services to USSS elements and other federal, state, county and local law enforcement agencies when requested and available.

III. Areas of Cooperation

A) Assistance is offered to the SSA, OIG, OI when requested, in the examination of handwriting/handprinting, threat letter searches through the Forensic Information System for Handwriting (FISH), document examination, ink comparisons and age determination, audio/video enhancement, fingerprint development and comparisons, Automated Fingerprint Identification Systems (AFIS) searches, forensic photography, and polygraph examinations.

B) Seminars will be offered to SSA, OIG, OI officials, when requested, to familiarize OIG personnel with the capabilities and potential costs of FSD support. Laboratory tours and crime scene search operations also are offered.

C) Representatives of FSD will provide instruction, when requested, at the Federal Law Enforcement Training Center (FLETC) for students involved in SSA, OIG, OI classes.

D) SSA, OIG, OI will pay all mission specific travel costs (per diem and transportation) incurred by FSD representatives. All requests for services will be made and provided consistent with the provisions of the Economy Act, 31 USC 1535.

IV. Implementation

A) USSS cases have priority in forensic examinations. The USSS, FSD currently prioritizes cases submitted for examination based upon the importance placed on the investigation by the USSS or upon the satisfaction of the judicial system and its requirements. The SSA, OIG, OI will establish a similar procedure for case submission to ensure that those cases deemed most important will be given the necessary attention by FSD.


B) Other operational procedures are to be established by representatives of USSS, FSD and SSA, OIG, OI to ensure a workable implementation of a final Memorandum of Understanding.

C) At its discretion, SSA, OIG, OI will continue to use various other forensic laboratories.

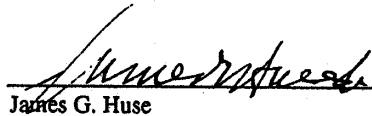
V. Administration

A) A completed Memorandum of Understanding between the USSS, FSD and SSA, OIG, OI will be renewable, annually, upon agreement of both parties.

Approved by:


Paul A. Hackenberry
Assistant Director
Office of Investigations
U. S. Secret Service

2/14/97
date


James G. Huse
Assistant Inspector General for Investigations
U. S. Social Security Administration

1/29/97
date

**Policy Statement of the United States Department of Justice
Regarding the Use of Force and Deadly Force**

POLICY STATEMENT USE OF DEADLY FORCE

GENERAL PRINCIPLES

- I. Law enforcement officers and correctional officers of the Department of Justice may use deadly force only when necessary, that is, when the officer has a reasonable belief that the subject of such force poses an imminent danger of death or serious physical injury to the officer or to another person.
 - A. Deadly force may not be used solely to prevent the escape of a fleeing suspect.
 - B. Firearms may not be fired solely to disable moving vehicles.
 - C. If feasible and if to do so would not increase the danger to the officer or others, a verbal warning to submit to the authority of the officer shall be given prior to the use of deadly force.
 - D. Warning shots are not permitted outside of the prison context.
 - E. Officers will be trained in alternative methods and tactics for handling resisting subjects which must be used when the use of deadly force is not authorized by this policy.

CUSTODIAL SITUATIONS

- II. Unless force other than deadly force appears to be sufficient, deadly force may be used to prevent the escape of a prisoner committed to the custody of the Attorney General or the Bureau of Prisons
 - A. if the prisoner is effecting his or her escape in a manner that poses an imminent danger to the safety of the officer or another person; or
 - B. if the prisoner is escaping from a secure facility or is escaping while in transit to or from a secure facility.
- III. If the subject is in a non-secure facility, deadly force may be used only when the subject poses an imminent danger of

- death or serious physical injury to the officer or another person.
- IV. If the subject is in transit to or from a non-secure facility and is not accompanied by a person who is in transit to or from a secure facility, deadly force may be used only when the subject poses an imminent danger of death or serious physical injury to the officer or to another person.
- V. After an escape from a facility or vehicle and its immediate environs has been effected, officers attempting to apprehend the escaped prisoner may use deadly force only when the escaped prisoner poses an imminent danger of death or serious physical injury to the officer or another person.
- VI. Deadly force may be used to maintain or restore control of a prison or correctional facility when the officer reasonably believes that the intended subject of the deadly force is participating in a disturbance in a manner that threatens the safety of the officer or another person.
- VII. In the prison context, warning shots may be fired within or in the immediate environs of a secure facility if there is no apparent danger to innocent persons: (A) If reasonably necessary to deter or prevent the subject from escaping from a secure facility; or (B) if reasonably necessary to deter or prevent the subject's use of deadly force or force likely to cause serious physical injury.

APPLICATION OF THE POLICY

VIII. This Policy is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, against the United States, its departments, agencies, or other entities, its officers or employees, or any other person.