V. Technical Specifications and Systems Security and Related Business Process Requirements

A. Technical Specifications and Systems Security

1. The Permitted Entity may use a real-time service or batch functionality, when available. All fees charged by SSA to the Permitted Entity will be applied regardless of the methods of service it uses.

2. Detailed technical requirements and procedures for using the eCBSV system are set forth on SSA's internet website at: https://www.ssa.gov/dataexchange/eCBSV/, which SSA may amend at its discretion.

3. If the Permitted Entity accesses the eCBSV system through the real-time platform client application, the Permitted Entity must maintain an automated audit trail record for five (5) years identifying either the Authorized User or the system process that initiated a request for information from SSA. Every SSN Verification request must be traceable to the Authorized User or the system process that initiated the transaction. The Permitted Entity shall process all SSN Verifications and Written Consents in a manner that will protect the confidentiality of the records and prevent the unauthorized use of the SSN Verifications and Consent Forms.

4. The Permitted Entity should integrate with SSA's entity services using identity federation. Identity federation requires the Permitted Entity to:

    a. Identity proof Authorized Users in a manner that meets National Institute of Standards and Technology (NIST) Special Publications (SP) 800-63-3 Identity Assurance Level (IAL) 2, require that authentication meets NIST SP 800-63-3 Authenticator Assurance Level (AAL) 2, and enable single sign-on for individuals that will use federation to access SSA web applications.

    b. Follow the session management guidelines for AAL2, found in NIST SP 800-63-3 B, Chapter 7 - https://pages.nist.gov/800-63-3/sp800-63b.html#sec7.

    c. Ensure controls are in place to properly set attributes that allow Authorized Users access to the eCBSV service.

    d. Recertify attributes that allow Authorized Users access to SSA web sites every 90 days.

    e. Ensure private keys are protected to prevent unauthorized access as outlined in NIST SP 800-57, "Recommendation for Key Management."

5. Consistent with its Permitted Entity Certification and existing obligations under the GLBA, the Permitted Entity shall maintain policies and procedures to ensure that SSN Verifications are encrypted at rest and in transit. e. The Permitted Entity shall

also ensure that SSN Verifications are stored within the jurisdiction of the United States (i.e., within the continental United States, Hawaii, Alaska, Puerto Rico, Guam, and the U.S. Virgin Islands). The Permitted Entity shall ensure that any entity involved with storing the SSN Verifications are United States based entities bound by the laws within the United States (notwithstanding the physical location of the business). .