SENSITIVE DOCUMENT

# ATTACHMENT 4

# ELECTRONIC INFORMATION EXCHANGE SECURITY REQUIREMENTS AND PROCEDURES


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

**SENSITIVE DOCUMENT**

**VERSION 6.0.2**
**April 2014**

## Table of Contents

**RECEIVING ELECTRONIC INFORMATION FROM THE SOCIAL SECURITY ADMINISTRATION**

## 1. Introduction

The law requires the Social Security Administration (SSA) to maintain oversight and assure the protection of information it provides to its *Electronic Information Exchange Partners* (EIEP). EIEPs are entities that have information exchange agreements with SSA.

The overall aim of this document is twofold. First, to ensure that SSA can properly certify EIEPs as compliant by the SSA security requirements, standards, and procedures expressed in this document before we grant access to SSA information in a production environment. Second, to ensure that EIEPs continue to adequately safeguard electronic information provided to them by SSA.

This document (which SSA considers SENSITIVE[1] and should only be shared with those who need it to ensure SSA-provided information is safeguarded), describes the security requirements, standards, and procedures EIEPs must meet and implement to obtain information from SSA electronically. This document helps EIEPs understand criteria that SSA uses when evaluating and certifying the system design and security features used for electronic access to SSA-provided information.

The addition, elimination, and modification of security control factors determine which level of security and due diligence SSA requires for the EIEP to mitigate risks. The emergence of new threats, attack methods, and the availability of new technology warrants frequent reviews and revisions to our System Security Requirements (SSR). Consequently, EIEPs should expect SSA's System Security Requirements to evolve in concert with the industry.

EIEPs must comply with SSA's most current SSRs to gain access to SSA-provided data. SSA will work with its partners to resolve deficiencies that occur subsequent to, and after, approval for access if updates to our security requirements cause an agency to be uncompliant. EIEPs may proactively ensure their ongoing compliance with the SSRs by periodically requesting the most current SSR package from their SSA contact. Making periodic adjustments is often necessary.

## 2. Electronic Information Exchange Definition

For discussion purposes herein, Electronic Information Exchange (EIE) is any electronic process in which SSA discloses information under its control to any third party for any purpose, without the specific consent of the subject individual or agent acting on his or her behalf. EIE involves individual data transactions and data files processed within the systems of parties to electronic information sharing agreements with SSA. These processes include direct terminal access or DTA to SSA systems, 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.

[1] Sensitive data - "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (The Privacy Act), but that has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy but is to be protected in accordance with the requirements of the Computer Security Act of 1987 (P.L.100-235)."

## 3. Roles and Responsibilities

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; managing SSA's fraud monitoring and reporting activities; 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 sharing agreements executed by SSA with outside entities. Within the context of SSA's security policies and the terms of electronic information sharing agreements with SSA's EIEPs, OIS exclusively conducts and brings to closure initial security certifications and periodic security compliance reviews of EIEPs that process, maintain, transmit, or store SSA-provided information in accordance with pertinent Federal requirements which include the following (see also ***Regulatory References***):

a. The **Federal Information Security Management Act (FISMA)** requires the protection of "Federal information in contractor systems, including those systems operated by state and local governments."

b. The Social Security Administration requires EIEPs to adhere to the policies, standards, procedures, and directives published in this Systems Security Requirements (SSR) document.

   Personally Identifiable Information (PII), covered under several Federal laws and statutes, is information about an individual including, but not limited to, personal identifying information including the Social Security Number (SSN).

   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.

   However, SSA is diligent in discharging its responsibility for establishing *appropriate* administrative, technical, and physical safeguards to ensure the security, confidentiality, 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.**

   The SSA Regional ***Data Exchange Coordinators*** (DECs) serve as a bridge between SSA and state EIEPs. In the security arena, DECs assist OIS in coordinating data exchange security review activities with state and local EIEPs; e.g., they provide points of contact with state agencies, assist 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 a suspected or actual loss of SSA-provided Personally Identifiable Information (PII).

## 4. General Systems Security Standards

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.***

a. 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 in conformance with SSA requirements,
- efficiently investigate fraud, data breaches, or security events that involve SSA-provided information, or
- 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 SSA's associated system security requirements and procedures.**

b. EIEPs must use the electronic connection established between the EIEP and SSA only in support of the current agreement(s) between the EIEP and SSA.

c. EIEPs must use the software and/or devices provided to the EIEP only in support of the current agreement(s) between the EIEP and SSA.

d. SSA prohibits modifying any software or devices provided to the EIEPs by SSA.

e. 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.

f. 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.***

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

h. The EIEP must process SSA-provided information under the immediate supervision and control of authorized personnel.

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

j. 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.

k. EIEPs must have an active and robust employee security awareness program, which is mandatory for all employees who access SSA-provided information.

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

m. At its discretion, SSA or its designee 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 we provide.

## 5. Systems Security Requirements

### 5.1 Overview

SSA must certify that the EIEP has implemented controls that meet the requirements and work as intended, before we will authorize initiating transactions to and from SSA through batch data exchange processes or online processes such as State Online Query (SOLQ) or Internet SOLQ (SOLQ-I).

The Technical Systems Security Requirements (TSSRs) address management, operational, and technical aspects of security safeguards to ensure only the authorized disclosure and use of SSA-provided information by SSA's EIEPs.

SSA recommends that the EIEP develop and publish a comprehensive Systems Security Policy document that specifically addresses:

- the classification of information processed and stored within the network,
- administrative controls to protect the information stored and processed within the network,
- access to the various systems and subsystems within the network,
- Security Awareness Training,
- Employee Sanctions Policy,

- Incident Response Policy, and

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

SSA's systems security requirements represent the current state-of-the-practice security controls, safeguards, and countermeasures required for Federal information systems by Federal regulations, statutes, standards, and guidelines. Additionally, SSA's systems security requirements also include 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.

## 5.2 General System Security Design and Operating Environment

EIEPs must provide descriptions and explanations of their overall system design, configuration, security features, and operational environment and include explanations of how they conform to SSA's requirements. Explanations must include the following:

- Descriptions of the operating environment(s) in which the EIEP will utilize, maintain, and transmit SSA-provided information

- Descriptions of the business process(es) in which the EIEP will use SSA-provided information

- Descriptions of the physical safeguards employed to ensure that unauthorized personnel cannot access SSA-provided information and details of how the EIEP keeps audit information pertaining to the use and access to SSA-provided information and associated applications readily available

- Descriptions of 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 (stored or not in use)

- Descriptions of 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.)

- Descriptions of how the configurations of devices (e.g., servers, workstations, and portable devices) involving SSA-provided information comply with recognized industry standards and SSA's system security requirements

- Description of how the EIEP implements adequate security controls (e.g., passwords enforcing sufficient construction strength to defeat or minimize risk-based identified vulnerabilities)

## 5.3 System Access Control

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) or a security software design which is equivalent to such products. The access control software must utilize personal identification numbers (PIN) and passwords or Biometric identifiers in combination with the user's system identification code (userID). 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).

Depending on the computing platform (e.g., client/server (PC), mainframe) and the access software implementation, the terms "PIN" and "user system identification code (userID)" may be, for practical purposes, synonymous. For example, the PIN/password combination may be required for access to an individual's PC after which, the userID/password combination may be required for access to a mainframe application. A biometric identifier may supplant one element in the pair of those combinations. **SSA strongly recommends 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 and ensure limitations for password repetition. Technical controls should enforce periodic password changes based on a risk-based standard (e.g., maximum password age of 90 days, minimum password age of 3 – 7 days) and enforce automatic disabling of user accounts that have been inactive for a specified period of time (e.g., 90 days).

The EIEP's password policies must also require more stringent password construction (e.g., passwords greater than eight characters in length requiring upper 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.

EIEPs must have management control and oversight of the function of authorizing individual user access to SSA-provided information and to oversee the process of issuing and managing access control PINs, passwords, biometric identifiers, etc. for access to the EIEP's system.

The EIEP's systems access rules must cover least privilege and individual accountability. The EIEP's rules should include procedures for access to sensitive information and transactions and functions related to it. Procedures should include control of transactions by permissions module, the assignment and limitation of system privileges, disabling accounts of separated employees (e.g., within 24 hours), individual accountability, work at home, dial-up access, and connecting to the Internet.

### 5.4 Automated Audit Trail

SSA requires EIEPs 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, 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 Audit Trail System must create transaction files to capture all input from interactive internet applications which access or query SSA-provided information.

If a State Transmission Component (STC) handles and audits the EIEP's transactions with SSA, the EIEP is responsible for ensuring that the STC's audit capabilities meet SSA's requirements for an automated audit trail system. The EIEP must also establish a process to obtain specific audit information from the STC regarding the EIEP's SSA transactions.

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 (preferably seven) years. Information in the audit file must be retrievable by an automated method. EIEPs must have the capability to make audit file information available to SSA upon request. EIEPs must back-up audit trail records on a regular basis to ensure their availability. EIEPs must apply the same level of protection to backup audit files that apply to the original files.

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 indicate to users that SSA verified the information, the EIEP's system must also capture an audit trail record of users who viewed 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.

### 5.5 Personally Identifiable Information (PII)

***PII*** is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. 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 a circumstance when SSA has reason to believe that information on hard copy or in electronic format, which contains PII provided by SSA, left the EIEP's custody or the EIEP disclosed it to an unauthorized individual or entity. PII loss is a reportable incident (refer to ***Incident Reporting***).

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***).

## 5.6 Monitoring and Anomaly Detection

**SSA recommends that 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 the following:

- The EIEP's security controls continue to be effective over time
- Only authorized individuals, devices, and processes have access to SSA-provided information
- The EIEP detects efforts by external and internal entities, devices, or processes to perform unauthorized actions (i.e., data breaches, malicious attacks, access to network assets, software/hardware installations, etc.) as soon as they occur
- The necessary parties are immediately alerted to unauthorized actions performed by external and internal entities, devices, or processes
- Upon detection of unauthorized actions, measures are immediately initiated to prevent or mitigate associated risk
- In the event of a data breach or security incident, the EIEP can efficiently determine and initiate necessary remedial actions
- The trends, patterns, or anomalous occurrences and behavior in user or network activity that may be indicative of potential security issues are readily discernible

The EIEP's system must include the capability to prevent employees from unauthorized browsing of SSA records. SSA strongly recommends 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 then need anomaly detection to detect and monitor 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 way that it goes undetected.

If the EIEP's design does not ***currently*** 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** to deter employees from browsing SSA records. These controls must include monitoring and anomaly detection features, either 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. The system must also produce reports that allow management and/or supervisors to monitor user activity, such as the following:

- **User ID Exception Reports:**

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

- **Inquiry Match Exception Reports:**

  This type of report captures information about users who may be initiating transactions for SSNs that have no client case association within the EIEP's system **(the EIEP's management should review 100 percent of these cases).**

- **System Error Exception Reports:**

  This type of report captures information about users who may not understand or may be violating proper procedures for access to SSA-provided information.

- **Inquiry Activity Statistical Reports:**

  This type of report captures information about transaction usage patterns among authorized users and is a tool which enables the EIEP's management to monitor typical usage patterns in contrast to 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.

## 5.7 Management Oversight and Quality Assurance

The EIEP must establish and/or maintain ongoing management oversight and quality assurance capabilities to ensure that only authorized employees have access to SSA-provided information. They must ensure ongoing compliance with the terms of the EIEP's electronic information sharing agreement with SSA and the SSRs established for access to SSA-provided information. The entity responsible for management oversight must 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 employees and position types which require SSA-provided information to do their jobs.

The EIEP must ensure that employees granted access to SSA-provided information receive adequate training on the sensitivity of the information, associated safeguards, operating procedures, and the penalties for misuse.

SSA recommends that EIEPs establish the following job functions and require that employees tasked with these job functions do not also share the same job functions as personnel who request or use information from SSA.

- Perform periodic self-reviews to monitor the EIEP's ongoing usage of SSA-provided information.

- Perform random sampling of work activity that involves SSA-provided information to determine if the access and usage comply with SSA's requirements.

## 5.8 Data and Communications Security

EIEPs must 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 should align with the Standards established by the National Institute of Standards and Technology (NIST). SSA recommends the Advanced Encryption Standard (AES) or triple DES (Data Encryption Standard 3), if AES is unavailable, encryption method for securing SSA-provided information during transport. Files encrypted for external users (when using tools such as Microsoft WORD encryption,) require a key length of nine characters. We also recommend that the key (also referred to as a *password*) contain both special characters and a number. SSA requires that the EIEP deliver the key so that the key 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 Information Exchange Agreement 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 redisclosure of SSA-provided information without written approval. The prohibition applies to both internal and external sources who do not have a "need-to-know[2]." **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.**

EIEPs must 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

[2] Need-to-know - access to the information must be necessary for the conduct of one's official duties.

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 it unrecoverable or destroy the electronic device if they do not need to recover the data. 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:

- **Overwriting**

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 and to protect data against laboratory attacks or forensics. Please refer to ***Definitions*** for more information regarding ***Media Sanitization***). Reformatting the media does not overwrite the data.

- **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). Degaussing requires a certified tool designed for particular types of media. Certification of the tool is required 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 (refer to ***Definitions*** for more information regarding ***Media Sanitization***).

- **Physical destruction**

Physical destruction is the method 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 retention of records. The EIEP must control print media containing SSA-provided information to restrict its access to authorized employees who need such access to perform their official duties. EIEPs must destroy print media containing SSA-provided information in a secure manner when it is no longer required for business purposes. The EIEP should 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.***

The EIEP must employ measures to ensure that communications and data furnished to SSA contain no viruses or other malware.

***Special Note:*** **If SSA-provided information will be stored in a commercial**

**cloud, please provide the name and address of the cloud provider. Also, please describe the security features contractually required of the cloud provider to protect SSA-provided information.**

## 5.9 Incident Reporting

SSA requires EIEPs to develop and implement policies and procedures to respond to data breaches or PII loses. You must explain how your policies and procedures conform to SSA's requirements. The procedures must include the following information:

*If the EIEP 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 and 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 877-697-4889*** *(select "Security and PII Reporting" from the options list). The EIEP will provide updates as they become available to the SSA contact, as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.*

The EIEP must agree to absorb all costs associated with notification and remedial actions connected to security breaches, if SSA determines that the risk presented by the breach or security incident requires the notification of the subject individuals. **SSA recommends that EIEPs seriously consider establishing incident response teams to address PII breaches.**

## 5.10 Security Awareness and Employee Sanctions

The EIEP must designate a department or party to take the responsibility to provide ongoing security awareness training for employees 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's responsibility for proper use and protection of SSA-provided information including its proper disposal
- 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

SSA requires the EIEP to provide security awareness training to all employees and contractors who access SSA-provided information. The training should be annual, mandatory, and certified by the personnel who receive the training. SSA also requires the EIEP to certify that each employee or contractor who views SSA-provided data also certify that they understand the potential criminal and administrative sanctions or penalties for unlawful disclosure.

## 5.11 Contractors of Electronic Information Exchange Partners

As previously stated in ***The General Systems Security Standards***, contractors of the EIEP must adhere to the same security requirements as employees of the EIEP. The EIEP is responsible for the oversight of its contractors and the contractor's compliance with the security requirements. The EIEP will enter into a written agreement with each of its contractors and agents who need SSA data to perform their official duties, whereby such contractors or agents agree to abide by all relevant Federal laws, restrictions on access, use, disclosure, and the security requirements in this Agreement.

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

The EIEP must be able to provide proof of the contractual agreement If the contractor processes, handles, or transmits information provided to the EIEP by SSA or has authority to perform on the EIEP's behalf, the EIEP should clearly state the specific roles and functions of the contractor. The EIEP will provide SSA written certification that the contractor is meeting the terms of the agreement, including SSA security requirements. The certification will be subject to our final approval before redisclosing our information.

The EIEP must also require that contractors who will process, handle, or transmit information provided to the EIEP by SSA sign an agreement with the EIEP that obligates the contractor to follow the terms of the EIEP's data exchange agreement with SSA. The EIEP or the contractor must provide a copy of the data exchange agreement to each of the contractor's employees before disclosing data and make certain that the contractor's employees receive the same security awareness training as the EIEP's employees. The EIEP should maintain awareness-training records for the contractor's employees and require the same annual certification procedures.

The EIEP will be required to conduct the review of contractors and is responsible for ensuring compliance of its contractors with security and privacy requirements and limitations. As such, the EIEP will subject the contractor to ongoing security compliance

reviews that must meet SSA standards. The EIEP will conduct compliance reviews at least triennially commencing no later than three (3) years after the approved initial security certification to SSA; and must provide SSA with written documentation of recurring compliance reviews, with the contractor, subject to our approval.

If the EIEP'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:

- safeguards for sensitive information
- computer system safeguards
- security controls and measures to prevent, detect, and resolve unauthorized access to, use of, and redisclosure of SSA-provided information
- continuous monitoring of the EIEP contractors' network infrastructures and assets

## 6. General -- Security Certification and Compliance Review Programs

SSA's security certification and compliance review programs are distinct processes. The certification program is a one-time process when an EIEP initially requests electronic access to SSA-provided information. The certification process entails two rigorous stages intended to ensure that technical, management, and operational security measures work as designed. SSA must ensure that the EIEPs fully conform to SSA's security requirements 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, however, ensures that the suite of security measures implemented by an EIEP to safeguard SSA-provided information remains in full compliance with SSA's security standards and requirements. 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.

### 6.1 The Security Certification Program

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

- Phase One: The Security Design Plan (SDP) phase is a formal written plan authored by the EIEP to comprehensively document its technical and non-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 SDP. OIS strongly recommends that these EIEPs prepare an SDP.**

  **The EIEP's preparation and maintenance of a current SDP will aid them in determining potential compliance issues prior to reviews, assuring continued compliance with SSA's security requirements, and providing for**

**more efficient security reviews.**

- Phase 2: The SSA Onsite Certification phase is a formal onsite review conducted by SSA to examine the full suite of technical and non-technical security controls implemented by the EIEP to safeguard data obtained from SSA electronically (refer to ***The Certification Process***).

## 6.2 Documenting Security Controls in the Security Design Plan (SDP)

### 6.2.1 When the SDP and Risk Assessment are Required

EIEPs must submit an SDP and a security risk assessment (RA) for evaluation when one or more of the following circumstances apply. The RA must be in electronic format. It must include discussion of the measures planned or implemented to mitigate risks identified by the RA and (as applicable) risks associated with the circumstances below:

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

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

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

An SDP must satisfactorily document the EIEP's compliance with all of SSA's SSRs in order to provide the minimum level of security acceptable to SSA for its EIEP's access to SSA-provided information.

EIEP's must correct deficiencies identified through the evaluation of the SDP and submit a revised SDP that incorporates descriptions and explanations of the measures implemented to

eliminate the deficiencies. SSA cannot grant access to SSA-provided information until the EIEP corrects the deficiencies, documents the SDP, and SSA approves the revisions. The EIEP will communicate the implementation of corrective actions to SSA on a regular basis. SSA will withhold final approval until the EIEP can rectify all deficiencies.

SSA may revoke the approval of the EIEP's SDP and its access to SSA-provided information if we learn the EIEP is non-compliant with one or more SSRs. The EIEP must submit a revised SDP, which incorporates descriptions and explanations of the measures the EIEP will implement to resolve the non-compliance issue(s). The EIEP must communicate the progress of corrective action(s) to SSA on a regular basis. SSA will consider the EIEP in non-compliant status until resolution of the issue(s), the EIEP's SDP documents the corrections, and we approve the SDP. If, within a reasonable time as determined by SSA, the EIEP is unable to rectify a deficiency determined by SSA to present a substantial risk to SSA-provided information or to SSA, SSA will withhold approval of the SDP and discontinue the flow of SSA-provided information.

***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 System Security Requirements (SSR) and exercise their responsibilities regarding protection of SSA-provided information.**

## 6.3 The Certification Process

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 non-technical and technical controls safeguard SSA-provided information from misuse and improper disclosure and that those safeguards function and work as intended.

At its discretion, SSA may request that the EIEP 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:

- a demonstration of the EIEP's implementation of each requirement
- random sampling of audit records and transactions submitted to SSA
- a walkthrough of the EIEP's data center to observe and document physical security safeguards
- a demonstration of the EIEP's implementation of electronic exchange of data with SSA
- discussions with managers/supervisors
- examination of management control procedures and reports (e.g., anomaly detection reports, etc.)
- demonstration of technical tools pertaining to user access control and if appropriate, browsing prevention, specifically:
    - If the design is based on a permission module or similar design, or it is transaction driven, the EIEP will demonstrate how the system triggers requests for information from SSA.

- If the design is based on a permission module, the EIEP will demonstrate how the process for requests for SSA-provided information prevent SSNs not present in the EIEP's system from sending requests to SSA. We will attempt to obtain information from SSA using at least one, randomly created, fictitious number not known to the EIEPs system.

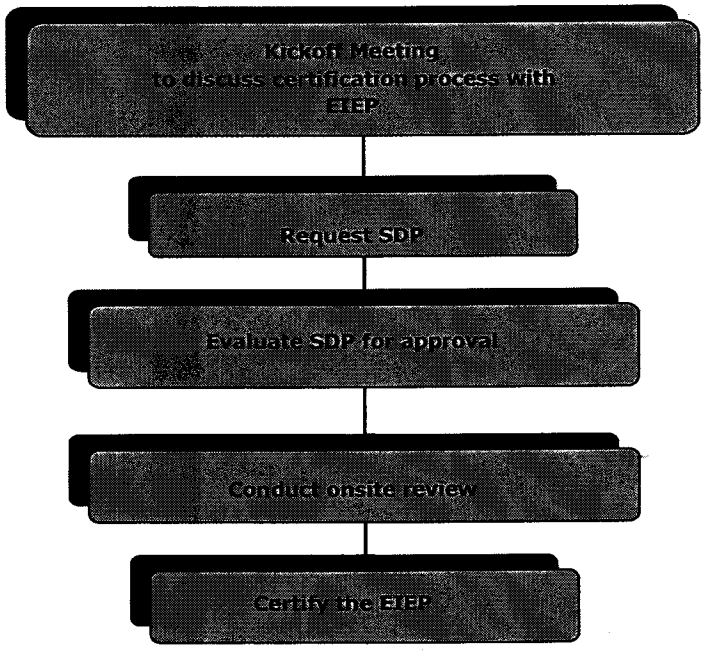
During a certification or compliance review, SSA or a certifier acting on its behalf, may request a demonstration of the EIEP's audit trail system (ATS) and its record retrieval capability. The certifier may request a demonstration of the ATS' capability to track the activity of employees who have the 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. We will 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 own in-house audit capabilities and the process used to obtain audit information from the STC.

If the EIEP employs a contractor who processes, handles, or transmits the EIEP's SSA-provided information offsite, SSA, at its discretion, may 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 exercise, 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 following is a high-level flow chart of the OIS Certification Process:

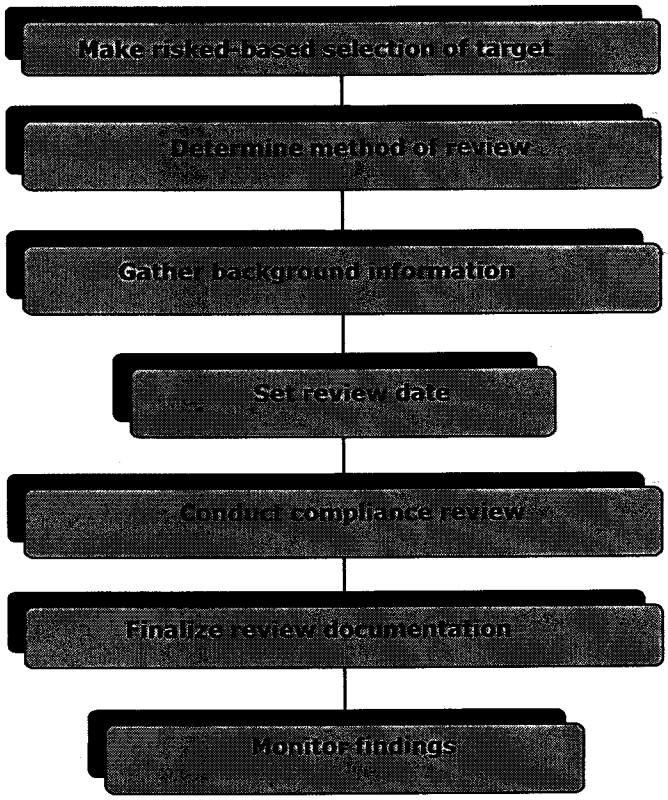


## 6.5 The Compliance Review Program and Process

Similar to the certification process, the compliance review program entails a rigorous process intended to ensure that EIEPs who receive electronic information from SSA are in full compliance with the Agency's security requirements and standards. As a practice, SSA attempts to conduct compliance reviews following a two to five ~~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 significant change in the outside EIEP's computing platform
- a violation of any of SSA's systems security requirements
- an unauthorized disclosure of SSA information by the EIEP

The following is a high-level flow chart of the OIS Compliance Review Process:




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

SSA may, also 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 demonstration of the EIEP's implementation of each requirement
- random sampling of audit records and transactions submitted to SSA
- a walkthrough of the EIEP's data center to observe and document physical security safeguards
- a demonstration of the EIEP's implementation of online exchange of data with SSA
- discussions with managers/supervisors
- examination of management control procedures and reports (e.g. anomaly detection reports, etc.)
- demonstration of technical tools pertaining to user access control and, if appropriate, browsing prevention:
    - If the design uses a permission module or similar design, or is transaction driven, the EIEP will demonstrate how the system triggers requests for information from SSA.
    - If the design uses a permission module, the EIEP will demonstrate the process used to request SSA-provided information and prevent the EIEP's system from processing SSNs not present in the EIEP's system. We can accomplish this by attempting to obtain information from SSA using at least one, randomly created, fictitious number not known to the EIEP's system.

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

- the EIEP has experienced a security breach or incident involving SSA-provided information
- the EIEP has unresolved non-compliancy issue(s)
- to review an offsite contractor's facility that processes SSA-provided information
- the EIEP is a legacy organization that has not yet been through SSAs security certification and compliance review programs
- 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 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 (i.e., the compliance review is not being conducted to address a special circumstance, such as a disclosure violation) 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 Final Report will address findings and recommendations from SSA's compliance review, which includes a plan for monitoring each issue until closure.

***NOTE: SSA handles documentation provided for compliance reviews as sensitive information. 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 information sharing 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.***

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. We may also use additional factors to determine whether SSA will perform an onsite or remote compliance review.

- **High/Medium Risk Criteria**
  - undocumented closing of prior review finding(s)
  - implementation of technical/operational controls that affect security of SSA-provided information (e.g. implementation of new data access method)
  - PII breach
- **Low Risk Criteria**
  - no prior review finding(s) or prior finding(s) documented as closed
  - no implementation of technical/operational controls that impact security of SSA-provided information (e.g. implementation of new data access method)
  - no PII breach

### 6.5.1 EIEP Compliance Review Participation

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

- a sample of managers and/or supervisors 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
- the individuals responsible for performing security awareness and employee sanction functions to learn how you fulfill this requirement
- 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

- the individual(s) responsible for management oversight and quality assurance functions to confirm how your agency accomplishes this requirement

- additional individuals as deemed appropriate by SSA

### 6.5.2 Verification of Audit Samples

Prior to or during the compliance review, SSA will present to the EIEP a sampling of transactions previously submitted to SSA for verification. SSA requires the EIEP to verify whether each transaction was, per the terms of their agreement with SSA, legitimately submitted by a user authorized to do so.

SSA requires the EIEP to provide a written attestation of the transaction review results. The document must provide:

- confirmation that each sample transaction located in the EIEP's audit file submitted by its employee(s) was for legitimate and authorized business purposes

- an explanation for each sample transaction located in the EIEP's audit file(s) determined to have been unauthorized

- an explanation for each sample transaction not found in the EIEP's ATS

When SSA provides the sample transactions to the EIEP, detailed instructions will be included. Only an official responsible for the EIEP is to provide the attestation.

## 6.6 Scheduling the Onsite Review

SSA will not schedule the onsite review until we approve the EIEP's SDP. SSA will send approval notification via email. 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 follow as soon as reasonably possible.

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

- the reason for submission of a plan

- the severity of security issues, if any

- circumstances of the previous review, if any

- SSA workload considerations

Although the scheduling of the review is contingent upon approval of the SDP, SSA may perform an onsite review prior to approval if we determine that it is necessary to complete our evaluation of a plan.

**(THIS PAGE HAS BEEN LEFT BLANK INTENTIONALLY)**

## 7. Additional Definitions

**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 and preexisting EIEP PII.

**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).

**Dial-up:**

Sometimes used synonymously with *dial-in*, refers to digital data transmission over the wires of a local telephone network.

**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:**

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

- 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.

- 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.

  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.

- 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. For example, 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.

**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:**

Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest of the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

**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 that is provided to an external entity under the terms of an information exchange agreement with SSA. The following are examples of

SSA-provided data/information:

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

- 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 that is 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 to certify the accuracy of the information. The following are examples of SSA information:

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

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

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

- 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

- 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 that 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:**

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

**Third Party:**

This term 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:

- is not stipulated access to SSA-provided information by an information-sharing agreement between an EIEP and SSA
- has no information-sharing agreement with SSA
- 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.

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

## 8. Regulatory References

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

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

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

## 9. Frequently Asked Questions

**(Click links for answers or additional information)**

1. Q: What is a breach of data?
   A: Refer also 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 SDP was submitted. Can the Onsite Review be scheduled now?
   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 meant by 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 SDP?
   A: Refer to When the SDP and RA are Required.

7. Q: Does an EIEP have to submit an SDP when the agreement is

renewed?

A: The EIEP does not have to submit an SDP ***because*** the agreement between the EIEP and SSA was renewed. There are, however, circumstances that require an EIEP to submit an SDP. Refer to When the SDP and RA are Required.

8. Q: Is it acceptable to save SSA data 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 data 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 SDP as a .PDF file?

A: No, it is not. The document must remain editable.

12. Q: Should the EIEP write the SDP from the standpoint of my agency's SVES access itself, or from the standpoint of access to all data provided to us by SSA?

A: The SDP is to encompass your agency's electronic access to SSA-provided information as per the electronic data sharing agreement between your agency and SSA. Refer to Developing the SDP.

13. Q: If we have a "transaction-driven" system, do we still need a permission module? If employees cannot initiate a query to SSA, why would we need the permission module?

A: "Transaction driven" basically means that queries automatically submit requests (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 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 the process wherein SSA performs periodic site visits to its Electronic Information Exchange Partners (EIEP) to certify whether the EIEP's 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.

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

Refer also to the Review Determination Matrix.

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 identifiable information (PII) since its previous compliance review.
- SSA rates the EIEP as a low-risk agency or state

# ATTACHMENT 5

# WORKSHEET FOR REPORTING LOSS OR POTENTIAL LOSS OF PERSONALLY IDENTIFIABLE INFORMATION

**ATTACHMENT 5** **09/27/06**

**Worksheet for Reporting Loss or Potential Loss of Personally Identifiable Information**

**1. Information about the individual making the report to the NCSC:**

| | | | | | |
|---|---|---|---|---|---|
| Name: | | | | | |
| Position: | | | | | |
| Deputy Commissioner Level Organization: | | | | | |
| Phone Numbers: | | | | | |
| Work: | | Cell: | | Home/Other: | |
| E-mail Address: | | | | | |
| Check one of the following: | | | | | |
| Management Official | | Security Officer | | Non-Management | |

**2. Information about the data that was lost/stolen:**

Describe what was lost or stolen (e.g., case file, MBR data):

Which element(s) of PII did the data contain?

| | | | |
|---|---|---|---|
| Name | | Bank Account Info | |
| SSN | | Medical/Health Information | |
| Date of Birth | | Benefit Payment Info | |
| Place of Birth | | Mother's Maiden Name | |
| Address | | Other (describe): | |

Estimated volume of records involved:

**3. How was the data physically stored, packaged and/or contained?**

Paper or Electronic? (circle one):

If Electronic, what type of device?

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Laptop | | Tablet | | Backup Tape | | Blackberry | |
| Workstation | | Server | | CD/DVD | | Blackberry Phone # | |
| Hard Drive | | Floppy Disk | | USB Drive | | | |
| Other (describe): | | | | | | | |

Additional Questions if Electronic:

| | Yes | No | Not Sure |
|---|---|---|---|
| a. Was the device encrypted? | | | |
| b. Was the device password protected? | | | |
| c. If a laptop or tablet, was a VPN SmartCard lost? | | | |
| Cardholder's Name: | | | |
| Cardholder's SSA logon PIN: | | | |
| Hardware Make/Model: | | | |
| Hardware Serial Number: | | | |

Additional Questions if Paper:

| | Yes | No | Not Sure |
|---|---|---|---|
| a. Was the information in a locked briefcase? | | | |
| b. Was the information in a locked cabinet or drawer? | | | |
| c. Was the information in a locked vehicle trunk? | | | |
| d. Was the information redacted? | | | |
| e. Other circumstances: | | | |

4. **If the employee/contractor who was in possession of the data or to whom the data was assigned is not the person making the report to the NCSC (as listed in #1), information about this employee/contractor:**

| | | | | | |
|---|---|---|---|---|---|
| Name: | | | | | |
| Position: | | | | | |
| Deputy Commissioner Level Organization: | | | | | |
| Phone Numbers: | | | | | |
| Work: | | Cell: | | Home/Other: | |
| E-mail Address: | | | | | |

5. **Circumstances of the loss:**
   a. When was it lost/stolen?

   b. Brief description of how the loss/theft occurred:

   c. When was it reported to SSA management official (date and time)?

6. **Have any other SSA components been contacted? If so, who? (Include deputy commissioner level, agency level, regional/associate level component names)**

7. **Which reports have been filed? (include FPS, local police, and ~~SSA reports~~)**

| **Report Filed** | Yes | No | Report Number |
|---|---|---|---|
| Federal Protective Service | | | |
| Local Police | | | |

| | Yes | No |
|---|---|---|
| SSA-3114 (Incident Alert) | | |
| SSA-342 (Report of Survey) | | |
| Other (describe) | | |

8. **Other pertinent information (include actions under way, as well as any contacts with other agencies, law enforcement or the press):**