

**COMPUTER MATCHING AGREEMENT
BETWEEN
THE CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
AND
THE SOCIAL SECURITY ADMINISTRATION**

Match # 1012

I. Purpose

This computer matching agreement (agreement) establishes the terms, conditions, and safeguards under which the Social Security Administration (SSA) will conduct a computer match with the Corporation for National and Community Service (CNCS). SSA will verify Social Security numbers (SSN) and provide to CNCS the citizenship status (as recorded in SSA records) of individuals applying to serve in approved national service positions, and those designated to receive national service education awards, under the National and Community Service Act of 1990 (NCSA) 42 U.S.C. § 12501, *et seq.*

CNCS is a Federal agency (42 U.S.C. § 12651, *et seq.*) that administers programs that engage individual participants in community and national service positions. On September 29, 2020 CNCS adopted the operating name of AmeriCorps. The adoption of this operating name did not alter the formal legal name of CNCS. For purposes of this agreement, we refer to the agency party with whom SSA conducts a computer match as CNCS.

A participant in a CNCS national service program must be a citizen or national of the United States, or a lawful permanent resident alien of the United States (42 U.S.C. §§ 12591(a)(5) and 12602(a)(3); Section 146(a) of the NCSA). Individuals who successfully complete their terms of service are eligible to receive Education Awards, and, under certain circumstances, members can transfer their earned education awards to family members, as long as the transferees meet eligibility requirements, including being citizens, nationals, or lawful permanent resident aliens of the United States (Section 146(a)(3) and 148(f)(8)(B) of the NCSA, 42 U.S.C. §§ 12602(a)(3) and 12604(f)(8)(B)).

Some of the programs CNCS administers are grant programs and CNCS relies on the grantee to obtain and provide the individual participants' SSN and citizenship documentation when requested. "Grant" is used in this document as defined in 31 U.S.C. § 6304. The recipient of a grant is a "grantee."

II. Legal Authority

This agreement is executed in compliance with the Privacy Act of 1974, 5 U.S.C. § 552a, as amended by the Computer Matching and Privacy Protection Act (CMPPA) of 1988, as amended, and the regulations and guidance promulgated thereunder.

SSA's legal authority to disclose information under this agreement is pursuant to section 1106 of the Social Security Act (Act) (42 U.S.C. § 1306); the Privacy Act of 1974, (5 U.S.C.

§ 552a), as amended, including by the CMPPA and the regulations and guidance promulgated thereunder; the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) (Public Law 108-458 § 7213); and SSA's disclosure regulations at 20 C.F.R. Part 401.

Section 146(a)(3) of the NCSA (42 U.S.C. § 12602(a)) sets forth the eligibility requirements for an individual to receive an Education Award from the National Service Trust upon successful completion of a term of service in an approved national service position. Section 1711 of the Serve America Act (Pub. L. No. 111-13) directs CNCS to enter into an agreement to verify statements made by an individual declaring that such individual is in compliance with section 146(a)(3) of the NCSA by comparing information provided by the individual with relevant information that is in the possession of another Federal agency.

In accordance with the study CNCS completed pursuant to section 1711 of the Serve America Act, CNCS determined that a computer matching program with SSA is the most effective means to verify an individual's statement that he or she is in compliance with section 146(a)(3) of the NCSA.

III. Responsibilities of the Parties

A. CNCS's Responsibilities

1. CNCS will transmit verification requests to SSA. Each verification request will contain all of the mandatory data elements identified in section V for each individual for whom CNCS is requesting verification.
2. CNCS acknowledges that SSA's verification (CNCS input data matches SSA records) of the name, date of birth (DOB), indication of death (if applicable), SSN, and citizenship status CNCS transmits to SSA only establishes that the submitted information matches information in SSA's master files. The verification does not authenticate the identity of the individual or conclusively prove that the individual submitting the information is who he or she claims to be.
3. CNCS will not reject an individual for placement in an approved national service position, or deny an individual a national service educational award from the National Service Trust, relying solely on the results of this data exchange, if additional information refuting the SSA response is provided to CNCS, as specified in Section VIII below.
4. CNCS will provide Congress and the Office of Management and Budget (OMB) with notice of this program in accordance with the Computer Matching and Privacy Protection Act of 1988, and will publish the required matching notice in the Federal Register (Fed. Reg.).
5. CNCS will not provide the SSA verification results to grantees or any other third parties.

B. SSA's Responsibilities

1. SSA will compare the data CNCS transmits in its verification requests with SSA data in SSA's Numident database, as authorized by the systems of records (SOR) 60-0058, Master Files of Social Security Number (SSN) Holders and SSN Applications (Enumeration System).
2. SSA will verify SSNs and provide an indicator of citizenship status, as recorded in SSA records, in accordance with article V below.

IV. Justification and Anticipated Results

A. Justification

Data exchange under this matching program is necessary for CNCS to compare CNCS data from that found in SSA data for individuals for the national service program and those designated to receive national service education awards. CNCS' use of SSA data does not prove that the identity verified is accurate, only whether the citizenship data obtained from SSA matches the information from CNCS. SSA and CNCS determined that computer matching is the most efficient, economical, and comprehensive method of exchanging and processing this information. The principal alternative to a matching program is a manual comparison. Such an activity would impose a considerable administrative burden and create significant delays. Accordingly, no other administrative activity can efficiently accomplish the purpose of the computer matching program.

By enhancing CNCS's ability to verify the identity of individuals for approved national service positions, CNCS anticipates that the matching program under this agreement will assist in preventing persons from fraudulently enrolling as members in its programs or fraudulently receiving Segal Education Awards.

B. Anticipated Results

This matching agreement saved CNCS administrative costs of approximately \$216,660 in fiscal year (FY) 2020. It costs \$6.25 per record for a full time CNCS employee to complete a manual verification. CNCS expects to save approximately \$340,000 by performing this match during the term of this agreement. SSA does not expect any savings for any SSA programs to result from this matching program. See Attachment A for the Cost-Benefit Analysis.

V. Description of Records Matched

A. Systems of Records

SSA will disclose to CNCS information from the Enumeration System, published in full on December 29, 2010 (75 Fed. Reg. 82121), as amended on July 5, 2013 (78 Fed. Reg. 40542), February 13, 2014 (79 Fed. Reg. 8780), July 3, 2018 (83 Fed. Reg. 31250-31251),

and November 1, 2018 (83 Fed. Reg. 54969). The Enumeration System database maintains records about each individual who has applied for and obtained an SSN. The information in this system of records may be updated during the effective period of this agreement as required by the Privacy Act.

CNCS will provide SSA with data from its SOR, as authorized by the CNCS-04-CPO-MMF-Member Management Files, MMF SOR, published in full on January 23, 2020 (85 Fed. Reg. 3896).

B. Specified Data Elements

CNCS will provide SSA with the following mandatory identifying information for each individual for whom CNCS requests information: SSN, First Name, and Last Name. CNCS may also provide optional information: DOB.

The SORs involved in this computer matching program have routine uses permitting the disclosures needed to conduct this match from SSA. CNCS relies on the SSA data to help verify the information applicants provide.

SSA will match the SSN and name (and DOB if provided) from the CNCS request file. For verified records, SSA will provide an indication of citizenship status and an indication of death (if present), as recorded in SSA records.

C. Number of Records

CNCS estimates requesting approximately 100,000 verifications per year.

D. Frequency of Matching

CNCS will transmit data daily to SSA via a batch process. SSA will send a response file the next business day.

VI. Accuracy Assessments

The SSA Enumeration System used for SSN matching is 100 percent accurate based on SSA's Office of Analytics, Review, and Oversight ("FY 2018 Enumeration Accuracy Review Report, April 2019").

SSA is not the agency responsible for conferring citizenship. While SSA records may provide an indication of citizenship, they provide neither definitive, nor current, information on citizenship status.

An applicant for an original SSN provides identifying information upon application for that number. However, there is no obligation for the SSN holder to report a subsequent change in immigration status to SSA unless that SSN holder files a claim for benefits. Thus, some previously established citizenship information in SSA's records might not be current.

VII. Procedures for Individualized Notice

A. Applicants/Grantees

CNCS will provide each individual or grantee, at the time of application, notice that the information provided on the application is subject to verification through a computer matching program. The CNCS enrollment application package contains a privacy certification notice that the applicant must sign authorizing CNCS to verify the information provided.

For transferees, at the time an award is transferred, CNCS will provide an individual notice to transferees that the SSN is subject to verification through a computer matching program. CNCS will send a privacy notice to the transferee, and in the case of a minor, to the parent or legal guardian. The transferee, parent, or legal guardian must sign the privacy certification authorizing CNCS to verify the information provided.

SSA notifies all individuals who apply for benefits for its respective programs that it will conduct matching programs. SSA includes notice of computer matching on all applications for Social Security benefits and Supplemental Security Income payments.

B. Beneficiaries/Annuitants

SSA will provide subsequent notices of computer matching to its respective retirees, annuitants, beneficiaries, and recipients as required. For Federal retirement annuitants subject to civil service annuity offsets, SSA provides direct notice of computer matching via annual cost of living adjustment notices.

CNCS will also publish specific notices of this matching program in the Federal Register, in accordance with the requirements of the Privacy Act and applicable OMB guidelines.

VIII. Verification Procedures and Opportunity to Contest

A. Verification Procedures

Through the SSA computer matching process, CNCS receives information as to whether there is an affirmative match for each individual. CNCS will take no adverse action regarding any individual identified through the matching process based solely on information that CNCS obtains from the match. When SSA identifies an individual for whom there is no affirmative match, CNCS or its grantee will contact the affected individual to give him/her an opportunity to verify the matching results in accordance with the requirements of the Privacy Act and applicable OMB guidelines. CNCS will not tell grantees that SSA data is the basis for the lack of verification.

The affected individual will have an opportunity to contest the accuracy of the information provided to CNCS by SSA. CNCS will independently review the

individual's information and make an assessment based on all supplemental information provided.

B. Notice and Opportunity to Contest

When SSA identifies an individual for whom there is no affirmative match, CNCS or its grantee will manually verify the individual's information. This manual verification process will include providing the individual 30 days to provide independent documentation of his or her SSN and/or citizenship status. If the manual verification is not completed, the individual cannot become an AmeriCorps member. CNCS will not refer individuals to SSA to resolve citizenship non-confirmation responses. CNCS understands that SSA is not the custodian of U.S. citizenship records.

IX. Procedures for Retention and Timely Destruction of Identifiable Records

CNCS will retain the electronic files received from SSA only for the period of time required for any processing related to the matching program and will then destroy all such data by electronic purging unless CNCS is required to retain the information in order to meet evidentiary standards. CNCS may use the SSA data governed by this agreement to update its master files of new national service participants and those designated to receive National Service educational awards. In case of such retention for evidentiary purposes, CNCS will retire the retained data in accordance with applicable Federal Records Retention Schedules (44 U.S.C. § 3303a). CNCS may not create permanent files or separate systems comprised solely of the data provided by SSA.

SSA will delete electronic data input files received from CNCS after it processes the applicable match(es). SSA will retire its data in accordance with the Federal Records Retention Schedule.

X. Records Usage, Duplication, and Rediscovery Restrictions

SSA and CNCS will adhere to the following limitations on the use, duplication, and redisclosure of the electronic files and data provided by the other agency under this matching program:

- A. SSA and CNCS will use and access the data, and any data that the match creates, only for the purposes described in this agreement.
- B. SSA and CNCS will not use the data to extract information concerning individuals therein for any purpose not specified in this agreement. Other than for purposes of this agreement, SSA and CNCS will not create a file that consists solely of information concerning the individuals involved in the specific matching program.
- C. SSA and CNCS will not duplicate or disseminate the data, within or outside their respective agencies, without the written permission of SSA or CNCS, except as required by Federal law. SSA and CNCS will not give such permission unless the law requires

disclosure or the disclosure is essential to the agreement. For such permission, the agency requesting permission must specify in writing what data it is requesting be duplicated or disseminated, to whom the data will be disseminated, and the reasons that justify such duplication or dissemination.

- D. The data that CNCS and SSA each provide as part of the agreement will remain the property of the providing agency. SSA and CNCS will return or destroy the data as soon as the matching process is complete, except as provided in section IX.

XI. Security Procedures

SSA and CNCS will comply with the requirements of the Federal Information Security Management Act (FISMA) (44 U.S.C. Chapter 35, Subchapter II), as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283); related OMB circulars and memoranda, such as Circular A-130, *Managing Information as a Strategic Resource* (July 28, 2016) and Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information* (January 3, 2017); National Institute of Standards and Technology (NIST) directives; and the Federal Acquisition Regulations, including any applicable amendments published after the effective date of this agreement. These laws, directives, and regulations include requirements for safeguarding Federal information systems and personally identifiable information (PII) used in Federal agency business processes, as well as related reporting requirements. Both agencies recognize, and will implement, the laws, regulations, NIST standards, and OMB directives, including those published subsequent to the effective date of this agreement.

FISMA requirements apply to all Federal contractors, organizations, or entities that possess or use Federal information, or that operate, use, or have access to Federal information systems on behalf of an agency. Both agencies are responsible for oversight and compliance of their contractors and agents.

A. Incident Reporting

If either SSA or CNCS experiences an incident involving the loss or breach of PII provided by SSA or CNCS under the terms of this agreement, the agency experiencing the incident will follow the incident reporting guidelines issued by OMB. In the event of a reportable incident under OMB guidance involving PII, the agency experiencing the incident is responsible for following its established procedures, including notification to the proper organizations (e.g., United States Computer Emergency Readiness Team, the agency's privacy office). In addition, the agency experiencing the incident (e.g., electronic or paper) will notify the other agency's Systems Security Contact named in this agreement. If CNCS is unable to speak with the SSA Systems Security Contact within one hour or if for some other reason notifying the SSA Systems Security Contact is not practicable (e.g., it is outside of the normal business hours), CNCS will call SSA's National Network Service Center toll free at 1-877-697-4889. If SSA is unable to speak with CNCS's Systems Security Contact within one hour, SSA will contact CNCS's

security contact information at CNCS's Office of Information Technology Help Desk at (202) 606-6600.

B. Breach Notification

SSA and CNCS will follow PII breach notification policies and related procedures issued by OMB. If the agency that experienced the breach determines that the risk of harm requires notification to affected individuals or other remedies, that agency will carry out these remedies without cost to the other agency.

C. Administrative Safeguards

SSA and CNCS will restrict access to the data matched, and to any data created by the match, to only those users (e.g. employees, contractors, etc.) who need it to perform their official duties in connection with the uses of the data authorized in this agreement. Further, SSA and CNCS will advise all personnel who have access to the data matched and to any data created by the match of the confidential nature of the data, the safeguards required to protect the data, and the civil and criminal sanctions for noncompliance contained in the applicable Federal laws.

D. Physical Safeguards

SSA and CNCS will store the data matched and any data created by the match in an area that is physically and technologically secure from access by unauthorized persons at all times (e.g., door locks, card keys, biometric identifiers, etc.). Only authorized personnel will transport the data matched and any data created by the match. SSA and CNCS will establish appropriate safeguards for such data, as determined by a risk-based assessment of the circumstances involved.

E. Technical Safeguards

SSA and CNCS will process the data matched and any data created by the match under the immediate supervision and control of authorized personnel in a manner that will protect the confidentiality of the data, so that unauthorized persons cannot retrieve any data by computer, remote terminal, or other means. Only authorized personnel can access agency data on the agencies' systems using appropriate credentials. SSA and CNCS will strictly limit authorization to those electronic data areas necessary for the authorized analyst to perform his or her official duties.

F. Application of Policy and Procedures

SSA and CNCS will adopt policies and procedures to ensure that each agency uses the information contained in their respective records or obtained from each other solely as provided in this agreement. SSA and CNCS will comply with these guidelines and any subsequent revisions.

G. Security Assessments

NIST Special Publication 800-37, as revised, encourages agencies to accept each other's security assessments in order to reuse information system resources and/or to accept each other's assessed security posture in order to share information. NIST 800-37 further encourages that this type of reciprocity is best achieved when agencies are transparent and make available sufficient evidence regarding the security state of an information system so that an authorizing official from another organization can use that evidence to make credible, risk-based decisions regarding the operation and use of that system or the information it processes, stores, or transmits. Consistent with that guidance, the parties agree to make available to each other upon request system security evidence for the purpose of making risk-based decisions. Requests for this information may be made by either party at any time throughout the duration or any extension of this agreement.

XII. Comptroller General Access

The Government Accountability Office (Comptroller General) may have access to all CNCS and SSA data it deems necessary, in order to monitor or verify compliance with this agreement.

XIII. Reimbursement

SSA will collect funds from CNCS during FY 2021 through the Intra-Governmental Payment and Collection (IPAC) system on a quarterly basis, sufficient to reimburse SSA for the costs it has incurred for performing services through the date of billing. SSA will mail a copy of the IPAC billing, and all original supporting documentation, to CNCS at 250 E Street SW, Suite 300, Washington, DC 20525, no later than five (5) calendar days following the processing of the IPAC transaction. At least quarterly, but no later than 30 days after an accountable event, SSA will provide CNCS with a performance report (e.g., a billing statement) that details all work performed to date. Additionally, at least quarterly, SSA and CNCS will reconcile balances related to revenue and expenses for work performed under this agreement.

This agreement does not authorize SSA to incur obligations for payment of funds through the performance of the services described herein. Only the execution of Fiscal Forms (e.g., Form SSA-1235, Agreement Covering Reimbursable Services and Forms FS-7600A and FS-7600B), authorizes the performance of such services. SSA may incur obligations by performing services under a reimbursable agreement only on a FY basis. Accordingly, attached to and made a part of this agreement, is executed Fiscal Forms that provides authorization for SSA to perform services under this agreement in FY 2021. Prior to any performance of activities under this agreement, both parties will execute a new Fiscal Forms for each fiscal year that SSA will perform services under this agreement. The Fiscal Forms for each FY will identify reimbursable cost estimates for that FY. SSA's ability to perform work beyond FY 2021 is subject to the availability of funds.

XIV. Duration, Modification, and Termination

A. Effective Date

The effective date of this agreement is April 1, 2021, provided that CNCS reports the proposal to re-establish this matching program to the Congressional committees of jurisdiction and OMB in accordance with 5 U.S.C. § 552a(o)(2)(A) and OMB Circular A-108 (December 23, 2016), and CNCS publishes the notice of the matching program in the Federal Register in accordance with 5 U.S.C. § 552a(e)(12).

B. Duration

This agreement will be in effect for a period of 18 months.

C. Renewal

The Data Integrity Boards (DIB) of CNCS and SSA may, within 3 months prior to the expiration of this agreement, renew this agreement for a period not to exceed 12 months, if CNCS and SSA can certify to their DIBs that:

1. The matching program will be conducted without change; and
2. CNCS and SSA have conducted the matching program in compliance with the original agreement.

If either agency does not want to continue this program, it must notify the other agency of its intention not to continue at least 90 days before the end of the period of the agreement.

D. Revision

The agencies may modify this agreement at any time by a written revision, mutually agreed to by both agencies, approved by the DIBs of each agency, and signed by the DIB signatories or their designees of each agency.

E. Termination

CNCS and SSA may terminate this agreement at any time with the consent of both agencies. Either agency may unilaterally terminate this agreement upon written notice to the other agency, in which case the termination will be effective 90 days after the receipt date of such written notice or at a later date if such later date is specified in the notice.

SSA may immediately and unilaterally suspend the data flow under this agreement if SSA:

1. Determines that CNCS has used or disclosed the information in an unauthorized manner;

2. Determines that CNCS has violated or failed to follow the terms of this agreement; or
3. Has reason to believe that CNCS breached the terms for security of data. If SSA suspends the data flow in accordance with this subsection, SSA will suspend the data until SSA makes a final determination of a breach.

If CNCS terminates this agreement, SSA is authorized to collect costs incurred prior to the termination plus any termination costs.

XV. Disclaimer

SSA is not liable for any damages or loss resulting from errors in information provided to CNCS under this agreement. SSA is not liable for damages or loss resulting from the destruction of any materials or data provided by CNCS. All information furnished to CNCS is subject to the limitations and qualifications, if any, transmitted with such information. If, because of any such error, loss, or destruction, SSA must re-perform the services, CNCS will treat the additional cost as a part of the full costs incurred in compiling and furnishing such information and will pay for such additional costs.

The performance or delivery by SSA of the goods and/or services described herein, and the timeliness of said delivery, are authorized only to the extent that they are consistent with proper performance of the official duties and obligations of SSA and the relative importance of this request to others. If, for any reason, SSA delays or fails to provide services, or discontinues the services, or any part thereof, SSA is not liable for any damage or loss resulting from such delay, or for any such failure or discontinuance.

XVI. Dispute Resolution

Disputes related to this agreement will be resolved in accordance with instructions provided in the Treasury Financial Manual Volume 1, Part 2, Chapter 4700, Appendix 6, *Intragovernmental Transaction Guide*.

XVII. Persons to Contact

A. The SSA contacts are:

Computer Systems Issues

Angil Escobar, Branch Chief
OEIS/DECIDE/Data Exchange and Verification Branch
Office Enterprise Information Systems
Office of Systems
Social Security Administration
6401 Security Boulevard, 3-F-3 Robert M. Ball Building
Baltimore, MD 21235
Telephone: (410) 965-7213
Email: Angil.Escobar@ssa.gov

Matching Agreement Issues

Donald Scott, Government Information Specialist
Office of Privacy and Disclosure
Office of the General Counsel
6401 Security Boulevard, G-401 West High Rise
Baltimore, MD 21235-6401
Telephone: (410) 965-8850
Email: Donald.Scott@ssa.gov

Information Security Issues/Systems Security Contact

Jennifer Rutz, Division Director
Office of Information Security
Division of Compliance and Assessments
Suite 3883 Perimeter East Building
6201 Security Boulevard
Baltimore, MD 21235
Telephone: (410) 966-8253
Email: Jennifer.Rutz@ssa.gov

Finance Issues

Lynn Spruill
Office of Finance
Office of Financial Policy and Operations
6401 Security Boulevard, 2-K-5 ELR
Baltimore, MD 21235
Telephone: (410) 597-1673
Fax: (410) 597-0810
Email: Lynn.Spruill@ssa.gov

Project Coordinator

Stephanie Meilinger
Office of Data Exchange and International Agreements
Office of Data Exchange, Policy Publications, and International Negotiations
6401 Security Boulevard
4-C-8-D Annex
Baltimore, MD 21235
Telephone: (410) 966-0476
Email: Stephanie.Meilinger@ssa.gov

B. The CNCS contacts are:

Information Security Issues/Systems Security Contact

Terrence King, Acting Chief Information Security Officer (CISO)
Office of Information Technology
Corporation for National and Community Service
250 E Street, SW, Suite 300
Washington, DC 20525
Telephone: (202) 606-6701/(202) 815-4246
Email: tking@cns.gov

Finance Issues

Malena Brookshire, Chief Financial Officer (CFO)
Office of the Chief Financial Officer
Corporations for National and Community Service
250 E Street, SW, Suite 300
Washington, DC 20525
Telephone: (202) 937-7411
Email: MBrookshire@cns.gov

Systems Operations

Jerry Prentice Jr., MBA
Director, National Service Trust
Corporation for National and Community Service
250 E Street, SW, Suite 300
Washington, DC 20525
Telephone: (202) 606-6883
Email: JXPrentice@cns.gov

Matching Agreement Issues

Hayley Hoffman, Associate General Counsel
Office of the General Counsel
Corporation for National and Community Service
250 E Street, SW, Suite 300
Washington, DC 20525
Telephone: (202) 937-6618
Email: HHoffman@cns.gov

XVIII. Integration Clause

This agreement, Attachment A, and the accompanying Fiscal Forms as referenced in article XIII, constitute the entire agreement of the parties with respect to this subject matter and supersedes all other data exchange agreements between CNCS and SSA that pertain to the disclosure of identity and citizenship information made between SSA and CNCS for the purposes described herein. SSA and CNCS have made no representations, warranties, or promises outside of this agreement. This agreement takes precedence over any other documents that may be in conflict with it.

XIX. Authorized Signatures

The signatories below warrant and represent that they have the competent authority on behalf of their respective agencies to enter into the obligations set forth in this agreement.

Electronic Signature Acknowledgement: The signatories may sign this document electronically by using an approved electronic signature process. Each signatory electronically signing this document agrees that his/her electronic signature has the same legal validity and effect as his/her handwritten signature on the document, and that it has the same meaning as his/her handwritten signature.

SOCIAL SECURITY ADMINISTRATION**MARY**Digitally signed by MARY
ZIMMERMAN**ZIMMERMAN**Date: 2020.12.04 13:21:56
-05'00'

Date _____

Mary Ann Zimmerman
Deputy Executive Director
Office of Privacy and Disclosure
Office of the General Counsel

Matthew RamseyDigitally signed by Matthew Ramsey
Date: 2020.12.21 10:45:07 -05'00'

Date _____

Matthew D. Ramsey
Chair
Data Integrity Board

CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

JEFFREY HEFTER Digitally signed by JEFFREY HEFTER
Date: 2020.12.08 08:14:13 -05'00'

Date _____

Scott Hefter
Chief Operation Officer (COO)

Pape Cisse

Digitally signed by NDIOGOU CISSE
DN: c=US, o=U.S. Government, ou=Corporation for
National and Community Service, cn=NDIOGOU
CISSE, 0.9.2342.19200300.100.1.1=95771001864512
Date: 2020.12.16 16:05:50 -05'00'

Date _____

Pape Cissé
Chief Information Officer (CIO) &
Senior Agency Official for Privacy (SAOP),
Chair of the Data Integrity Board (DIB)