ELECTRONIC INFORMATION EXCHANGE SECURITY REQUIREMENTS AND PROCEDURES FOR STATE AND LOCAL AGENCIES EXCHANGING ELECTRONIC INFORMATION WITH THE SOCIAL SECURITY ADMINISTRATION

Version 8.50

October 10, 2019

Note: All previous versions of the Technical Systems Security Requirements (TSSR) are superseded and thus obsolete.

Revision History

Version	Revision Date	Description	Author
8.0	6/21/2018	Draft completed by Guy Fortson. Parallel changes in TSSRv8 updated by William Kraemer	GGF/WJK
8.01		Spelling & Grammar Check of 8.0 lead to a few spelling errors fixed and subject-verb agreement issues	WJK
8.02		Update 8.1.7 "Responsibilities on Monetary Damages" to reflect TSSR language; update statement on TPM and HSM to explain the benefits of TPM and HSM regarding faster processing and securing cryptographic keys in the computer chips; add links in each section to top (top of page) to get back to table of contents (akin to those in SEQv8.02); add state abbreviation and department acronyms for title page in larger font.	WJK
8.1	11/21/2018	Update to include 800-47 Interconnection Security Agreement (ISA) language	WJK
8.11	11/29/2018	Updated a few more sections for better alignment with ISA template sent previously.	WJK
8.20	01/31/2019	Updated ISA language from revised ISA template.	GR
8.50	10/10/2019	Merged updates for TSSR sections 5.2, 5.9 and 5.13 into document and corresponding SEQv8.5 sections. Added Data Center requirements and testing requirements.	WJK

TABLE OF CONTENTS

1. Introduction

(top)

Federal standards require the Social Security Administration (SSA) to maintain oversight of the information it provides to its Electronic Information Exchange Partners (EIEPs). EIEPs are entities that have electronic information exchange agreements with the agency. EIEPs must protect the information with efficient and effective security controls.

This document consistently references the concept of EIEPs, however, the SSA Security Evaluation Questionnaire (SEQ) document will use the terms "**state agency"** or "**state agency, contractor(s), and agent(s)"** for clarity. Most state officials and agreement signatories are not familiar with the acronym EIEP; therefore, SSA will continue to use the terms "state agency" or "state agency, contractor(s), and agent(s)" in the same manner as the Computer Matching and Privacy Protection Act (CMPPA) and Information Exchange Agreements (IEA). This allows for easier alignment and mapping back to the information exchange agreements between state agencies and SSA. It will also provide a more "user-friendly" experience for the state officials who complete these forms on behalf of their state agencies.

The objective of this document is twofold. The first is to ensure that SSA can properly certify EIEPs as compliant with SSA security standards, requirements, and procedures. The second is to ensure that EIEPs adequately safeguard electronic information provided to them by SSA.

This document helps EIEPs understand the criteria that SSA uses when evaluating and certifying the system design and security features used for electronic access to SSA-provided information. Finally, this document provides the framework and general procedures for SSA's Security Certification and Compliance Review Programs.

The primary statutory authority that supports the information contained in this document is the Federal Information Security Management Act (FISMA), as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283). FISMA became law as part of the Electronic Government Act of 2002**.** FISMA is the United States legislation that defines a comprehensive framework to protect government information, operations, and assets against natural or manufactured threats. FISMA assigned the National Institute of Standards and Technology (NIST), a branch of the U.S. Department of Commerce, the responsibility to outline and define compliance with FISMA. Unless otherwise stated, all of SSA's requirements mirror the NIST-defined management, operational, and technical controls listed in the various NIST Special Publications (SP) libraries of technical guidance documents.

To gain electronic access to SSA-provided information, under the auspices of a data exchange agreement, EIEP's must comply with SSA's most current **Technical System Security Requirements (**hereafter referred to as **TSSRs)** to gain access to SSA-provided information. This document is synonymous with the Electronic Information Exchange Security Requirements and Procedures for State and Local Agencies Exchanging Electronic Information with the Social Security Administration in the

agreements. The TSSR specifies minimally acceptable levels of security standards and controls to protect SSA-provided information. SSA maintains the TSSR as a living document—subject to change--that addresses emerging threats, new attack methods and the development of new technology that potentially places SSA-provided information at risk. SSA will work with EIEPs to resolve deficiencies, which result from updates to the TSSRs. SSA refers to this process as Gap Analysis. EIEPs may proactively ensure their ongoing compliance with the TSSRs by periodically requesting the most current TSSR package from their SSA Point of Contact (POC) from the data exchange agreement.

SSA's standard for categorization of information and information systems is to provide appropriate levels of security according to risk level of Moderate in accordance with NIST 800-60. Additions, deletions, or modification of security controls directly affect the level of security and due diligence SSA requires EIEPs use to mitigate risks. The emergence of new threats, attack methods, and the development of new technology warrants frequent reviews and revisions to our TSSR. Consequently, EIEPs should expect SSA's TSSR to evolve in harmony with the industry.

2. Electronic Information Exchange (EIE) Definition

(top)

For discussion purposes herein, EIE is any electronic process in which SSA discloses information under its control to any third party for program or non-program purposes, without the specific consent of the subject individual or any agent acting on his or her behalf. EIE involves individual data transactions and data files processed within the programmatic systems of parties to electronic information sharing agreements with SSA. This includes batch processing, and variations thereof (e.g., online query) regardless of the systematic method used to accomplish the activity or to interconnect SSA with the EIEP.

3. Roles and Responsibilities

(top)

The SSA ***Office of Information Security (OIS)*** has agency-wide responsibility for interpreting, developing, and implementing security policy; providing security and integrity review requirements for all major SSA systems; developing and disseminating security training and awareness materials, and providing consultation and support for a variety of agency initiatives. SSA's security reviews ensure that external systems receiving information from SSA are secure and operate in a manner consistent with SSA's Information Technology (IT) security policies and in compliance with the terms of electronic information exchange agreements executed by SSA with outside entities. The information transferred over this interconnection may be used only for purposes explicitly stated in the corresponding data exchange agreement(s). Within the context of SSA's security policies and the terms of the electronic data exchange agreements with SSA's EIEPs, SSA exclusively conducts and brings to closure initial security certifications and triennial security compliance reviews. This includes (but not limited

to) any EIEP that processes, maintains, transmits, or stores SSA-provided information in accordance with pertinent Federal requirements.

a. The SSA Regional ***Data Exchange Coordinators*** (DECs) serve as a bridge between SSA and EIEPs. DECs assist in coordinating information exchange security review activities with EIEPs; (e.g., providing points of contact with state agencies, assisting in setting up security reviews, etc.) DECs are also the first points of contact for states if an employee of a state agency or an employee of a state agency's contractor or agent becomes aware of suspected or actual loss of SSA-provided information.

b. SSA requires **EIEPs** to adhere to the standards, requirements, and procedures, published in this TSSR document.

- "Personally Identifiable Information (PII)," covered under several Federal laws and statutes, refers to specific information about an individual used to trace that individual's identity. Information such as his/her name, Social Security Number (SSN), date and place of birth, mother's maiden name, or biometric records, alone, or when combined with other personal or identifying information is linkable or linked to a specific individual's medical, educational, financial, and employment information.

- The data (last 4 digits of the SSN) that SSA provides to its EIEPs for purposes of the Help America Vote Act (HAVA) does not identify a specific individual; therefore, is not "PII" as defined by the Act.

- Both SSA and EIEPs must remain diligent in the responsibility for establishing ***appropriate*** management, operational, and technical safeguards to ensure the confidentiality, integrity, and availability of its records and to protect against any anticipated threats or hazards to their security or integrity.

NOTE: Disclosure of Federal Tax Information (FTI) is limited to certain Federal agencies and state programs supported by federal statutes under Sections 1137, 453, and 1106 of the Social Security Act. For information regarding safeguards for protecting FTI, consult IRS Publication 1075, **Tax Information Security Guidelines for Federal, State, and Local Agencies.**

c. A **State Transmission/Transfer Component (STC)** is an organization that performs as an electronic information conduit or collection point for one or more other entities (also referred to as a hub). An STC must also adhere to the same management, operational and technical controls as SSA and the EIEP.

4. General Systems Security Standards
(top)

EIEPs that request and receive information electronically from SSA must comply with the following general systems security standards concerning access to and control of SSA-provided information.

> ***NOTE: EIEPs may not create separate files or records comprised solely of the information provided by SSA to administer programs governed by the presiding CMPPA and/or information exchange agreement.***

1. **Intent.** EIEPs must ensure that means, methods, and technology used to process, maintain, transmit, or store SSA-provided information neither prevents nor impedes the EIEP"s ability to:

   - safeguard the information to comply with SSA and NIST requirements.
   - efficiently investigate fraud, data breaches, or security events that involve SSA-provided information
   - detect instances of misuse or abuse of SSA-provided information

   For example, Utilization of cloud computing may have the potential to jeopardize an EIEP's compliance with the terms of their agreement or associated systems security requirements and procedures.

2. **Oversight.** The EIEP must process SSA-provided information under the immediate supervision and control of authorized personnel. Any changes to the processing of SSA-provided information must be approved through a documented change management process.

3. **Schedule. A** preliminary schedule for all activities involved in planning, establishing, and maintaining the interconnection will be developed and coordinated through the Office of Data Exchange (ODX). Also, both parties agree to the schedule and conditions for terminating or reauthorizing the interconnection.

4. **Data Transmission.**

   a. The EIEP must use the electronic connection established between the EIEP and SSA and any software and/or devices provided to the EIEPs only in support of the current agreement(s) between the EIEPs and SSA.

   b. SSA prohibits the EIEP from modifying any software or devices provided to the EIEPs by SSA.

   c. EIEPs must ensure that SSA-provided information is not processed, maintained, transmitted, or stored in or by means of data communications channels, electronic devices, computers, or computer networks located in geographic or virtual areas not subject to U.S. law.

5. **Data Protection.**

   a. Access. EIEPs must restrict access to the information to authorized users who need it to perform their official duties.

      NOTE: Contractors and agents (hereafter referred to as contractors) of the EIEP who process, maintain, transmit, or store SSA-provided information are held to the same security requirements as employees of the EIEP. Refer to the section Contractors of Electronic Information Exchange Partners in the Systems Security Requirements for additional information.

   a. Storage. EIEPs must store information received from SSA in a manner that, at all times, is physically and electronically secure from access by unauthorized persons.

   b. Safeguards. EIEPs must employ both physical and technological barriers to prevent unauthorized retrieval of SSA-provided information via computer, remote terminal, or other means.

   c. Confidentiality. EIEPs must advise employees with access to SSA-provided information of the confidential nature of the information, the safeguards required to protecting the information, and the civil and criminal sanctions for non-compliance contained in the applicable Federal and state laws.

6. **Incident Response.** EIEPs must have formal PII incident response procedures. When faced with a security incident, caused by malware, unauthorized access, software issues, or acts of nature, the EIEP must be able to respond in a manner that protects SSA-provided information affected by the incident.

7. **Security Awareness.** EIEPs must have an active and robust security awareness and training program, which is mandatory for all employees who access SSA-provided information.

8. **Contingency Planning.**

   a. In accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) on Contingency Planning requirements and recommendations, SSA requires EIEPs to document a senior management approved Contingency Plan that includes a Disaster Recovery Plan (DRP) that addresses both natural disaster and cyber-attack situations.

   b. SSA additionally requires the Contingency Plan to include details regarding the organizational business continuity plan (BCP) and a business impact analyses (BIA) that address the security of SSA-provided information if a disaster occurs.

   c. Critical data is to be backed up regularly, stored in a secure off-site location to prevent loss or damage, and retained for a period approved by both parties.

9. **Interconnection Security Agreement (ISA).** The ISA describes the process of data communication and the impact of the data interchange. An interconnection is defined, as the direct connection between two or more Information Technology Systems for

the purpose of sharing/exchanging the information. The interconnection must be in compliance with NIST Special publication 800-47 titled "Interconnecting Information Technology Systems", and to satisfy CA-3 control of the NIST Special publication 800-53 titled "Security & Privacy Controls for Federal Information Systems and Organizations".

10. **Planned Disconnection**. Any planned disconnections should be coordinated with the SSA internal business liaison who will notify the appropriate SSA components and the EIEP point of contact concerning the planned disconnection at least 30 business days before the disconnection takes place. Before terminating the interconnection, the initiating party should notify the other party in writing, and it should receive an acknowledgment in return. The notification should describe the reason(s) for the disconnection, provide the proposed timeline for the disconnection, and identify technical and management staff who will conduct the disconnection.

11. **Emergency Disconnect**. If one or both organizations detect an attack, intrusion attempt, or other contingency that exploits or jeopardizes the connected systems or their data, it might be necessary to abruptly terminate the interconnection without providing written notice to the other party. This extraordinary measure should be taken only in extreme circumstances and only after consultation with appropriate technical staff and senior management.

    The system owner or designee should immediately notify the other party's emergency contact by telephone or other verbal method, and receive confirmation of the notification. Both parties should work together to isolate and investigate the incident, including conducting a damage assessment and reviewing audit logs and security controls, in accordance with incident response procedures. If the incident was an attack or an intrusion attempt, law enforcement authorities should be notified, and all attempts should be made to preserve evidence.

    The initiating party should provide a written notification to the other party in a timely manner (e.g., within five days). The notification should describe the nature of the incident, explain why the interconnection was terminated, describe how the interconnection was terminated, and identify actions taken to isolate and investigate the incident. In addition, the notification may specify when and under what conditions the interconnection may be restored, if appropriate.

12. **Contingency Planning**. Both organizations should coordinate contingency planning training, testing, and exercises to minimize the impact of disasters and other contingencies that could damage the connected systems or jeopardize the confidentiality and integrity of shared data. Considerations include emergency alerts and notification; damage assessment; response and recovery, and data retrieval. The organizations are to notify each other about changes to emergency Point of Contact (POC) information (primary and alternate), including changes in staffing, addresses, telephone and fax

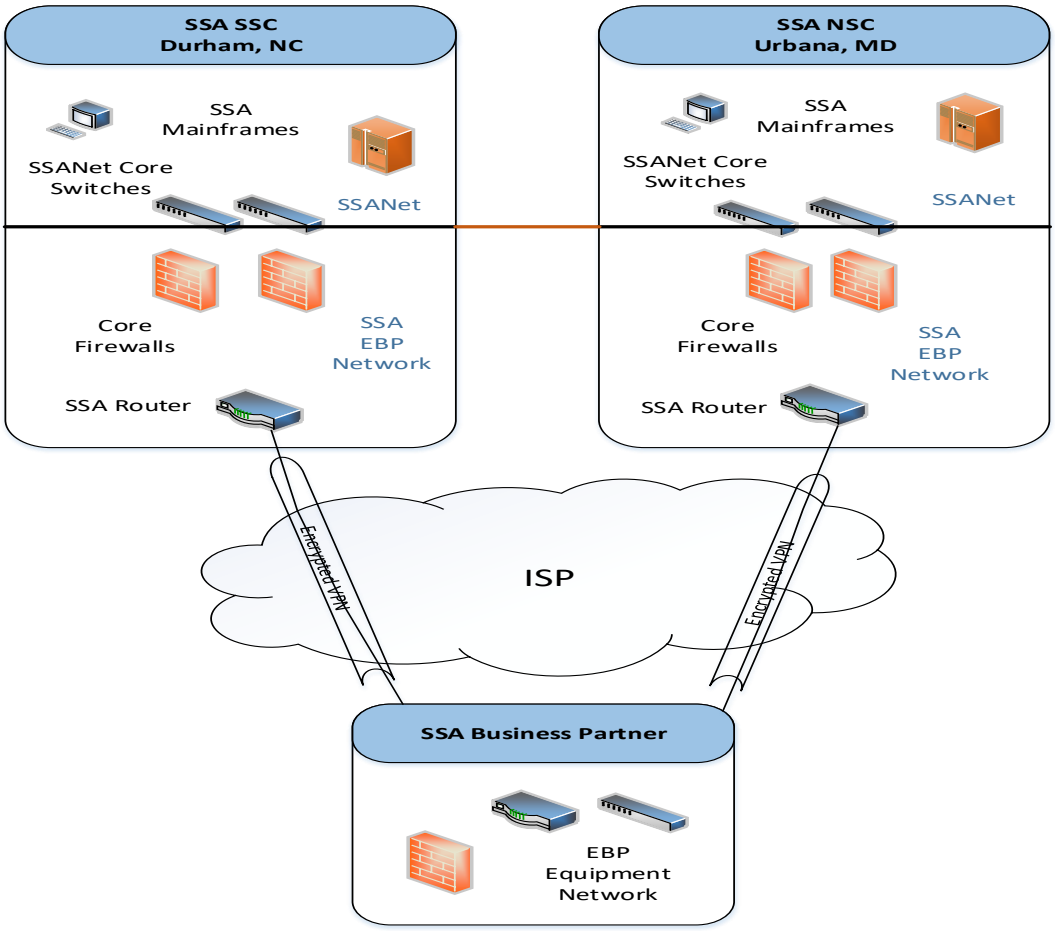
numbers, and e-mail addresses.

13. **System Configuration**. If a party intends to make technical changes to the system architecture that party will report those changes to the other party's designated technical staff counterparts before the changes are implemented. The initiating party agrees to conduct a risk assessment based on the new system architecture and to modify and re-sign a new Interconnection Security Agreement within one (1) month of implementation.

14. **Topological Drawing**. The ISA should include a topological drawing illustrating the interconnectivity from SSA to the EIEP. The drawing should include the following:

    - All communications paths, circuits, and other components used for the interconnection, from "Organization A's" system to "Organization B's" system.
    - The drawing should depict the logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations) and the physical location of the connection point.

IMAGE 1: TOPOLOGICAL DIAGRAM



15. **Security Reviews.** At its discretion, SSA or a designated third party (i.e. contractor) must have the option to conduct onsite security reviews or make other provisions, to ensure that EIEPs maintain adequate security controls to safeguard the information provided.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5. Systems Security Requirements

(top)

5.1 Overview

(top)

SSA's TSSR represent the current industry standard for security controls, safeguards, and countermeasures required for Federal information systems by Federal regulations, statutes, standards, and guidelines. Additionally, SSA's TSSR includes organizationally defined interpretations, policies, and procedures mandated by the authority of the Commissioner of Social Security in areas when or where other cited authorities may be silent or non-specific.

SSA must certify that the EIEP has implemented security controls that meet the requirements and work as intended, before the authorization to initiate transactions to and from SSA, through batch data exchange processes or online processes such as State Online Query (SOLQ), Internet SOLQ (SOLQ-I), Unemployment Inquiry Query (UIQ), or Social Security Online Verification (SSOLV).

The TSSR addresses management, operational, and technical aspects of safeguards to ensure only authorized disclosure and usage of SSA provided information used, maintained, transmitted, or stored by SSA's EIEPs. SSA requires EIEPs to maintain an organizational access control structure that adheres to a three-tiered best practices model. The SSA recommended model is "separation of duties," "need-to-know" and "least privilege." based on each user's position and job-related duties.

SSA requires EIEPs to document and notify SSA if they plan to share SSA-provided information with another entity, or to allow them direct access to their system. This includes (but not limited to) law enforcement, other state agencies, and state/Federal organizations that perform audit, quality, or integrity functions.

SSA recommends that the EIEP develop, publish, and maintain a comprehensive Information Technology (IT) Systems Security Policy (SSP) document that specifically addresses:

1) the classification of information processed and stored within the network,

2) management, operational, and technical controls to protect the information stored and processed within the network,

3) access to the various systems and subsystems within the network,

4) Security Awareness Training,

5) Employee and End User Sanctions Policy,

6) Contingency Planning and Disaster Recovery,

7) Incident Response Policy, and

8) The disposal of protected information and sensitive documents derived from the system or subsystems on the network.

9) The use of SSA production data in a testing or development environment to verify a new software application or development environment is fully functional such as a newly coded eligibility system or network operating system as UNIX, Linux or Windows.

10) A change in physical storage and processing environment such as a new data center not previously certified or a migration to a cloud or managed service provider such as AWS or Azure.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.2 General System Security Design and Operating Environment

(Planning (PL) Family – (System Security Plan), Contingency Plan (CP) Family, Physical and Environmental (PE) Family, NIST SP 800-53 rev. 4) –

(top)

All security controls evaluated at the Moderate level.

In accordance with the NIST suite of Special Publications (SPs) (e.g., 800-53, 800-34, 800-47, etc.), SSA requires the EIEP to maintain policies, procedures, descriptions, and explanations of their overall system design, configuration, security features, and operational environment. They should include explanations of how they conform to SSA's TSSRs. The EIEPs General System Security design and Operating Environment must also address:

a) The operating environment(s) in which the EIEP will utilize, maintain, store, and transmit SSA-provided information,

b) The business process(es) in which the EIEP will use SSA-provided information,

c) The physical safeguards employed to ensure that unauthorized personnel, the public or visitors to the agency cannot access SSA-provided information,

d) Details of how the EIEP keeps audit information pertaining to the use and access to SSA-provided information and associated applications readily available,

e) Electronic safeguards, methods, and procedures for protecting the EIEP's network infrastructure and for protecting SSA-provided information while in transit, in use within a process or application, and at rest,

f) A senior management approved Information System Contingency Plan (ISCP) that addresses both internal and external threats. SSA requires the ISCP to include details regarding the organizational business continuity plan (BCP) and a business impact analyses (BIA) that addresses the security of SSA-provided information if a disaster occurs. SSA recommends that state agencies perform disaster exercises at least once annually.

g) How the EIEP prevents unauthorized retrieval of SSA-provided information by computer, remote terminal, or other means; including descriptions of security software other than access control software (e.g., security patch and anti-malware software installation and maintenance, etc.),

h) How the configurations of devices (e.g., servers, workstations, portable devices) involving SSA-provided information complies with recognized industry standards (i.e. NIST SP's) and SSA's TSSR.

i) The organizational structure of the agency, number of users, and all external entities that will have access to the system and/or application that displays, transmits, and/or application that displays, transmits and/or stores SSA-provided information.

j) Hardware and software supporting the interconnection, including interconnection points is in a secure location that is protected from unauthorized access, interference, or damage. The environmental controls are in place to protect against hazards such as fire, water, and excessive heat and humidity. In addition, computer workstations are in secure areas to protect them from damage, loss, theft, or unauthorized physical access. Access badges, cipher locks, or biometric devices are in place to control access to secure areas.

k) Data encryption is to use the strongest defined in FIPS-197 (Advanced Encryption Standard (AES)). Server authentication is to require the use of a key exchange. VPN software or a dedicated circuit will be used for all data transfers.

l) Firewalls are in place to protect internal networks and other resources from unauthorized access across the interconnection, or configure existing firewalls accordingly. If the interconnection involves the use of servers, they are hosted in a separately protected "demilitarized zone" (DMZ), which may be accomplished by installing two firewalls: one on the external line and one at the connection to internal networks. (Alternately, a firewall could be installed on the external line and a security portal installed at the internal connection.) Firewall ports are configured properly and all default passwords have been changed.

m) One or both organizations have implement IDS to detect undesirable or malicious activity that could affect the interconnection or data that pass over it. A combination of network-based and host-based IDSs may be used, if appropriate. Alert mechanisms are in place to notify system administrators or security officers when intrusions or unusual activities are detected

n) The security of the information transferred on this two-way connection is protected using FIPS 140-2 validated encryption mechanisms. The connections at each end are located within controlled access facilities. Individual users will

not have access to the data except through their authorized system security access control software.

o) EIEP's system and users will protect the integrity of SSA data and systems, and in reciprocity SSA's system and users will protect the integrity of the EIEP's data and systems, in accordance with the EIEP's policy, the Privacy Act and Trade Secrets Act (18 US Code 1905) and the Unauthorized Access Act (18 US Code 2701 and 2710).

p) The use of live SSA information in test environments should generally be avoided and is not authorized unless specifically approved by the Office of Information Security through the submission of a formal request. At least 60 day in advance, agencies must formally request SSA approval to use live SSA information in a testing environment.

SSA defines live data as primarily unmodified, non-sanitized data extracted from SSA files that identifies a specific individual SSA provided information. The use of live data in testing environments is limited to the terms of the Information Exchange Agreement or other authorized SSA purposes and may be disclosed only to those individuals with a need-to-know.

Any systems within pre-production testing environments ideally will be configured according to requirements in this publication. However, the Office of Information Security understands most agencies may not be able to fully implement all TSSR requirements in a test environment.

Agencies wishing to use live SSA data in pre-production must submit a formal request to SSA's Office of Information Security for authority to use live data for testing, providing a detailed explanation of the safeguards in place to protect the data and the necessity for using live data during testing.

Need and Use Justification statements should be revised to cover this use of SSA data, if not already addressed. State agencies should check their Information Exchange Agreements to verify if "testing purposes" is covered.

Testing efforts that use live SSA data primarily fall into two categories: one-time testing and ongoing testing.

An example of a one-time testing use of live SSA data would be for system testing that is done prior to a new system implementation and, once testing has validated that the data will work properly, the live SSA data is not required to continue to remain in the test environment. For one-time testing efforts, the Office of

Safeguards requires the SSA data to be deleted from systems and databases upon completion of testing efforts, and that the hard drive of the test systems be sanitized electronically prior to repurposing the system for other state agency testing efforts.

Duration for ongoing test activities will be agreed upon as part of the live data request process. Some examples of ongoing testing efforts include:

a. Testing of extract, transform, and load (ETL) process to validate federal data loading into a database.

b. Application testing of eligibility modeling that requires data match between the entire population of state and federal information, where building a set of dummy data is not feasible.

Note: At its discretion, SSA or a third party (i.e. contractor) must have the option to conduct onsite security reviews or make other provisions, to ensure that EIEPs maintain adequate security controls to safeguard the information provided.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.3 System Access Control

(Access Control (AC) Family, NIST SP 800-53 rev. 4, NIST SP 800-63)

(top)

EIEPs must utilize and maintain technological (logical) access controls that limit access to SSA-provided information and associated transactions and functions to only those users, processes acting on behalf of authorized users, or devices (including other information systems) authorized for such access based on their official duties or purpose(s). EIEPs must employ a recognized user-access security software package (e.g., RAC-F, ACF-2, TOP SECRET, Active Directory, etc.) or a security software design, which is equivalent to such products. The access control software must employ and enforce (1) PIN/password, and/or (2) PIN/biometric identifier, and/or (3) Smartcard/biometric identifier, etc., (for authenticating users), (and lower case letters, numbers, and special characters; password phrases) for the user accounts of persons, processes, or devices whose functions require access privileges in excess of those of ordinary users.

The EIEP's password policies must require stringent password construction as supported by current NIST guidelines for the user accounts of persons, processes, or devices whose functions require access privileges above those of ordinary users. **SSA strongly requires Two-Factor Authentication.**

The EIEP's implementation of the control software must comply with recognized industry standards. Password policies should enforce sufficient construction strength (length and complexity) to defeat or minimize risk-based, identified vulnerabilities

The EIEP's password policies must require stringent password construction (e.g., passwords greater than eight characters in length requiring upper and lower case letters, numbers, and/or special characters; password phrases) for the user accounts of persons, processes, or devices whose functions require access privileges in excess of those of ordinary users.

In addition, SSA has the following specific requirements in the area of Access Control:

1. Upon hiring or before granting access to SSA-provided information, EIEPs should verify the identities of any employees, contractors, and agents who will have access to SSA-provided information in accordance with the applicable agency or state's "personnel identity verification policy."

2. SSA requires that state agencies have a logical control feature that designates a maximum number of unsuccessful login attempts for agency workstations

and devices that store or process SSA-provided information, in accordance with NIST guidelines. SSA recommends no fewer than three (3) and no greater than five (5).

3. SSA requires that the state agency designate specific official(s) or functional component(s) to issue PINs, passwords, biometric identifiers, or Personal Identity Verification (PIV) credentials to individuals who will access SSA-provided information. **SSA also requires that the state agency prohibit any functional component(s) or official(s) from issuing credentials or access authority to themselves or other individuals within their job-function or category of access.**

4. SSA requires that EIEPs grant access to SSA-provided information based on least privilege, need-to-know, and separation of duties. State agencies should not routinely grant employees, contractors, or agents access privileges that exceed the organization's business needs. SSA also requires that EIEPs periodically review employees, contractors, and agent's system access to determine if the same levels and types of access remain applicable.

5. If an EIEP employee, contractor, or agent is subject to an adverse administrative action by the EIEP (e.g., reduction in pay, disciplinary action, termination of employment), SSA recommends the EIEP remove his or her access to SSA-provided information in advance of the adverse action to reduce the possibility that will the employee will perform unauthorized activities that involve SSA-provided information.

6. SSA requires that remote access for work home and Internet access comply with applicable Federal and state security policy and standards. Furthermore, the EIEPs access control policy must define the safeguards in place to adequately protect SSA-provided information for work-at-home, remote access, and/or Internet access.

7. SSA requires EIEPs to design their system with logical control(s) that prevent unauthorized browsing of SSA-provided information. SSA refers to this setup as a **Permission Module**. The term "**Permission Module**" supports a business rule and systematic control that prevents users from browsing a system that contains SSA-provided information. It also supports the principle of **referential integrity**. It should prevent non-business related or unofficial access to SSA-provided information. Before a user or process requests SSA-provided information for verification, the system should verify it is an authorized transaction. Some organizations use the term "referential

integrity" to describe the verification step. A properly configured Permission Module should prevent a user from performing any actions not consistent with a need-to-know business process. If a logical permission module configuration is not possible, the state agency must enforce its Access Control List (ACL) in accordance with the principle of least privilege. **The only acceptable compensating control for a system that lacks a permission module is a 100% review of all transactions that involve SSA-provided information.**

8. Logical access controls are in place to designate users who have access to system resources and the types of transactions and functions they are permitted to perform. Access control lists (ACL) and access rules specify the access privileges of authorized personnel, including the level of access and the types of transactions and functions that are permitted (e.g., read, write, execute, delete, create, and search). Hardware and software are configured with ACLs, or the ACLs are administered offline and distributed to routers and other devices. Access control rules are in place to grant appropriate access privileges to authorized personnel, based on their roles or job functions. Only system administrators have access to the controls. In addition, a log-on warning banner is in place to notify unauthorized users that they have accessed a computer system that contains Federal data and unauthorized use can be punishable by fines or imprisonment. Each organization's Legal Counsel has approved the terms of the warning.

9. Identification and authentication is used to prevent unauthorized personnel from entering an IT system. Strong mechanisms are in place to identify and authenticate users to ensure that they are authorized to access the interconnection. Mechanisms that may be used include user identification and passwords, digital certificates, authentication tokens, biometrics, and smart cards. If passwords are used, they are at least eight characters long, have a mixture of alphabetic and numeric characters, and are changed at predetermined intervals. Master password files are encrypted and protect against unauthorized access. If digital signatures are used, the technology conforms to Federal Information Processing Standard (FIPS) 186-2, Digital Signature Standard (DSS). Depending on data sensitivity, organizations may permit users to access the interconnection after they have authenticated to their local domain, reducing the need for multiple passwords or other mechanisms. Applications operating across the interconnection could rely on authentication information from the user's local domain, using a proxy authentication mechanism.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.4 Automated Audit Trail System (ATS)

(Audit and Accountability (AU) Family, NIST SP 800-53 rev. 4)

(top)

SSA requires EIEPs, STCs, or other agencies that provide audit trail services to other state agencies that receive information electronically from SSA, to implement and maintain a fully automated audit trail system (ATS). The system must be capable of creating, storing, protecting, and (efficiently) retrieving and collecting records identifying the individual user who initiates a request for information from SSA or accesses SSA-provided information. At a minimum, individual audit trail records must contain the data needed (including date and time stamps) to associate each query transaction or access to SSA-provided information with its initiator (i.e., user identification), device/workstation, their action, if any, and the relevant business purpose/process (e.g., SSN verification for Medicaid). Each entry in the audit file must be stored as a separate record, not overlaid by subsequent records. The ATS must create transaction files to capture all input from interactive internet applications that access or query SSA-provided information.

- The agency's ATS must keep records of "read only" views and system access events that do not result in a change to data or a new transaction.

- All viewing of SSA provided information require an Audit Trail (No Exceptions).

SSA requires that the agency's ATS create an audit record when users view screens that contain SSA-provided information. If an STC or other agency handles and audits the EIEP's transactions with SSA or viewing of SSA-provided information, the EIEP is responsible for ensuring that the STC's or other agency's audit capabilities meet NIST's guidelines for an automated audit trail system. The EIEP must also establish a process to obtain specific audit information from the STC or other agency regarding the EIEP's SSA transactions and viewing of SSA-provided information.

SSA requires that EIEPs have automated retrieval and collection of audit records. Such automated functions can be via online queries, automated reports, batch processing, or any other logical means of delivering audit records in an expeditious manner. Information in the audit file must be retrievable by an automated method and must allow the EIEP the capability to make them available to SSA upon request.

Access to the audit file must be restricted to authorized users with a "need to know," audit file data must be unalterable (read-only), and maintained for a minimum of three (3) (preferably seven (7)) years. Information in the audit file must be retrievable

by an automated method and must allow the EIEP the capability to make them available to SSA upon request. The EIEP must backup audit trail records on a regular basis to ensure its availability. EIEPs must apply the same level of protection to backup audit files that apply to the original files to ensure the integrity of the data.

If the EIEP retains SSA-provided information in a database (e.g., Access database, SharePoint, etc.), or if certain data elements within the EIEP's system indicates to users that SSA verified the information, the EIEP's system must also capture an audit trail record of users who view SSA-provided information stored within the EIEP's system. The retrieval requirements for SSA-provided information at rest and the retrieval requirements for regular transactions are identical. **Similar to the Permission Module requirement above, the only acceptable compensating control for a system that lacks an Automated Audit Trail System (ATS) is a 100% review of all transactions that involve SSA-provided information.**

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.5 Personally Identifiable Information (PII)

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and AP Family – Authority and Purpose (Privacy Controls), NIST SP 800-53 rev. 4), OMB Memorandum M-17-12

(top)

Personally Identifiable Information (PII) is information used to distinguish or trace an individual's identity, such as their name, Social Security Number, biometric records, alone or when combined with other personal or identifying information linked or linkable to a specific individual. An item such as date and place of birth, mother's maiden name, or father's surname is PII, regardless of whether combined with other data.

SSA defines ***a PII loss*** as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) an authorized user accesses or potentially accesses personally identifiable information for an other than authorized purpose. PII loss is a reportable incident. SSA requires that contracts for periodic disposal/destruction of case files or other media contain a non-disclosure agreement signed by all personnel who will encounter products that contain SSA-provided information.

If a PII loss involving SSA-provided information occurs or is suspected, the EIEP must be able to quantify the extent of the loss and compile a complete list of the individuals potentially affected by the incident (refer to ***Incident Reporting***).

The EIEP should have procedural documents to describe methods and controls for safeguarding SSA-provided PII while in use, at rest, during transmission, or after archiving. The document(s) should explain how the EIEP manages and handles SSA-provided information on print and removable media, and explain how the methods and controls conform to NIST requirements. SSA requires that any items that contain SSA-provided PII always remain in the custody of authorized EIEP employees, contractors, or agents. SSA also requires that the agency destroy the items when no longer required for the EIEP's business process. If retained in paper files for evidentiary purposes, the EIEP should safeguard such PII in a manner that prevents unauthorized personnel from accessing such materials. All agencies that receive SSA-provided information must maintain an inventory of all documents that outline statewide or agency policy and procedures regarding retention schedules and storing SSA provided information.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.6 Monitoring and Anomaly Detection

(Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations, NIST SP 800-137, E-Government Act of 2002 (P.L. 107-347), and Security Assessment and Authorization (CA) and Risk Assessment (RA) Families, NIST SP 800-53 rev. 4)

(top)

SSA requires that the EIEPs use an Intrusion Protection System (IPS) or an Intrusion Detection System (IDS). The EIEP must establish and/or maintain continuous monitoring of its network infrastructure and assets to ensure that:

a) the EIEP's security controls continue to be effective over time,

b) the EIEP uses industry-standard Security Information Event Manager (SIEM) tools, anti-malware software, and effective antivirus protection,

c) only authorized individuals, devices, and processes have access to SSA-provided information,

d) the EIEP detects efforts by external and internal entities, devices, or processes to perform unauthorized actions (e.g., data breaches, malicious attacks, access to network assets, software/hardware installations, etc.) as soon as they occur,

e) the necessary parties are immediately alerted to unauthorized actions performed by external and internal entities, devices, or processes,

f) upon detection of unauthorized actions, measures are immediately initiated to prevent or mitigate associated risk,

g) in the event of a data breach or security incident, the EIEP can efficiently determine and initiate necessary remedial actions, and

h) trends, patterns, or anomalous occurrences and behavior in user or network activity that may be indicative of potential security issues are readily discernible.

i) Appropriate authentication required to access each of the interconnected systems.

j) Detection, refusal and logging of any connection attempt from a non-prescribed host.

k) Detection, refusal and logging of any request for unapproved service or use of the interconnection.

l) Operational Security Mode. The SSA Network is operating in a multi-level security mode. Access to required resources is only allowed via secure transport, with system level security further restricting access to data.

m) Security Documentation. Adheres to the NIST regulations governing Security Assessment and Authorization (SA&A) for all security authorization boundaries. Applicable System Security Plans (SSPs) are to be updated.

n) Change Management. In the event that [EXTERNAL AGENCY] or SSA make changes which trigger the need for re-authorization it would require the ISA to be updated and reauthorized by both parties.

The EIEP's system must include the capability to prevent users from unauthorized browsing of SSA records. SSA requires the use of a transaction-driven **permission module design**, whereby employees are unable to initiate transactions not associated with the normal business process. If the EIEP uses such a design, they also must have anomaly detection to monitor an employee's unauthorized attempts to gain access to SSA-provided information and attempts to obtain information from SSA for clients not in the EIEP's client system. The EIEP should employ measures to ensure the permission module's integrity. Users should not be able to create a bogus case and subsequently delete it in such a manner that it goes undetected. The SSA permission module design employs both role and rules based logical access control restrictions. (Refer to ***Access Control***)

If the EIEP's design ***does not use*** a permission module ***and*** is not transaction-driven, until at least one of these security features exists, the EIEP must develop and implement **compensating security controls (both management and operational)** to deter employees from browsing SSA records. These controls must include monitoring and anomaly detection features, such as: systematic, manual, or a combination thereof. Such features must include the capability to detect anomalies in the volume and/or type of transactions or queries requested or initiated by individuals and include systematic or manual procedures for verifying that requests and queries of SSA-provided information comply with valid official business purposes.

Risk Management Program

SSA requires that EIEPs develop and maintain a published Risk Assessment Policy and Procedures document. A Risk Management Program may include, but is not limited to the following:

1. A risk assessment policy that addresses purpose, scope, roles, responsibilities,

management commitment, coordination among organizational entities, and compliance,

2. Procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls,

3. A function that conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits,

4. An independent function that conducts vulnerability and risk assessments, reviews risk assessment results, and disseminates such information to senior management,

5. A firm commitment from senior management to update the risk assessment whenever there are significant changes to the information system or environment of operation or other conditions that may affect the security of SSA-provided information,

6. A robust vulnerability scanning protocol that employs industry standard scanning tools and techniques that facilitate interoperability among tools and automates parts of the vulnerability management process,

7. Remediates legitimate vulnerabilities in accordance with an organizational assessment of risk, and

8. Shares information obtained from the vulnerability scanning process and security control assessments with senior management to help eliminate similar vulnerabilities in other information systems that receive, process, transmit, or store SSA-provided information.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.7 Management Oversight and Quality Assurance

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and the AC – Access Control & PM – Program Management Families, NIST SP 800-53 rev. 4)

(top)

SSA requires the EIEP's senior management officials to establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized users have access to SSA-provided information. This will ensure there is ongoing compliance with the terms of the EIEP's electronic information sharing agreement with SSA and the TSSRs established for access to SSA-provided information. The senior management official's entity responsible for management oversight should consist of one or more of the EIEP's management officials whose job functions include responsibility to ensure that the EIEP only grants access to the appropriate users and position types (least privilege), which require the SSA-provided information to do their jobs (need-to-know).

SSA requires the EIEP's senior management officials ensure that users granted access to SSA-provided information receive adequate training on the sensitivity of the information, associated safeguards, operating procedures, and the civil and criminal consequences or penalties for misuse or improper disclosure.

SSA requires that EIEPs establish the following job functions and require that only users whose job functions are separate from personnel who request or use SSA-provided information.

SSA requires that EIEPs establish the following job functions separate from personnel who request or use SSA-provided information. Federal requirements, SSA policy, and NIST guidelines exclude any employee who uses SSA provided information to process programmatic workloads to make benefit or entitlement determinations from participation in management or quality assurance functions.

a) Perform periodic self-reviews to monitor the EIEP's ongoing usage of SSA-provided information.
b) Perform random sampling of work activity that involves SSA-provided information to determine if the access and usage comply with SSA's requirements

SSA recommends the EIEPs produce reports that allow management and/or supervisors to monitor user activity. If applicable, the EIEP's senior management officials must have a process for distributing monitoring and exception reports to appropriate local managers/supervisors or to local security officers. The process must ensure that only those whose responsibilities include monitoring anomalous activity of users, to include those who have elevated system rights and privileges, use the reports. SSA supports the use of a modernized Security Information and Event Management (SIEM) solution as a tool to enhance the agency's continuous monitoring program. The following types of reports represent a baseline of the information most modern SIEM solutions may produce. While SSA does not define the exact type of reports necessary to maintain a healthy continuous monitoring

program, EIEPs must use a comprehensive strategy to safeguard SSA-provided information from unauthorized access and disclosure. Federal policies dictates that EIEPs have management and operational controls that account for all access to SSA-provided information by end users, database administrators, and management personnel.

1. **User ID Login Exception Reports, or similar:**

   This type of report captures information about users who enter incorrect user IDs when attempting to gain access to the system or to a transaction that initiates requests for information from SSA, including failed attempts to enter a password.

2. **Inquiry Match Exception Reports. or similar:**

   This type of report captures information about users who initiate transactions for SSNs that have no client case association within the EIEP's system, if, and only if, such systems lack a Permission Module **(the EIEP's management must review 100% of these cases).**

3. **System Error Exception Reports or similar:**

   This type of report captures information about users, usually with elevated privileges, who may not understand or who inadvertently violate proper procedures for access to SSA-provided information. This report pertains to archived SSA provided information retained for auditing or state retention regulatory purposes.

4. **Inquiry Activity Statistical Reports or similar:**

   This type of report captures information about transaction usage patterns among authorized end users and enables the EIEP's management to contrast typical usage patterns with extraordinary usage patterns.

The EIEP must have a process for distributing these monitoring and exception reports to appropriate local managers/supervisors or to local security officers. The process must ensure that only those whose responsibilities include monitoring anomalous activity of users, to include those who have exceptional system rights and privileges, use the reports.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.8 Data and Communications Security

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and the Access Control (AC), Configuration Management (CM), Media Protection (MP), and System and Communication (SC) Families, NIST SP 800-53 rev. 4)

(top)

SSA requires EIEPs to encrypt PII and SSA-provided information when transmitting across dedicated communications circuits between its systems, intrastate communications between its local office locations, and on the EIEP's mobile computers, devices and removable media. The EIEP's encryption methods must align with the Guidelines established by the National Institute of Standards and Technology (NIST).

Encryption is used to ensure that data cannot be read or modified by unauthorized users. Encryption is implemented in devices such as routers, switches, firewalls, servers, and computer workstations. Devices are configured to apply the appropriate level of encryption required for data that pass over the interconnection. If required, encryption mechanisms (e.g., digital signatures) are in place to authenticate users to the interconnection and to shared applications, and to provide nonrepudiation.

EIEP agree to maintain adequate security controls in accordance with FIPS 199, FIPS 200 and NIST SP 800-53 Recommended Security Controls for Federal Systems, including specific access control lists (ACL) at perimeter routers and firewalls, to permit outbound and inbound network traffic for only specified protocols, ports, and hosts. Routers and firewalls shall be configured to prevent exploitation of the interconnection to gain unauthorized access to other organizations or interconnected IT systems, networks, devices and resources. Security controls to provide this protection include:

SSA requires encryption based on FIPS 140-2. **Files encrypted for external users (when using tools such as Microsoft Word encryption,) require a key length of at least nine characters.** SSA recommends that the key (also referred to as a password) contain both special characters and numbers. SSA supports the NIST Guidelines that requires the EIEP deliver the key so that it does not accompany the media. The EIEP must secure the key when not in use or unattended.

SSA discourages the use of the public Internet for transmission of SSA-provided information. If, however, the EIEP uses the public Internet or other electronic communications, such as emails and faxes to transmit SSA-provided information, they must use a secure encryption protocol such as Secure Socket Layer (SSL) or Transport Layer Security (TLS). SSA also recommends 256-bit encryption protocols or more secure methods such as Virtual Private Network technology. The EIEP should only send data to a secure address or device to which the EIEP can control and limit access to only specifically authorized individuals and/or processes. **SSA recommends that EIEPs use Media Access Control (MAC) Filtering and Firewalls to protect access points from unauthorized devices attempting to connect to the network.**

EIEPs should not retain SSA-provided information any longer than business purpose(s) dictate. The IEA with SSA stipulates a time for data retention. The EIEP should delete, purge, destroy, or return SSA-provided information when the business purpose for retention no longer exists.

The EIEP may not save or create separate files comprised solely of information provided by SSA. The EIEP may apply specific SSA-provided information to the EIEP's matched record from a preexisting data source. Federal law prohibits duplication and disclosure of SSA-provided information without written approval from SSA. This prohibition applies to both internal and external sources who do not have a "need-to-know."
SSA recommends that EIEPs use either **Trusted Platform Module (TPM)** or **Hardware Security Module (HSM)** technology solutions to encrypt data at rest on hard drives and other data storage media.

SSA requires EIEPs to prevent unauthorized disclosure of SSA-provided information after they complete processing and after the EIEP no longer requires the information. The EIEP's operational processes must ensure that no residual SSA-provided information remains on the hard drives of user's workstations after the user exits the application(s) that use SSA-provided information. If the EIEP must send a computer, hard drive, or other computing or storage device offsite for repair, the EIEP must have a non-disclosure clause in their contract with the vendor. If the EIEP used the item in connection with a business process that involved SSA-provided information and the vendor will retrieve or may view SSA-provided information during servicing, SSA reserves the right to inspect the EIEP's vendor contract. The EIEP must remove SSA-provided information from electronic devices before sending it to an external vendor for service. SSA expects the EIEP to render SSA-provided information unrecoverable or destroy the electronic device if they do not need to recover the information. The same applies to excessed, donated, or sold equipment placed into the custody of another organization.

To sanitize media, the EIEP should use one of the following methods:

1. **Overwriting/Clearing:**

   Overwrite utilities can only be used on working devices. Overwriting is appropriate only for devices designed for multiple reads and writes. The EIEP should overwrite disk drives, magnetic tapes, floppy disks, USB flash drives, and other rewriteable media. The overwrite utility must completely overwrite the media. SSA recommends the use of ***purging*** media sanitization to make the data irretrievable, protecting data against laboratory attacks or forensics. Reformatting the media does not overwrite the data.

2. **Degaussing:**

   Degaussing is a sanitization method for magnetic media (e.g., disk drives, tapes, floppies, etc.). Degaussing is not effective for purging non-magnetic

media (e.g., optical discs). SSA and NIST Guidelines require EIEP to use a certified tool designed to degauss each particular type of media. NIST guidelines require certification of the tool to ensure that the magnetic flux applied to the media is strong enough to render the information irretrievable. The degaussing process must render data on the media irretrievable by a laboratory attack or laboratory forensic procedures.

3. **Physical destruction:**

   NIST guidelines require physical destruction when degaussing or over-writing cannot be accomplished (for example, CDs, floppies, DVDs, damaged tapes, hard drives, damaged USB flash drives, etc.). Examples of physical destruction include shredding, pulverizing, and burning.

State agencies may retain SSA-provided information in hardcopy only if required to fulfill evidentiary requirements, provided the agencies retire such data in accordance with applicable state laws governing state agency's retention of records. The EIEP must control print media containing SSA-provided information to restrict access to authorized employees who need such access to perform official duties. EIEPs must destroy print media containing SSA-provided information in a secure manner when no longer required for business purposes. SSA requires the EIEP to destroy paper documents that contain SSA-provided information by burning, pulping, shredding, macerating, or other similar means that ensure the information is unrecoverable.

NOTE: Hand tearing or lining through documents to obscure information does not meet SSA's requirements for appropriate destruction of PII.

State agencies may use any accretions, deletions, or changes to the SSA-provided information governed by the CMPPA agreement to update their master files or federally funded state-administered benefit program applicants and recipients and retain such master files in accordance with applicable state laws governing State Agencies' retention of records.

Data and information that pass from one IT system to the other are scanned with antivirus software to detect and eliminate malicious code, including viruses, worms, and Trojan horses. Antivirus software is installed on all servers and computer workstations linked to the interconnection. The software is automatically updated and properly maintained with current virus definitions. In addition, virus scanning is included in user training to ensure that users understand how to scan computers, file downloads, and e-mail attachments. Procedures are written and responsibilities are assigned for responding to and recovering from malicious code attacks.

Special Note regarding Cloud Service Providers:

If the EIEP will store SSA-provided information through a Cloud Service Provider, please provide the name and address of the cloud provider. Describe the security responsibilities the contract requires to protect SSA-provided information.

SSA will ask for detailed descriptions of the security features contractually required of the cloud provider and information regarding how they will protect SSA-provided information at rest and when in transit.

EIEPs cannot legally process, transmit, or store SSA-provided information in a cloud environment without explicit permission from SSA's Chief Information Officer (CIO).

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.9 Incident Reporting

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and the Incident Response (IR) Family, NIST SP 800-53 rev. 4)

(top)

FISMA, NIST guidelines, and Federal Law require the EIEP to develop and implement policies and procedures to respond to potential data breaches or PII loses. EIEPs must articulate, in writing, how the policies and procedures conform to SSA's requirements. The procedures must include the following information:

> *If your agency experiences or suspects a breach or loss of PII or a security incident, which includes SSA-provided information, they must notify the State official responsible for Systems Security designated in the agreement. That State official or delegate must then notify the SSA Regional Office Contact or the SSA Systems Security Contact identified in the agreement. If, for any reason, the responsible State official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact* ***within one hour****, the responsible State Agency official or delegate must report the incident by contacting* ***SSA's National Network Service Center (NNSC) toll free at 1-877-697-4889*** *(select "Security and PII Reporting" from the options list). As the final option, in the event SSA contacts and NNSC both cannot be reached, the EIEP is to contact SSA's Office of Information Security, Security Operations Center at 1-866-718-6425 The EIEP will provide updates as they become available to SSA contact, as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.*

If SSA, or another Federal investigating entity (e.g. TIGTA or DOJ), determines that the risk presented by a breach or security incident requires that the state agency notify the subject individuals, the agency must agree to absorb all costs associated with notification and remedial actions connected to security breaches. **SSA and NIST Guidelines encourage agencies to consider establishing incident response teams to address PII and SSA-provided information breaches.**

Incident reporting policies and procedures are part of the security awareness program. Incident reporting pertains to all employees, contractors, or agents regardless as to whether they have direct responsibility for contacting SSA. The written policy and procedures document should include specific names, titles, or functions of the individuals responsible for each stage of the notification process. The document should include detailed instructions for how, and to whom each employee, contractor, or agent should report the potential breach or PII loss.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.10 Security Awareness Training and Employee Sanctions

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and Awareness and Training (AT), Personnel Security (PS), and Program Management (PM) Families, NIST SP 800-53 rev. 4)

(top)

The EIEP must have an active and robust security awareness program and security training for all employees, contractors, and agents who access SSA-provided information. The training and awareness programs must include:

a. the sensitivity of SSA-provided information and addresses the Privacy Act and other Federal and state laws governing its use and misuse,

b. the rules of behavior concerning use and security in systems and/or applications processing SSA-provided information,

c. the restrictions on viewing and/or copying SSA-provided information,

d. the responsibilities of employees, contractors, and agent's pertaining to the proper use and protection of SSA-provided information,

e. the proper disposal of SSA-provided information,

f. the security breach and data loss incident reporting procedures,

g. the basic understanding of procedures to protect the network from malware attacks,

h. spoofing, phishing and pharming, and network fraud prevention, and

i. the possible criminal and civil sanctions and penalties for misuse of SSA-provided information.

The training must be annual, mandatory, and certified by the personnel who receive the training. SSA also requires the EIEP to certify that each employee, contractor, and agent who views SSA-provided information certify that they understand the potential criminal, civil, and administrative sanctions or penalties for unlawful assess and/or disclosure.

SSA requires the state agency to require employees, contractors, and agents to sign a non-disclosure agreement, attest to their receipt of Security Awareness Training, and acknowledge the rules of behavior concerning proper use and security in systems that process SSA-provided information. The non-disclosure attestation must also include

acknowledgement from each employee, contractor, and agent that he or she understands and accepts the potential criminal and/or civil sanctions or penalties associated with misuse or unauthorized disclosure of SSA-provided information. The state agency must retain the non-disclosure attestations for at least five (5) to seven (7) years for each individual who processes, views, or encounters SSA-provided information as part of their duties.

SSA strongly recommends the use of login banners, emails, posters, signs, memoranda, special events, and other promotional materials to encourage security awareness throughout your enterprise.

The state agency must designate a department or party to take the responsibility to provide ongoing security awareness training for all employees, contractors, and agents who access SSA-provided information. Training must include:

- The sensitivity of SSA-provided information and address the Privacy Act and other Federal and state laws governing its use and misuse
- Rules of behavior concerning use and security in systems processing SSA-provided information
- Restrictions on viewing and/or copying SSA-provided information
- The employee, contractor, and agent's responsibility for proper use and protection of SSA-provided information
- Proper disposal of SSA-provided information
- Security incident reporting procedures
- Basic understanding of procedures to protect the network from malware attacks
- Spoofing, Phishing and Pharming scam prevention
- The possible sanctions and penalties for misuse of SSA-provided information

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.11 Contractors of Electronic Information Exchange Partners

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and Risk Assessment (RA), System and Services Acquisition (SA), Awareness and Training (AT), Personnel Security (PS), and Program Management (PM) Families, NIST SP 800-53 rev. 4)

(top)

The state agency's employees, contractors, and agents who access, use, or disclose SSA information in a manner or purpose not authorized by the Agreement may be subject to both civil and criminal sanctions pursuant to applicable Federal statutes. The state agency will provide its contractors and agents with copies of the Agreement, related IEAs, and all related attachments before initial disclosure of SSA data to such contractors and agents. Prior to signing the Agreement, and thereafter at SSA's request, the state agency will obtain from its contractors and agents a current list of the employees of such contractors and agents with access to SSA information and provide such lists to SSA.

Contractors of the state agency must adhere to the same security requirements as employees of the state agency. The state agency is responsible for the oversight of its contractors and the contractor's compliance with SSA's security requirements. The state agency must enter into a written agreement with each of its contractors and agents who need SSA information to perform their official duties. Such contractors or agents agree to abide by all relevant Federal laws, restrictions on access, use, disclosure, and the security requirements contained within the state agency's agreement with SSA.

The state agency must provide proof of the contractual agreement with all contractors and agents who encounter SSA-provided information as part of their duties. If the contractor processes, handles, or transmits information provided to the state agency by SSA or has authority to perform on the state agency's behalf, the state agency should clearly state the specific roles and functions of the contractor within the agreement. The state agency will provide SSA written certification that the contractor is meeting the terms of the agreement, including SSA security requirements. The service level agreements with the contractors and agents must contain non-disclosure language as it pertains to SSA-provided information.

The state agency must also require that contractors and agents who will process, handle, or transmit information provided to the state agency by SSA to include language in their signed agreement that obligates the contractor to follow the terms of the state agency's information exchange agreement with SSA. The state agency must also make certain that the contractor and agent's employees receive the same security awareness training as the state agency's employees. The state agency, the contractor, and the agent should maintain awareness-training records for their employees and require the same mandatory annual certification procedures.

SSA requires the state agency to subject the contractor to ongoing security compliance

reviews that must meet SSA standards. The state agency will conduct compliance reviews at least triennially commencing no later than three (3) years after the approved initial security certification to SSA. The state agencies will provide SSA with documentation of their recurring compliance reviews of their contractors and agents. The state agencies will provide the documentation to SSA during their scheduled compliance and certification reviews or upon SSA's request.

If the state agency's contractor will be involved with the processing, handling, or transmission of information provided to the EIEP by SSA offsite from the EIEP, the EIEP must have the contractual option to perform onsite reviews of that offsite facility to ensure that the following meet SSA's requirements:

a) safeguards for sensitive information,
b) computer system safeguards
c) security controls and measures to prevent, detect, and resolve unauthorized access to, use of, and disclosure of SSA-provided information, and
d) continuous monitoring of the EIEP contractors or agent's network infrastructures and assets.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.12 Cloud Service Providers (CSP) for Electronic Information Exchange Partners

(NIST SP 800-144, NIST SP 800-145, NIST SP 800-146, OMB Memo M-14-03, NIST SP 800-137)

(top)

The National Institute of Standards and Technology (NIST) Special Publication (SP) 800-145 defines Cloud Computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models." The three service models, as defined by NIST SP 800-145 are Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS). The Deployment models are Private Cloud, Community Cloud, Public Cloud, and Hybrid Cloud. Furthermore, The Federal Risk and Authorization Program (FedRAMP) is a risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

SSA requires the State Agency, contractor(s), and agent(s) to exercise due diligence to avoid hindering legal actions, warrants, subpoenas, court actions, court judgments, state or Federal investigations, and SSA special inquiries for matters pertaining to SSA-provided information.

SSA requires the State Agency, contractor(s), and agent(s) to agree that any state-owned or subcontracted facility involved in the receipt, processing, storage, or disposal of SSA-provided information operate as a "de facto" extension of the State Agency and is subject to onsite inspection and review by the State Agency or SSA with prior notice.

SSA requires that the State Agency thoroughly describe all specific contractual obligations of each party to the Cloud Service Provider (CSP) agreement between the state agency and the CSP vendor(s). If the obligations, services, or conditions widely differ from agency to agency, SSA requires separate SEQ Questionnaires to address the CSP services provided to each state agency involved in the receipt, processing, storage, or disposal of SSA-provided information.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)

5.13 Physical Security Requirements for Data Centers Holding SSA Data

(The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347), and Physical Access Controls (PE-3) Family, NIST SP 800-53 rev. 4)

(top)

SSA requires the State Agency to develop, document, and disseminate a physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, and coordination with SSA compliance. The State Agency also must develop, document, and procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls. SSA requires the State agency to review and updated these policies and procedures annually.

The State Agency must develop approve, and maintain a list of individuals with authorized access to the facility where the information system resides. The State Agency must issue authorization credentials such as badges, ID cards, etc. for facility access. The State Agency's management will review the access list detailing authorized facility access by individuals regularly (as defined by the policy or the frequency of these reviews should be relative to the level of sensitivity of the systems and the risk involved). The State Agency will remove individuals from the facility access list when access is no longer required (as defined by the policy). The State Agency will require two forms of identification from PIV cards, driver's licenses, or other form of government photo identification for visitor access to the facility where the information system resides. The State Agency will prevent or restrict unescorted access to the facility where the information system resides with persons who possess appropriate credentials.

The State Agency will develop, approve, and maintain a list of individuals with authorized access to the facility where the information system resides by:

1. Verifying individual access authorizations before granting access to the facility.
2. Controlling ingress/egress to the facility using organization-defined physical access control systems/devices; guards.
3. Maintaining physical access audit logs for entry/exit points.
4. Providing security safeguards to control access to areas within the facility officially designated as publicly accessible.
5. Escorting visitors and monitors visitor activity.
6. Securing keys, combinations, and other physical access devices
7. Inventorying by physical access device on a frequent basis (as defined by the policy or the frequency of these reviews should be relative to the level of sensitivity of the systems and the risk involved).
8. Changing combinations and keys and/or when keys are lost, combinations are

compromised, or individuals are transferred or terminated.

9. Performing security checks at the physical boundary of the facility or information system for unauthorized exfiltration of information or removal of information system components
10. Employing guards and/or alarms to monitor every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.
11. Using lockable physical casings to protect information system components from unauthorized physical access.

The State Agency will control physical access to system distribution and transmission lines within organizational facilities using safeguards (e.g., locked wiring closets, disconnected or locked spare jacks, protection by conduit or cable trays).

The State Agency will control physical access to information system output devices (e.g., Monitors, printers, copiers, scanners, fax machines, and audio devices) to prevent unauthorized individuals from obtaining the output.

The State Agency will monitor physical access to the facility where the information system resides to detect and respond to physical security incidents (e.g., accesses outside of normal work hours, repeated accesses to areas not normally accessed, accesses for unusual lengths of time, out-of-sequence accesses).

The State Agency will regularly review physical access logs (as defined by the policy or the frequency of these reviews should be relative to the level of sensitivity of the systems and the risk involved).

The State Agency must ensure the results of the reviews and investigations are vetted through the organizational incident response capability.

The State Agency will monitor physical intrusion alarms and surveillance equipment and will employ video surveillance of operational areas and retain video recordings for a predefined retention period(as defined by the policy or the frequency of these reviews should be relative to the level of sensitivity of the systems and the risk involved).

The State Agency will maintain visitor access records to the facility where the information system resides for predefined retention period (as defined by the policy or the frequency of these reviews should be relative to the level of sensitivity of the systems and the risk involved).

The State Agency will review visitor access records periodically (as defined by the

policy or the frequency of these reviews should be relative to the level of sensitivity of the systems and the risk involved).

The data center must have a process it follows in order to authorize, monitor, and control information system components entering and exiting the facility and maintains records of those items.

The data center must maintain the same or similar security controls if it allows for any alternate work sites. The State Agency data center management must assess as feasible, the effectiveness of the security controls at alternative work sites regularly (as defined by the policy or the frequency of these reviews should be relative to the level of sensitivity of the systems and the risk involved). If alternate work sites are allowed, employees must have a means to communicate with information security personnel in case of security incidents or problems, as is the case at the main work site, the data center itself.

6. Security Certification and Compliance Review Programs

(NIST SP 800-18 – System Security Plans and Planning (PL) Family, NIST SP 800-53 rev. 4)

(top)

SSA's security certification and compliance review programs are distinct processes. The certification program is a unique episodic process when an EIEP initially requests electronic access to SSA-provided information or makes substantive changes to existing exchange protocol, delivery method, infrastructure, or platform. The certification process entails two stages (refer to 6.1 for details) intended to ensure that management, operational, and technical security measures work as designed. SSA must ensure that the EIEPs fully conform to SSA's security requirements at the time of certification and satisfy both stages of the certification process before SSA will permit online access to its data in a production environment.

The compliance review program entails cyclical security review of the EIEP performed by, or on behalf of SSA. The purpose of the review is to assess an EIEP's conformance to SSA's current security requirements at the time of the review engagement. The compliance review program applies to both online and batch access to SSA-provided information. Under the compliance review program, EIEPs are subject to ongoing and periodic security reviews by SSA.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY.)

6.1 The Security Certification Program

(NIST SP 800-18 – System Security Plans, Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)

(top)

The security certification process applies to EIEPs that seek online electronic access to SSA-provide information and consists of two general phases:

a) **Phase 1:** The Security Evaluation Questionnaire (SEQ) is a formal written plan authored by the EIEP to document its management, operational, and technical security controls to safeguard SSA-provided information (refer to ***Documenting Security Controls in the Security Design Plan***.

NOTE: SSA may have legacy EIEPs (EIEPs not certified under the current process) who have not prepared an SEQ. SSA strongly recommends that these EIEPs prepare an SEQ.

The EIEP's preparation and maintenance of a current SEQ will aid them in determining potential compliance issues prior to reviews, assuring continued compliance with SSA's TSSRs, and providing for more efficient security reviews.

b) **Phase 2:** The SSA Onsite Certification is a formal security review conducted by SSA, or on its behalf, to examine the full suite of management, operational, and technical security controls implemented by the EIEP to safeguard data obtained from SSA electronically (refer to ***The Certification Process***.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY.)

6.2 Documenting Security Controls in the SEQ

(NIST SP 800-18 – System Security Plans, Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)

(top)

6.2.1 When an SEQ is required:

(top)

EIEPs must submit an SEQ when one or more of the following circumstances apply:

a) to obtain approval for requested access to SSA-provided information for an initial agreement,
b) to obtain approval to reestablish previously terminated access to SSA-provided information,
c) to obtain approval to implement a new operating or security platform that will involve SSA-provided information,
d) to obtain approval for significant changes to the EIEP's organizational structure, technical processes, operational environment, or security implementations planned or made since approval of their most recent SEQ or of their most recent successfully completed security review,
e) to confirm compliance when one or more security breaches or incidents involving SSA-provided information occurred since approval of the EIEP's most recent SEQ or of their most recent successfully completed security review,
f) to document descriptions and explanations of measures implemented as the result of a data breach or security incident,
g) to document descriptions and explanations of measures implemented to resolve non-compliancy issue(s), and
h) to obtain a new approval after SSA revoked approval of the most recent SEQ.

SSA may require a new SEQ if changes occurred (other than those listed above) that may affect the terms of the EIEP's data exchange agreement with SSA.

SSA will not approve the SEQ or allow the initiation of transactions and/or access to SSA-provided information before the EIEP complies with the TSSRs.

NOTE: EIEPs that function only as an STC, transferring SSA-provided information to other EIEPs must, per the terms of their agreements with SSA, adhere to SSA's TSSR and exercise their responsibilities regarding protection of SSA-provided information.
(See Page 48 Definition of STC.)

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY.)

6.3 The Certification Process

(NIST SP 800-18 – System Security Plans, Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)

(top)

Once the EIEP has successfully satisfied Phase 1, SSA will conduct an onsite certification review. The objective of the onsite review is to ensure the EIEP's management, operational, and technical controls safeguarding SSA-provided information from misuse and improper disclosure, and that those safeguards function and work as intended.

At its discretion, SSA may request the EIEP to participate in an onsite review and compliance certification of their security infrastructure.

The onsite review may address any or all of SSA's security requirements and include, when appropriate:

1) a demonstration of the EIEP's implementation of each security requirement,

2) a physical review of pertinent supporting documentation to verify the accuracy of responses in the SEQ,

3) a demonstration of the functionality of the software interface for the system that will receive, process, and store SSA-provided information,

4) a demonstration of the Automated Audit Trail System (ATS),

5) a walkthrough of the EIEP's data center to observe and document physical security safeguards,

6) a demonstration of the EIEP's implementation of electronic exchange of data with SSA,

7) a discussion with managers, supervisors, information security officers, system administrators, or other state stakeholders,

8) an examination of management control procedures and reports pertaining to anomaly detection or anomaly prevention,

9) a demonstration of technical tools pertaining to user access control and, if appropriate, browsing prevention,

10) a demonstration of the permission module or similar design, to show how the system triggers requests for information from SSA, and

11) a demonstration of how data requests for SSA-provided information are filtered by the EIEP's system to prevent requests to SSA if the SSN is not present in the EIEP's system.

SSA may attempt to obtain information from the State Agency using at least one, randomly created, fictitious number not known to the EIEPs system.

During a certification, compliance review, or recertification (and re-authorization), SSA, or a certifier acting on its behalf, may request a demonstration of the EIEP's ATS and its record retrieval capability. SSA or a certifier may request a demonstration of the ATS' capability to track the activity of employees who have the potential to access SSA-provided information within the EIEP's system. The certifier may request more information from those EIEPs who use an STC to handle and audit transactions. SSA or a certifier may conduct a demonstration to see how the EIEP obtains audit information from the STC regarding the EIEP's SSA transactions.

If an STC handles and audits an EIEP's transactions, SSA requires the EIEP to demonstrate both their in-house audit capabilities and the process used to obtain audit information from the STC.

If the EIEP employs a contractor or agent who processes, handles, or transmits the EIEP's SSA-provided information offsite, SSA, at its discretion, may request to include the contractor's facility in the onsite certification review. The inspection may occur with or without a representative of the EIEP.

Upon successful completion of the onsite certification review, SSA will authorize electronic access to production data by the EIEP. SSA will provide written notification of its certification to the EIEP and all appropriate internal SSA components.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY.)

6.4 The Compliance Review Program and Process

(NIST SP 800-18 – System Security Plans, Configuration Management (CM), Security Assessment and Authorization Controls (CA), and Planning (PL) Families, NIST SP 800-53 rev. 4)

(top)

Similar to the certification process, the compliance review program entails a process intended to ensure that EIEPs that receive electronic information from SSA are in full compliance with the SSA's TSSRs. SSA requires EIEPs to complete and submit (based on a timeline agreed upon by SSA and EIEP's stakeholders) a Security Evaluation Questionnaire (SEQ). The SEQ describes the EIEP's management, operational, and technical controls used to protect SSA-provided information from misuse and improper disclosure. SSA also requires the ability to verify that those safeguards function and work as intended.

As a practice, SSA attempts to conduct compliance reviews following a 3 to 5 year periodic review schedule. However, as circumstances warrant, a review may take place at any time. Three prominent examples that would trigger an ad hoc review are:

a) a significant change in the outside EIEP's computing platform,
b) a violation of any of SSA's TSSRs, or
c) an unauthorized disclosure of SSA-provided information by the EIEP.

SSA may conduct onsite compliance reviews and include both the EIEP's main facility and a field office.

SSA may, at its discretion, request that the EIEP participate in an onsite compliance review of their security infrastructure to confirm the implementation of SSA's security requirements.

The onsite review may address any or all of SSA's security requirements and include, where appropriate:

a) a demonstration of the EIEP's implementation of each requirement
b) a random sampling of audit records and transactions submitted to SSA
c) a walkthrough of the EIEP's data center to observe and document physical security safeguards
d) a demonstration of the EIEP's implementation of online exchange of data with SSA,
e) a discussion with managers, supervisors, information security officers, system administrators, or other state stakeholders,
f) an examination of management control procedures and reports pertaining to anomaly detection and prevention reports,
g) a demonstration of technical tools pertaining to user access control and, if appropriate, browsing prevention,

h) a demonstration of how a permission module or similar design triggers requests for information from SSA, and
i) a demonstration of how a permission module prevents the EIEP's system from processing SSNs not present in the EIEP's system.

SSA can accomplish this by attempting to obtain information from State Agencies using at least one, randomly created, fictitious number not known to the EIEP's system.

SSA may perform an onsite or remote review for reasons including, but not limited, to the following:

a) the EIEP has experienced a security breach or incident involving SSA-provided information,

b) the EIEP has unresolved non-compliancy issue(s),

c) to review an offsite contractor's facility that processes SSA-provided information,

d) the EIEP is a legacy organization that has not yet been through SSAs security certification and compliance review programs, and

e) the EIEP requested that SSA perform an IV & V (Independent Verification and Validation review).

During the compliance review, SSA, or a certifier acting on its behalf, may request a demonstration of the system's audit trail and retrieval capability. The certifier may request a demonstration of the system's capability for tracking the activity of employees who view SSA-provided information within the EIEP's system. The certifier may request EIEPs that have STCs that handle and audit transactions with SSA to demonstrate the process used to obtain audit information from the STC.

If an STC handles and audits the EIEP's transactions with SSA, we may require the EIEP to demonstrate both their in-house audit capabilities and the processes used to obtain audit information from the STC regarding the EIEP's transactions with SSA.

If the EIEP employs a contractor who will process, handle, or transmit the EIEP's SSA-provided information offsite, SSA, at its discretion, may request to include in the onsite compliance review an onsite inspection of the contractor's facility. The inspection may occur with or without a representative of the EIEP. The format of the review in routine circumstances (e.g., the compliance review is not being conducted to address a special circumstance, such as a disclosure violation, etc.) will generally consist of reviewing and updating the EIEP's compliance with the systems security requirements described above in this document. At the conclusion of the review, SSA will issue a formal report to appropriate EIEP personnel. The Compliance Report will address findings and recommendations from SSA's compliance review, which includes a plan for monitoring each issue until closure.

NOTE: SSA will never request documentation for compliance reviews unless necessary to assess the EIEP's security posture. The information is only accessible to authorized individuals who have a need for the information as it relates to the EIEP's compliance with its electronic data exchange agreement with SSA and the associated system security requirements and procedures. SSA will not retain the EIEP's documentation any longer than required. SSA will delete, purge, or destroy the documentation when the retention requirement expires.

Compliance Reviews are either on-site or remote reviews. High-risk reviews must be onsite reviews, medium risk reviews are usually onsite, and low risk reviews may qualify for a remote review via telephone. The past performance of the entire state determines whether a review is onsite or remote **SSA determines a state's risk level based on the "high water mark principle."** If one agency is high risk, the entire state is high risk. The following is a high-level example of the analysis that aids SSA in making a preliminary determination as to which review format is appropriate. SSA may also use additional factors to determine whether SSA will perform an onsite or remote compliance review.

A. High/Medium Risk Criteria

1) undocumented closing of prior review finding(s),
2) implementation of management, operational or technical controls that affect security of SSA-provided information (e.g. implementation of new data access method), or
3) a reported PII breach within the state.

B. Low Risk Criteria

1) no prior review finding(s) or prior finding(s) documented as closed.
2) no implementation of technical/operational controls that impact security of SSA provided information (e.g. implementation of new data access method), and
3) no reported PII breach.

6.4.1 EIEP Compliance Review Participation

(top)

SSA may request to meet with the following stakeholders during the compliance review:

a) a sample of managers, supervisors, information security officers, system administrators, etc. responsible for enforcing and monitoring ongoing compliance to security requirements and procedures to assess their level of training to monitor their employee's use of SSA-provided information, and for reviewing reports and taking necessary action

b) the individuals responsible for performing security awareness and employee sanction functions to learn how EIEPs fulfill this requirement

c) a sample of the EIEP's employees to assess their level of training and understanding of the requirements and potential sanctions applicable to the use and misuse of SSA-provided information

d) the individual(s) responsible for management oversight and quality assurance functions to confirm how the EIEP accomplishes this requirement

e) any additional individuals as deemed appropriate by SSA (i.e. analysts, Project/Program Manager, claims reps, etc.)

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY.)

6.5 Scheduling the Onsite Review

(top)

SSA will not schedule the onsite review until SSA approves the EIEP's SEQ or the EIEPs stakeholders participating in the compliance review have agreed upon a schedule. There is no prescribed period for arranging the subsequent onsite review (***certification review*** for an EIEP requesting initial access to SSA-provided information for an initial agreement or ***compliance review*** for other EIEPs). Unless there are compelling circumstances precluding it; the onsite review will occur as soon as reasonably possible.

The scheduling of the onsite review may depend on additional factors including:

a) the reason for submission of the SEQ,

b) the severity of security issues, if any,

c) circumstances of the previous review, if any, and

d) SSA's workload and resource considerations.

(THE REST OF THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY.)

7. Additional Definitions

(top)

Back Button:

Refers to a button on a web browser's toolbar, the *backspace button* on a computer keyboard, a programmed keyboard button or mouse button, etc., that returns a user to a previously visited web page or application screen.

Breach:

Refers to actual loss, loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where unauthorized persons have access or potential access to PII or Covered Information, whether physical, electronic, or in spoken word or recording

Browsing:

Requests for or queries of SSA-provided information for purposes not related to the performance of official job duties

Choke Point:

The firewall between a local network and the Internet is a choke point in network security, because any attacker would have to come through that channel, which is typically protected and monitored.

Cloud Computing:

The term refers to Internet-based computing derived from the cloud drawing representing the Internet in computer network diagrams. Cloud computing providers deliver on-line and on-demand Internet services. Cloud Services normally use a browser or Web Server to deliver and store information.

Cloud Computing (NIST SP 800-145 Excerpt):

Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.

Essential Characteristics:

On-demand self-service - A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access - Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling - The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (e.g., country, state, or datacenter). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity - Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service - Cloud systems automatically control and optimize resource use by leveraging a metering capability1 at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

Service Models:

Software as a Service (SaaS) - The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure2. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS) - The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.3 The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS) - The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Deployment Models:

Private cloud - The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers (e.g., business units). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud - The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud - The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud - The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

_____

1 Typically this is done on a pay-per-use or charge-per-use basis.

2 A cloud infrastructure is the collection of hardware and software that enables the five essential characteristics of cloud computing. The cloud infrastructure can be viewed as containing both a physical layer and an abstraction layer. The physical layer consists of the hardware resources that are necessary to support the cloud services being provided, and typically includes server, storage and network components. The abstraction layer consists of the software deployed across the physical layer, which manifests the essential cloud characteristics. Conceptually the abstraction layer sits above the physical layer.

3 This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.

Cloud Drive:

A cloud drive is a Web-based service that provides storage space on a remote server.

Cloud Audit:

Cloud Audit is a specification developed at Cisco Systems, Inc. that provides cloud computing service providers a standard way to present and share detailed, automated statistics about performance and security.

Commingling:

Commingling is the creation of a common database or repository that stores and maintains both SSA-provided information and preexisting EIEP PII.

Data Exchange:

Data Exchange is a logical transfer of information from one government entity's systems of records (SOR) to another agency's application or mainframe through a secure and exclusive connection.

Degaussing:

Degaussing is the method of using a "special device" (i.e., a device that generates a magnetic field) in order to disrupt magnetically recorded information. Degaussing can be effective for purging damaged media and media with exceptionally large storage capacities. Degaussing is not effective for purging non-magnetic media (e.g., optical discs).

The Federal Risk and Authorization Program (FedRAMP):
FedRAMP is a risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.

Function:
One or more persons or organizational components assigned to serve a particular purpose, or perform a particular role. The purpose, activity, or role assigned to one or more persons or organizational components.

Hub:
As it relates to electronic data exchange with SSA, a hub is an organization, which serves as an electronic information conduit or distribution collection point. The term Hub is interchangeable with the terms "StateTransmission Component," "State Transfer Component," or "STC."

ICON:
Interstate Connection Network (various entities use 'Connectivity' rather than 'Connection')

IV&V:
Independent Verification and Validation

Legacy System:
A term usually referring to a corporate or organizational computer system or network that utilizes outmoded programming languages, software, and/or hardware that typically no longer receives support from the original vendors or developers.

Manual Transaction:

A user-initiated operation (also referred to as a "user-initiated transaction"). This is the opposite of a system-generated automated process.

Example: A user enters a client's information including the client's SSN and presses the "ENTER" key to acknowledge that input of data is complete. A new screen appears with multiple options, which include "VERIFY SSN" and "CONTINUE". The user has the option to verify the client's SSN or perform alternative actions.

Media Sanitization:

a) Disposal: Refers to the discarding (e.g., recycling) media that contains no sensitive or confidential data.

b) Overwriting/Clearing: This type of media sanitization is adequate for protecting information from a robust keyboard attack. Clearing must prevent retrieval of information by data, disk, or file recovery utilities. Clearing must be resistant to keystroke recovery attempts executed from standard input devices and from data

scavenging tools. For example, overwriting is an acceptable method for clearing media. Deleting items, however, is not sufficient for clearing.

This process may include overwriting all addressable locations of the data, as well as its logical storage location (e.g., its file allocation table). The aim of the overwriting process is to replace or obfuscate existing information with random data. Most rewriteable media may be cleared by a single overwrite. This method of sanitization is not possible on un-writeable or damaged media.

c) Purging: This type of media sanitization is a process that protects information from a laboratory attack. The terms *clearing* and *purging* are sometimes synonymous. However, for some media, clearing is not sufficient for purging (i.e., protecting data from a laboratory attack). Although most re-writeable media requires a single overwrite, purging may require multiple rewrites using different characters for each write cycle.

This is because a laboratory attack involves threats with the capability to employ non-standard assets (e.g., specialized hardware) to attempt data recovery on media outside of that media's normal operating environment.

d) Degaussing is also an example of an acceptable method for purging magnetic media. The EIEP should destroy media if purging is not a viable method for sanitization.

e) Destruction: Physical destruction of media is the most effective form of sanitization. Methods of destruction include burning, pulverizing, and shredding. Any residual medium should be able to withstand a laboratory attack.

Permission Module:

A utility or subprogram within an application, which automatically enforces the relationship of a request for or query of SSA-provided information to an authorized process or transaction before initiating a transaction. The System will not allow a user to request information from SSA unless the EIEP's client system contains a record of the subject individual's SSN. A properly configured Permission Module also enforces referential integrity and prevents unauthorized random browsing of PII.

Screen Scraping:

Screen scraping is normally associated with the programmatic collection of visual data from a source. Originally, screen scraping referred to the practice of reading text data from a computer display terminal's screen. This involves reading the terminal's memory through its auxiliary port, or by connecting the terminal output port of one computer system to an input port on another. The term screen scraping is synonymous with the term bidirectional exchange of data.

A screen scraper might connect to a legacy system via Telnet, emulate the keystrokes needed to navigate the legacy user interface, process the resulting display output, extract the desired data, and pass it on to a modern system.

More modern screen scraping techniques include capturing the bitmap data from a screen and running it through an optical character reader engine, or in the case of graphical user interface applications, querying the graphical controls by programmatically obtaining references to their underlying programming objects.

Security Breach:

An act from outside an organization that bypasses or violates security policies, practices, or procedures.

Security Incident:

A security incident happens when a fact or event signifies the possibility that a breach of security may be taking place, or may have taken place. All threats are security incidents, but not all security incidents are threats**.**

Security Violation:

An act from within an organization that bypasses or disobeys security policies, practices, or procedures.

Sensitive Data:

Sensitive data is a special category of personally identifiable information (PII) that has the potential to cause great harm to an individual, government agency, or program if abused, misused, or breached. It is sensitive information protected against unwarranted disclosure and carries specific criminal and civil penalties for an individual convicted of unauthorized access, disclosure, or misuse. Protection of sensitive information usually involves specific classification or legal precedents that provide special protection for legal and ethical reasons.

Security Information Management (SIM):

SIM is software that automates the collection of event log data from security devices such as firewalls, proxy servers, intrusion detection systems and anti-virus software. The SIM translates the data into correlated and simplified formats.

SMDS (Switched Multimegabit Data Service (SMDS):

SMDS is a telecommunications service that provides connectionless, high-performance, packet- switched data transport. Although not a protocol, it supports standard protocols and communications interfaces using current technology.

SSA-provided Data/Information:

Synonymous with "SSA-supplied data/information", defines information under the

control of SSA provided to an external entity under the terms of an information exchange agreement with SSA. The following are examples of SSA-provided data/information:

a) SSA's response to a request from an EIEP for information from SSA (e.g., date of death)

b) SSA's response to a query from an EIEP for verification of an SSN

SSA Data/Information:

This term, sometimes used interchangeably with "SSA-provided data/information," denotes information under the control of SSA provided to an external entity under the terms of an information exchange agreement with SSA. However, **"SSA data/information"** also includes information provided to the EIEP by a source other than SSA, but which the EIEP attests to that SSA verified it, or the EIEP couples the information with data from SSA as to certify the accuracy of the information. The following are examples of SSA information:

a) SSA's response to a request from an EIEP for information from SSA (e.g., date of death)

b) SSA's response to a query from an EIEP for verification of an SSN

c) Display by the EIEP of SSA's response to a query for verification of an SSN ***and*** the associated SSN provided by SSA

d) Display by the EIEP of SSA's response to a query for verification of an SSN ***and*** the associated SSN provided to the EIEP by a source other than SSA

e) Electronic records that contain only SSA's response to a query for verification of an SSN ***and*** the associated SSN whether provided to the EIEP by SSA or a source other than SSA

SSN:

Social Security Number

STC:

A State Transmission/Transfer Component is an organization, which performs as an electronic information conduit or collection point for one or more other entities (also referred to as a hub).

System-Generated Transaction:

A transaction automatically triggered by an automated system process.

Example: A user enters a client's information including the client's SSN on an input screen and presses the "ENTER" key to acknowledge that input of data is complete. An automated process then matches the SSN against the organization's database and when the systems finds no match, automatically sends an electronic request for verification of

the SSN to SSA.

Systems Process:

Systems Process refers to a software program module that runs in the background within an automated batch, online, or other process.

Third Party:

Third Party pertains to an entity (person or organization) provided access to SSA-provided information by an EIEP or other SSA business partner for which one or more of the following apply:

a) is not stipulated access to SSA-provided information by an information-sharing agreement between an EIEP and SSA
b) has no data exchange agreement with SSA
c) SSA does not directly authorize access to SSA-provided information

Transaction-Driven:

This term pertains to an automatically initiated online query of or request for SSA information by an automated transaction process (e.g., driver license issuance, etc.). The query or request will only occur the automated process meets prescribed conditions.

Uncontrolled Transaction:

This term pertains to a transaction that falls outside a permission module. An uncontrolled transaction is not subject to a systematically enforced relationship between an authorized process or application and an existing client record.

8. Regulatory References

(top)

- Federal Information Processing Standards (FIPS) Publications
- Federal Information Security Management Act of 2002 (FISMA)
- Homeland Security Presidential Directive (HSPD-12)
- National Institute of Standards and Technology (NIST) Special Publications (SPs)
- Office of Management and Budget (OMB) Circular A-123, *Management's Responsibility for Internal Control*
- Office of Management and Budget (OMB) Circular A-130, Appendix III, *Management of Federal Information Resources*
- Office of Management and Budget (OMB) Memo M-06-16, *Protection of Sensitive Agency Information, June 23, 2006*
- Office of Management and Budget (OMB) Memo M-07-16, *Memorandum for the Heads of Executive Departments and Agencies May 22, 2007*
- Office of Management and Budget (OMB) Memo M-07-17, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007*
- Privacy Act of 1974, as amended

9. Frequently Asked Questions

(top)

(Click links for answers or additional information)

1. Q: What is a breach of data?
   A: Refer to Security Breach, Security Incident, and Security Violation.

2. Q: What is employee browsing?
   A: Requests for or queries of SSA-provided information for purposes not related to the performance of official job duties

3. Q: Okay, so the EIEP submitted the SEQ. Can SSA schedule the Onsite Review?
   A: Refer to Scheduling the Onsite Review.

4. Q: What is a **"Permission Module**?"
   A: A utility or subprogram within an application, which automatically enforces the relationship of a request for or query of SSA-provided information to an authorized process or transaction before initiating a transaction. For example, if requests for verification of an SSN for issuance of a driver's license happens automatically from within a state driver's license application. The System will not allow a user to request information from SSA unless the EIEP's client system contains a record of the subject individual's SSN.

5. Q: What is **"Screen Scraping**?"
   A: Screen scraping is normally associated with the programmatic collection of visual data from a source. Originally, screen scraping referred to the practice of reading text data from a computer display terminal's screen. This involves reading the terminal's memory through its auxiliary port, or by connecting the terminal output port of one computer system to an input port on another. The term screen scraping is synonymous with the term bidirectional exchange of data.

   A screen scraper might connect to a legacy system via Telnet, emulate the keystrokes needed to navigate the legacy user interface, process the resulting display output, extract the desired data, and pass it on to a modern system.

   More modern screen scraping techniques include capturing the bitmap data from a screen and running it through an optical character reader engine, or in the case of graphical user interface applications, querying the graphical controls by programmatically obtaining references to their underlying programming objects.

6. Q: When does an EIEP have to submit an SEQ?
   A: Refer to When the SEQ is Required.

7. Q: Does an EIEP have to submit an SEQ when the agreement is renewed?
A: The EIEP does not have to submit an SEQ ***because*** the agreement between the EIEP and SSA was renewed. There are, however, circumstances that require an EIEP to submit an SEQ.
Refer to When the SEQ is Required.

8. Q: Is it acceptable to save SSA-provided information with a verified indicator on a (EIEP) workstation if the EIEP uses an encrypted hard drive? If not, what options does the agency have?
A: There is no problem with an EIEP saving SSA-provided information on the encrypted hard drives of computers used to process SSA-provided information if the EIEP retains the information only as provided for in the EIEP's data-sharing agreement with SSA.
Refer to Data and Communications Security.

9. Q: Does SSA allow EIEPs to use caching of SSA-provided information on the EIEP's workstations?
A: Caching during processing is not a problem. However, SSA-provided information must clear from the cache when the user exits the application.
Refer to Data and Communications Security.

10. Q: What does the term "interconnections to other systems" mean?
A: As used in SSA's system security requirements document, the term "interconnections" is the same as the term "connections."

11. Q: Is it acceptable to submit the SEQ as a .PDF file?
A: No, it is not. The document must remain editable.

12. Q: Should the EIEP write the SEQ from the standpoint of the EIEP SVES (or applicable data element) access itself, or from the standpoint of access to all data provided to the EIEP by SSA?
A: The SEQ is to encompass the EIEP's entire electronic access to SSA-provided information as per the electronic data exchange agreement between the EIEP and SSA.
Refer to Developing the SEQ.

13. Q: If the EIEP has a "transaction-driven" system, does the EIEP still need a permission module? If employees cannot initiate a query to SSA, why would the EIEP need the permission module?
A: "Transaction driven" means that queries submit requests automatically (and it might depend on the transaction). Depending on the system's design, queries might not be automatic or it may still permit manual transactions. A system may require manual transactions to correct an error. SSA does not prohibit manual transactions if an ATS properly tracks such transactions. If a "transaction-driven" system permits any type of alternate access, it still requires a permission module, even if it restricts users from

performing manual transactions. If the system does ***not*** require the user to be in a particular application and/or the query to be for an existing record in the EIEP's system ***before*** the system will allow a query to go through to SSA, it would still need a permission module.

14. Q: What is an Onsite Compliance Review?
A: The Onsite Compliance Review is SSA's periodic site visits to its Electronic Information Exchange Partners (EIEP) to certify whether the EIEP's management, operational, and technical security measures for protecting data obtained electronically from SSA continue to conform to the terms of the EIEP's data sharing agreements with SSA and SSA's associated system security requirements and procedures.
Refer to the Compliance Review Program and Process.

15. Q: What are the criteria for performing an Onsite Compliance Review?
A: The following are criteria for performing the Onsite Compliance Review:

- EIEP initiating new access or new access method for obtaining information from SSA
- EIEP's cyclical review (previous review was performed remotely)
- EIEP has made significant change(s) in its operating or security platform involving SSA-provided information
- EIEP experienced a breach of SSA-provided personally identifying information (PII)
- EIEP has been determined to be high-risk

16. Q: What is a Remote Compliance Review?
A: The Remote Compliance Review is when SSA conducts the meetings remotely (e.g., via conference calls). SSA schedules conference calls with its EIEPs to determine whether the EIEPs technical, managerial, and operational security measures for protecting data obtained electronically from SSA continue to conform to the terms of the EIEP's data sharing agreements with SSA and SSA"s associated system security requirements and procedures.
Refer to the Compliance Review Program and Process.

17. Q: What are the criteria for performing a Remote Compliance Review?
A: The EIEP must satisfy the following criteria to qualify for a Remote Compliance Review:

- EIEP's cyclical review (SSA's previous review yielded no findings or the EIEP satisfactorily resolved cited findings)
- EIEP has made no significant change(s) in its operating or security platform involving SSA-provided information
- EIEP has not experienced a breach of SSA-provided personally identifying information (PII) since its previous compliance review.

- SSA rates the EIEP as a low-risk agency or state