**OFFICE OF**
**THE INSPECTOR GENERAL**

**SOCIAL SECURITY ADMINISTRATION**

# THE SOCIAL SECURITY ADMINISTRATION'S INCIDENT RESPONSE AND REPORTING SYSTEM

**August 2007** **A-14-07-17070**

# AUDIT REPORT

## Mission

**By conducting independent and objective audits, evaluations and investigations, we inspire public confidence in the integrity and security of SSA's programs and operations and protect them against fraud, waste and abuse. We provide timely, useful and reliable information and advice to Administration officials, Congress and the public.**

## Authority

**The Inspector General Act created independent audit and investigative units, called the Office of Inspector General (OIG). The mission of the OIG, as spelled out in the Act, is to:**

- **Conduct and supervise independent and objective audits and investigations relating to agency programs and operations.**
- **Promote economy, effectiveness, and efficiency within the agency.**
- **Prevent and detect fraud, waste, and abuse in agency programs and operations.**
- **Review and make recommendations regarding existing and proposed legislation and regulations relating to agency programs and operations.**
- **Keep the agency head and the Congress fully and currently informed of problems in agency programs and operations.**

**To ensure objectivity, the IG Act empowers the IG with:**

- **Independence to determine what reviews to perform.**
- **Access to all information necessary for the reviews.**
- **Authority to publish findings and recommendations based on the reviews.**

## Vision

**We strive for continual improvement in SSA's programs, operations and management by proactively seeking new ways to prevent and deter fraud, waste and abuse. We commit to integrity and excellence by supporting an environment that provides a valuable public service while encouraging employee development and retention and fostering diversity and innovation.**

# SOCIAL SECURITY

**MEMORANDUM**

Date: August 3, 2007 Refer To:

To: The Commissioner

From: Inspector General

Subject: The Social Security Administration's Incident Response and Reporting System (A-14-07-17070)

## OBJECTIVE

The objective of our review was to determine if the Social Security Administration (SSA) has an effective system for detecting, reporting, and responding to security incidents, in accordance with Federal regulations and established standards and guidelines.

## BACKGROUND

Computer security-related threats have not only become numerous, diverse, and rapidly evolving but also more damaging and disruptive. Incident response capabilities are necessary for rapidly detecting incidents, minimizing loss and destruction, and restoring computing services. Incident response and reporting guidelines and procedures should have consistent, effective, and efficient actions, which are particularly important for incidents that may lead to prosecution. Also, handling evidence in a forensically sound manner puts decision makers in a position where they can confidently take the necessary actions.[1]

For an organization, an effective incident response capability is a complex undertaking and requires substantial planning and resources which should include:

- continuous monitoring for threats through intrusion detection systems;
- establishing clear procedures to assess the business impact of incidents;
- implementing effective methods to collect, analyze and report data; and
- developing relationships with appropriate internal and external groups.

[1] National Institute of Standards and Technology Special Publication (SP) 800-86, *Guide to Integrating Forensic Techniques into Incident Response*, August 2006.

The Federal Information Security Management Act of 2002 (FISMA) requires Federal agencies to develop, document, and implement an information security program that includes procedures for detecting, reporting, and responding to security incidents.[2] In July 2006, the Office of Management and Budget (OMB) released updated guidance[3] on the reporting of security incidents involving Personally Identifiable Information (PII)[4] to the United States Computer Emergency Readiness Team (US-CERT). Agencies are now required to report all incidents involving PII to US-CERT within 1 hour of discovering the incident. In September 2006, OMB issued a memorandum[5] that contained the Identity Theft Task Force recommendations on the approach a department or agency should take in responding to a theft, loss, or unauthorized acquisition of personal information (i.e., incident) that poses a risk of subsequent identity theft.

SSA maintains some of the largest databases of any civilian Federal agency. These databases contain PII such as names, addresses, Social Security numbers (SSN), dates of birth, and mothers' maiden names. SSA's Office of Systems (OS) is responsible for maintaining these databases. Within OS, the Office of Telecommunications and Systems Operations (OTSO) is responsible for controlling and protecting the databases. To meet the requirements of FISMA, SSA developed several methods to detect, remediate, report, and track security incidents. SSA established a team within OS to handle security incidents on a daily basis. SSA also has a contractor that operates an automated intrusion detection system. SSA routinely monitors firewall activity to detect any incidents. Additionally, there is a help desk for employees to contact in the event of information technology problems including potential security incidents. Potential security incidents are tracked in SSA's Change Asset Problem Reporting System (CAPRS).

## RESULTS OF REVIEW

SSA has established a framework for its incident response and reporting system. There are various components within SSA that work together to protect the Agency's personal information and effectively remediate incidents when they occur. While the Agency works diligently to protect itself against the latest security related incidents, the following areas need improvement:

---

[2] Public Law (PL) 107-347, Title III, sections 301-303, 16 Stat. 2899, 2946-2959 (2002).

[3] OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 12, 2006.

[4] PII is any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, Social Security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

[5] OMB Memorandum, *Recommendations for Identity Theft Related Data Breach Notifications*, September 20, 2006.

- SSA needs to appropriately address all security incidents, and
- SSA needs to ensure that the Office of the Inspector General (OIG) is appropriately included in the incident response process.

## SSA NEEDS TO APPROPRIATELY ADDRESS ALL SECURITY INCIDENTS

We determined that SSA did not identify and report all appropriate incidents to the Office of the Chief Information Officer (OCIO), US-CERT, and OIG. SSA needs to report all appropriate security incidents to US-CERT and law enforcement as required by FISMA. US-CERT coordinates defense against and responses to cyber attacks across the Nation.

There are two types of security incidents: (1) computer security-related, and (2) PII. For the computer security-related incidents, US-CERT has published seven computer security incident and event categories for Federal agencies, in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-61.[6] The incident and event categories along with their respective reporting timeframes are reflected in Tables 1 and 2 which follow.

**Table 1**
**Federal Agency Incident Categories**

| Category | Name | Reporting Timeframe |
|---|---|---|
| Category 0 | Exercise/Network Defense Testing | Not Applicable – for Agency's internal use. |
| Category 1 | Unauthorized Access | Within 1 hour of discovery/detection. |
| Category 2 | Denial of Service | Within 2 hours of discovery/detection. |
| Category 3 | Malicious Code | Daily<br>Within 1 hour of discovery/detection if widespread across agency. |
| Category 4 | Improper Usage | Weekly |

**Table 2**
**Federal Agency Event Categories**

| Category | Name | Reporting Timeframe |
|---|---|---|
| Category 5 | Scans/Probes/Attempted Access | Monthly |
| Category 6 | Investigation | Not Applicable – for Agency's internal use. |

[6] NIST SP 800-61, *Computer Security Incident Handling Guide*, Section 2.1, January 2004; http://www.us-cert.gov/federal/reportingRequirements.html.

## Computer Security-Related Incidents

From October 1, 2005 through January 26, 2007, SSA did not report any computer security-related incidents to US-CERT. We reviewed all potential computer security-related incidents in CAPRS for that time period and found 75 cases that should have been reported. Specifically, we identified 39 "Category 3 – Malicious Code" incidents, 23 "Category 4 – Improper Usage" incidents, and 9 "Category 5 – Scans/Probes/Attempted Access" events that should have been reported to US-CERT. We identified an additional 4 "Category 5 – Scans/Probes/Attempted Access" events which were not included in SSA's CAPRS database, for a total of 75 incidents and events that should have been reported to US-CERT. For example, one incident not reported concerned a workstation that had a virus that could not be remediated through the normal channels of running anti-virus software. The workstation had to be re-imaged. Another example included hacking attempts where SSA sends a letter to the source's Internet Service Provider informing them of the illegal activity.

SSA reported that during 2004, it developed and US-CERT approved an approach that limited reporting to only incidents that could not be prevented, or if successful, caused undue harm. SSA could not provide documentation regarding this agreement with US-CERT. We contacted US-CERT personnel and they noted that it is not their practice to make these types of agreements with Federal agencies. Applying its own approach, SSA accordingly reported zero incidents. OS is responsible for identifying and evaluating potential incidents and informing the OCIO. However, we believe the Agency did not meet the intent of US-CERT's guidance[7] when it refrained from reporting instances where the activities were successfully mitigated and did not impact SSA services, internally or externally. Therefore, SSA needs to properly categorize and report computer-related security incidents in accordance with NIST and US-CERT. SSA plans to meet with US-CERT to discuss the Agency's incident categorization and reporting practices so it is consistent with Federal regulations and guidelines.

## Personally Identifiable Information Incidents

For the PII incidents, we identified a total of 1,106 potential incidents in CAPRS from August 9, 2006 through January 26, 2007. During our review of the potential PII incidents, we found 147 incidents involving more than 1 record (see Table 3) that were similar to other incidents SSA reported to US-CERT. US-CERT collects this information to identify trends and ensure Agencies take corrective measures if incidents recur and weaknesses continue to exist.

SSA reported 8 of the 147 incidents. For example, one of the eight incidents reported involved the theft of a laptop and case folders that were not recovered. We have listed some examples from the 139 unreported incidents that were similar to the 8 incidents reported.

---

[7] NIST SP 800-61, *Computer Security Incident Handling Guide*, Section 2.1, January 2004.

- A workstation was stolen from a field office that was burglarized. SSA never received the workstation back.
- A box was lost during shipment from a Disability Determination Services (DDS) office to a Program Service Center. The box contained eight disability folders that were not recovered.
- A DDS employee e-mailed 55 claimants' SSNs, name, and case numbers to a "Hotmail" e-mail account.

**Table 3**
**PII Incidents Involving More Than One Record**

| PII Categories | Incidents Reported by SSA | Unreported Incidents | Total Incidents |
|---|---|---|---|
| More than one record was disclosed and the records were returned or retrieved | 0 | 53 | 53 |
| More than one record was disclosed and the records were not returned or retrieved | 8 | 86 | 94 |
| **TOTAL** | **8** | **139** | **147** |

The Agency advised us that a risk-based approach was used to determine what was reported to the former Commissioner[8] and to US-CERT. The former Commissioner made the final decision on what was reported to US-CERT.

In addition to the 147 incidents involving multiple records identified above, we discovered 959 incidents that involved only 1 claimant's record. SSA reported only one incident (see Table 4) involving one record to US-CERT. This incident involved an SSA document that was given to an unauthorized individual and returned. We have listed below some examples that are similar to the one incident reported.

- A detailed earnings query was accidentally mailed out to a wrong individual.
- A DDS employee sent disability information to the wrong claimant.
- A request for medical information was inadvertently sent to the wrong doctor.

[8] Jo Anne B. Barnhart, Commissioner of Social Security 2001 – 2007.

| Table 4<br>PII Incidents Involving One Record | | | |
|---|---|---|---|
| **PII Categories** | **Incidents Reported by SSA** | **Unreported Incidents** | **Total Incidents** |
| One record was disclosed and the record was returned or retrieved. | 1 | 684 | 685 |
| One record was disclosed and the record was not returned or retrieved. | 0 | 274 | 274 |
| **TOTAL** | **1** | **958** | **959** |

SSA needs to develop a formal policy for reporting PII incidents to US-CERT and ensure its compliance. The Agency is revising the policy for reporting PII to reflect decisions of SSA's Commissioner. The Agency estimates that more of the PII incidents recorded in CAPRS will be reported to US-CERT when the new policy is fully implemented.

For the PII incidents returned to the Agency, SSA did not record the amount of time the PII was out of the Agency's possession. SSA should also track the length of time PII is out of its control.

The incidents and events listed above that were not reported to OCIO, US-CERT or law enforcement were the result of the following weaknesses in SSA's incident reporting policies and procedures.

- SSA lacks written procedures for detecting and reporting security incidents.
- SSA's policy definition for a security incident is compliant with NIST and US-CERT; but the definition was not consistently implemented throughout the Agency.
- SSA's roles and responsibilities for incident reporting do not comply with FISMA.

## SSA Lacks Written Procedures for Detecting and Reporting Security Incidents

SSA did not adequately report all security incidents to US-CERT because SSA does not have adequate written procedures for detecting and reporting security incidents. According to FISMA, Federal agencies should have procedures to detect, report, and respond to security incidents. During our audit, we found the Agency lacked procedures to review information provided by US-CERT for detecting security incidents. For example, US-CERT provides Federal agencies with data regarding suspicious Internet protocol addresses and key logging incidents for agencies to incorporate into their response programs. SSA did not always review or use this data to avoid or detect security incidents. As a result of the lack of regular reviews, security information available from US-CERT in September 2006 was not addressed until brought to SSA's attention in February 2007. At the end of the audit, SSA provided us procedures for reviewing and responding to security events from US-CERT.

We also found the Agency lacked formal written procedures for reporting security incidents to US-CERT but the Agency plans to develop them in accordance with NIST. OCIO plans to have this developed by the fourth quarter of Calendar Year 2007. Once SSA has finalized its revised incident security policy, then procedures can be written to address the specific functions.

## SSA's Policy Definition for a Security Incident is Compliant with NIST and US-CERT; but the Definition Was Not Consistently Implemented throughout the Agency

SSA's implementation of its applied definition of a security incident was inconsistent with formal Federal guidance. According to SSA, an approach was developed with US-CERT approval, which limited reporting to only incidents that could not be prevented, or if successful caused undue harm. SSA's Information Systems Security Handbook (ISSH) is the official security policy for the Agency. Although the ISSH definition of a security incident concurred with the NIST and US-CERT definition, the actual practices followed by the Agency were not documented in the ISSH, leaving misconceptions over what should be reported to US-CERT. However, as noted above, no documentation supporting an agreement with US-CERT was provided and US-CERT states it does not make agreements with individual agencies.

Prior to July 2006, the ISSH definition included "…suspected viruses, threats to persons, attempted systems intrusions, unauthorized release of Privacy Act information, theft of government or personal property, or any other suspicious situation."[9] In July 2006, the ISSH was updated to define a security incident as follows:

> An event in a computer system, or the threat of such an event, that would cause an adverse impact on the system. Examples of security incidents include malicious code (virus, worm, or Trojan horse), e-mail bombardment (spamming), an unauthorized change in system configuration or discovery of an unknown "hidden file", repeated attempts to access SSA's systems (hacking), or a stranger's attempt to learn PINs and passwords under false pretexts (social engineering).[10]

OTSO is the component responsible for monitoring SSA's firewall, logging security events that need to be researched, identifying security incidents, and reporting incidents

---

[9] Information Systems Security Handbook (ISSH), Chapter 16, *Security Incident Identification, Reporting and Resolution*, page 3, May 2001.

[10] ISSH, Chapter 7, July 15, 2006.

to the OCIO. The definition of a security incident SSA applied did not include "attempts" or "threats," as follows: "A computer incident is an adverse event, which compromises some aspect of computer or network security."[11]

NIST defines an incident as "…a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices."[12] While SSA's published definition of a security incident was similar to the US-CERT definition and included spamming, the definition was not being fully followed by OS. Consequently, OS only reported incidents involving PII to the OCIO and did not consider threats or attempted intrusions as security incidents. In addition, SSA needs to revise its definition of a security incident to concur with NIST.

## SSA's Roles and Responsibilities for Incident Reporting Do Not Comply with FISMA

SSA did not fully implement the roles and responsibilities for reporting security incidents in accordance with FISMA. FISMA requires Federal agencies to develop, document, and implement an agency-wide information security program.[13] FISMA designates the responsibility for developing and maintaining the agencywide information security program to the agencies' Chief Information Officers (CIO).[14] This security program must include an incident response capability. This capability includes procedures for detecting, reporting, and responding to security incidents.[15] FISMA also grants NIST the responsibility to develop security standards, guidelines, and procedures.[16] NIST states the incident response capability should include: "…organizational structure and delineation of roles, responsibilities, and levels of authority…."[17]

SSA has established a Security Response Team (SRT) to respond when significant incidents arise. As described in the Agency's ISSH, one of the roles of the SRT is to respond to incidents involving computer systems, Internet and Intranet servers, and Local Area Network (LAN) Servers, including malicious code (virus, worm, or Trojan horse) and e-mail bombardment (spamming), and alerts all end users to current threats

---

[11] *An Overview of the Computer Incident Response Process at the Social Security Administration*, Office of Systems, Office of Telecommunications and Systems Operations, Division of Telecommunications Security and Standards, April 28, 2005.

[12] NIST SP 800-61, *Computer Security Incident Handling Guide*, Section 2.1, January 2004.

[13] 44 United States Code (USC) § 3544.

[14] 44 USC § 3544(3)(B).

[15] 44 USC § 3544(a)(3)(B).

[16] 15 USC § 278g-3.

[17] NIST SP 800-61, *Computer Security Incident Handling Guide*, Section 2.3.1, January 2004.

to the system. Additionally, the ISSH states the SRT "…consists of security staff, systems personnel, and representatives of the Office of the Inspector General."[18]

SRT has not convened over the past several years when significant incidents have occurred. Part of the reason for this inactivity seems to be that the criteria for invoking the SRT has not been clearly defined and documented. Additionally, the components and their representatives serving on the SRT have not been clearly identified. We believe it is critical that the ISSH identify the components that are represented on the SRT. In this era of rapidly changing personnel, it is essential that the SRT be as clearly defined as possible to ensure effective continuity and performance of the incident response and reporting process.

SSA also did not comply with FISMA with regard to responsibility for notification of incidents. The ISSH states that the Deputy Commissioner for Systems (DCS) is "…responsible for preparing and sending reports to the US-CERT on security incidents."[19] According to FISMA, a Federal agency's CIO should notify and consult with US-CERT.[20] According to SSA, although DCS sends the monthly incident reports to the OCIO, DCS also sent the monthly incident reports directly to US-CERT through April 2006. SSA did not send any monthly reports to US-CERT from May through November 2006. Then, after internal Agency discussions on SSA's FISMA requirements, the OCIO began reporting the monthly incidents to US-CERT. Because of this lack of a formalized process, the type and number of incidents reported to US-CERT was inconsistent. SSA's security policy needs to be updated to reflect the current process for reporting incidents in accordance with FISMA. The OCIO plans to revise the Agency's security policy for reporting incidents.

## SSA NEEDS TO ENSURE THAT THE OIG IS INCLUDED IN THE INCIDENT RESPONSE PROCESS WHEN APPROPRIATE

Since September 11, 2001, Inspectors General have worked with agencies to afford greater protection over the Nation's critical assets. Identity theft has increasingly become a more prevalent and destructive crime. As the holder of one of the largest databases of PII, SSA can be a prime target for terrorists and criminals who wish to harm our Nation and its citizens. SSA's Inspector General has the tools and is in the position to help SSA secure information and prevent harm.

To mitigate the risk of identity theft, OMB issued a memorandum[21] recommending that all Federal agencies establish "…a core response group that can be convened in the event of a breach." The memorandum also recommended that, in the event of a

---

[18] ISSH, Chapter 7, Appendix B, *Roles and Responsibilities*.

[19] ISSH, Section 7.4, Appendix B.

[20] 44 USC § 3544(b)(7)(C)(iii).

[21] OMB Memorandum *Recommendations for Identity Theft Related Breach Notification*, September 20, 2006.

breach, the core response group conduct a risk analysis to determine whether the incident poses problems related to identity theft and, if the risk of identity theft is present, that the agency tailors its response accordingly.

The memorandum states:

> …a core group should include, at a minimum, an agency's chief information officer, chief legal officer, chief privacy officer (or their designees), a senior management official from the agency, and the agency's inspector general (or equivalent or designee). Such a group should ensure that the agency has brought together many of the basic competencies needed to respond, including expertise in information technology, legal authorities, the Privacy Act, and law enforcement.

In terms of safeguarding PII, SSA stated it is in the process of reviewing and revising the PII policies and procedures developed under the direction of the former Commissioner to reflect the direction of SSA's current Commissioner. Part of the revised process will be to put in place an agencywide governance model, which will include an executive level steering committee as well as other standing and ad hoc workgroups and teams which will oversee the development and implementation of the Agency's policies for safeguarding PII. For example, the Agency will use a cross component workgroup to develop PII notice and remediation issues including establishing a "core group" as recommended in OMB's memorandum[22] concerning data breach notification. However, as of June 1, 2007, SSA has not included the OIG in the core response group as recommended by OMB.

SSA did not consistently notify OIG's Office of Investigations when security incidents occurred so that OIG could have assisted in the preservation of electronic evidence and potentially pursue the matter for further investigation, if necessary. We identified at least six incidents and events that should have been referred to the OIG for investigation—two PII incidents and four security-related events. For example, one incident involved an employee having unauthorized password cracking software running on an external hard drive connected to his workstation. Another example involved an employee who misappropriated approximately 40 case folders for her personal use. The four security-related events involved hacking attempts when SSA sent abuse letters to Internet Service Providers (ISP). When the ISPs did not respond, SSA should have referred these cases to OIG so that an appropriate investigation would have been performed and appropriate action taken.

---

[22] OMB Memorandum *Recommendations for Identity Theft Related Breach Notification*, September 20, 2006.

FISMA requires Federal agencies, as part of their security program, to have procedures for notifying and consulting with law enforcement agencies, including the OIG, when incidents occur.[23] Additionally, NIST guidance recommends that law enforcement be contacted "…through designated individuals in a manner consistent with the requirements of the law and the organization's procedures."[24]

## CONCLUSION AND RECOMMENDATIONS

We found SSA has taken steps to detect, report, and respond to security incidents. The Agency has established a framework for its incident response and reporting system, and components within SSA work diligently to protect the Agency's personal information and effectively remediate incidents when they occur. However, we have identified areas that need improvement, such as in SSA's core response group, consistency in the Agency's incident reporting policy and practices, the classification and reporting of incidents, and in the stipulations of the SRT. Therefore, we recommend SSA:

1. Ensure the definition of a security incident consistent with NIST is known and used throughout the Agency.

2. Align policy, procedures and practices for reporting **PII incidents** including the Agency's escalation policy to US-CERT.

3. Fully develop and implement formal written procedures consistent with the Agency's policy and practice for reporting **Computer-Related Security incidents** to US-CERT.

4. Properly categorize and report computer-related security incidents in accordance with the NIST and US-CERT criteria.

5. Finalize and implement formal written procedures for reviewing and responding to security events from US-CERT.

6. Fully implement the SRT identified in the Agency's incident response policy. This includes adequately identifying all members of the SRT and defining criteria for when the SRT should be invoked.

7. Include the OIG in the core response group recommended by the September 20, 2006 OMB Memorandum.

8. Ensure that OIG is notified of all actual or potential security incidents when they occur, so OIG can determine whether further criminal investigation is required.

---

[23] 44 USC § 3544(b)(7)(C)(i).

[24] NIST SP 800-61, *Computer Security Incident Handling Guide*, Section 2.3.2.2, January 2004.

## AGENCY COMMENTS

SSA agreed with all our recommendations. See Appendix C for the full text of SSA's comments.

Patrick P. O'Carroll, Jr.

# Appendices

APPENDIX A – Acronyms

APPENDIX B – Scope and Methodology

APPENDIX C – Agency Comments

APPENDIX D – OIG Contacts and Staff Acknowledgments

# Acronyms

| | |
|---|---|
| CAPRS | Change, Asset, and Problem Reporting System |
| CIO | Chief Information Officer |
| DCS | Deputy Commissioner for Systems |
| DDS | Disability Determination Services |
| FISMA | Federal Information Security Management Act of 2002 |
| ISSH | Information Systems Security Handbook |
| ISP | Internet Service Providers |
| NIST | National Institute of Standards and Technology |
| OCIO | Office of the Chief Information Officer |
| OIG | Office of the Inspector General |
| OMB | Office of Management and Budget |
| OS | Office of Systems |
| OTSO | Office of Telecommunications and Systems Operations |
| PII | Personally Identifiable Information |
| SSA | Social Security Administration |
| SP | Special Publication |
| SRT | Security Response Team |
| U.S.C. | United States Code |
| US-CERT | United States Computer Emergency Readiness Team |

# Scope and Methodology

Our objective was to determine if the Social Security Administration (SSA) has an effective system for detecting, reporting, and responding to security incidents in accordance with Federal regulations and established standards and guidelines.

To meet our objective, we examined SSA policies, procedures and practices used by the Agency in their detection and reporting of attacks against its networks. Specifically, we examined:

- SSA's policy for the Agency's incident response and reporting system, in the November 15, 2006, June 15, 2006, and the May 2001 version of the *Information Systems Security Handbook*;
- Incident response procedures in *An Overview of the Computer Incident Response Process at the Social Security Administration,* Office of Systems (OS), Office of Telecommunications and Systems Operations, Division of Telecommunications Security and Standards, April 28, 2005;
- Monthly Computer Incident Reports from October 2005 through November 2006; and
- Incidents documented in the Change Asset Problem Reporting System according to the Federal Agency Incident Categories (see following table)[1] and recorded incidents when Internet Service Providers were contacted.

[1] US-CERT Federal Incident Reporting Guidelines, http://www.us-cert.gov/federal/reportingrequirements.html.

| Federal Agency Incident Categories | | | |
|---|---|---|---|
| **Category** | **Name** | **Description** | **Reporting Timeframe** |
| Category 0 | Exercise/ Network Defense Testing | This category is used during state, federal, national, international exercises and approved activity testing of internal/external network defenses or responses. | Not Applicable; this category is for each agency's internal use during exercises. |
| Category 1 | Unauthorized Access | In this category an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource | Within 1 hour of discovery/detection. |
| Category 2 | Denial of Service | An attack that *successfully* prevents or impairs the normal authorized functionality of networks, systems or applications by exhausting resources. This activity includes being the victim or participating in the Denial of Service. | Within 2 hours of discovery/detection if the successful attack is still ongoing and the agency is unable to successfully mitigate activity. |
| Category 3 | Malicious Code | *Successful* installation of malicious software (e.g., virus, worm, Trojan horse, or other code-based malicious entity) that infects an operating system or application. Agencies are NOT required to report malicious logic that has been *successfully quarantined* by antivirus software. | Daily<br>Note: Within 1 hour of discovery/detection if widespread across agency. |
| Category 4 | Improper Usage | A person violates acceptable computing use policies. | Weekly |

| Federal Agency Event Categories | | | |
|---|---|---|---|
| **Category** | **Name** | **Description** | **Reporting Timeframe** |
| Category 5 | Scans/Probes/ Attempted Access | This category includes any activity that seeks to access or identify a federal agency computer, open ports, protocols, service, or any combination for later exploit. This activity does not directly result in a compromise or denial of service. | Monthly<br>Note: If system is classified, report within 1 hour of discovery. |
| Category 6 | Investigation | *Unconfirmed* incidents that are potentially malicious or anomalous activity deemed by the reporting entity to warrant further review. | Not Applicable; this category is for each agency's use to categorize a potential incident that is currently being investigated. |

We also reviewed the:

- Federal Information Security Management Act of 2002 (FISMA);[2]
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, *Computer Security Incident Handling Guide,* January 2004;
- NIST SP 800-86, *Guide to Integrating Forensic Techniques into Incident Response,* August 2006;

[2] PL 107-347, Title III, 16 Stat. 2899, 2946-2961 (2002).

- Office of Management and Budget (OMB) Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments,* July 12, 2006;
- OMB Memorandum M-06-15, *Safeguarding Personally Identifiable Information,* May 22, 2006;
- OMB Memorandum M-06-20, *Fiscal Year 2006 Reporting Instructions for the Federal Information Security Act and Agency Privacy Management,* July 17, 2006;
- OMB Memorandum *Recommendations for Identity Theft Related Breach Notification*, September 20, 2006;
- OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, May 22, 2007; and
- *The First Responder's Guide to Computer Forensics*, Carnegie Mellon Software Engineering Institute, March 2005.

We interviewed representatives from International Business Machines Corporation, United States Computer Emergency Readiness Team, and the following SSA components:

- OS is responsible for technical aspects of implementation and maintenance related to SSA's incident reporting process; and
- Office of the Chief Information Officer (OCIO) directs and manages SSA's enterprise information technology security program. This includes establishing Agency-wide security policies, managing the reporting, and monitoring processes to ensure compliance.

We performed our field work in SSA Headquarters from September 2006 through April 2007. We determined that the data used in this report was sufficiently reliable to meet our audit objectives and intended use of the data. We determined that our use of this data should not lead to an incorrect or unintentional message. The audited entities were OCIO and OS. We conducted our review in accordance with generally accepted government auditing standards.

# Agency Comments

# SOCIAL SECURITY

MEMORANDUM

Date: July 19, 2007 Refer To: S1J-3

To: Patrick P. O'Carroll, Jr.
Inspector General

From: David V. Foster /s/
Chief of Staff

Subject: Office of the Inspector General (OIG) Draft Report, "The Social Security Administration's Incident Response and Reporting System" (A-14-07-17070)--INFORMATION

We appreciate OIG's efforts in conducting this review. Our comments on the draft report content and recommendations are attached.

Please let me know if we can be of further assistance. Staff inquiries may be directed to Ms. Candace Skurnik, Director, Audit Management and Liaison Staff, at extension 54636.

Attachment:
SSA Response

**COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL (OIG) DRAFT REPORT, "THE SOCIAL SECURITY ADMINISTRATION'S INCIDENT RESPONSE AND REPORTING SYSTEM"(A-14-07-17070)**

Thank you for the opportunity to review and comment on the draft report. We appreciate your conducting this audit of the Social Security Administration's (SSA) Response and Reporting System. We recognize the importance of ensuring that the Agency has an effective system for detecting, reporting, and responding to security related incidents, in accordance with Federal regulations and established standards and guidelines.

The report captures the essence of the 2004 agreement between SSA and the United States Computer Emergency Readiness Team (US-CERT) officials that limited SSA's reporting to only incidents that could not be prevented, or if were successful, caused undue harm. It is unfortunate that upon SSA OIG's inquiry to US-CERT officials, they would not confirm the agreement. However, we stand behind the veracity of the agreement.

Recommendation 1

SSA should ensure the definition of a security incident consistent with the National Institute of Standards and Technology (NIST) is known and used throughout the Agency.

Comment

We agree. SSA policy and other directives are inclusive of the definition for a security incident defined by NIST and will be communicated throughout the Agency.

Recommendation 2

SSA should align policy, procedures and practices for reporting personally identifiable information **(PII) incidents** including the Agency's escalation policy to the US-CERT.

Comment

We agree. The Agency will work to ensure practices and procedures for reporting and escalation of PII incidents align.

Recommendation 3

SSA should fully develop and implement formal written procedures consistent with the Agency's policy and practice for reporting **Computer-Related Security incidents** to US-CERT.

Comment

We agree. We will develop and implement formal written procedures consistent with Agency policy for reporting computer related security incidents to US-CERT. SSA will report computer related security incidents in accordance with SSA policy, standards and procedures.

Recommendation 4

SSA should properly categorize and report computer-related security incidents in accordance with the NIST and US-CERT criteria.

Comment

We agree. We have updated the Change, Asset, and Problem Reporting System queue to use the US-CERT categories for security incidents.

Recommendation 5

SSA should finalize and implement formal written procedures for reviewing and responding to security events from US-CERT.

Comment

We agree. We have updated the procedures to reflect all incidents reported from US-CERT, not just keyloggers.

Recommendation 6

SSA should fully implement the Security Response Team (SRT) identified in the Agency's incident response policy. This includes adequately identifying all members of the SRT and defining criteria for when the SRT should be invoked.

Comment

We agree. We will review and update the Agency's incident response policy to include identification of SRT members by position and re-defining criteria for activation.

Recommendation 7

SSA should include the OIG in the core response group recommended by the September 20, 2006 Office of Management and Budget Memorandum (OMB).

Comment

We agree. Upon completion and implementation of policy for Notification and Remediation, the OIG will be included in the core response group.

Recommendation 8

SSA should ensure that OIG is notified of all actual or potential security incidents when they occur, so OIG can determine whether further criminal investigation is required.

Comment

We agree. The OIG Criminal Investigations Unit will be notified of all actual or potential security incidents when they occur.

[In addition to the comments above, SSA provided technical comments which have been addressed in this report.]

# OIG Contacts and Staff Acknowledgments

### *OIG Contacts*

Kitt Winter, Director, Data Analysis and Technical Audit Division, (410) 965-9702

Phil Rogofsky, Audit Manager, Network Security and Telecommunications Branch, (410) 965-9719

### *Acknowledgments*

In addition to those named above:

Mary Ellen Moyer, Senior Program Analyst

Anita McMillan, Senior Auditor

For additional copies of this report, please visit our web site at www.socialsecurity.gov/oig or contact the Office of the Inspector General's Public Affairs Specialist at (410) 965-3218. Refer to Common Identification Number A-14-07-17070.

## DISTRIBUTION SCHEDULE

Commissioner of Social Security

Office of Management and Budget, Income Maintenance Branch

Chairman and Ranking Member, Committee on Ways and Means

Chief of Staff, Committee on Ways and Means

Chairman and Ranking Minority Member, Subcommittee on Social Security

Majority and Minority Staff Director, Subcommittee on Social Security

Chairman and Ranking Minority Member, Subcommittee on Human Resources

Chairman and Ranking Minority Member, Committee on Budget, House of Representatives

Chairman and Ranking Minority Member, Committee on Government Reform and Oversight

Chairman and Ranking Minority Member, Committee on Governmental Affairs

Chairman and Ranking Minority Member, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, House of Representatives

Chairman and Ranking Minority Member, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Subcommittee on Labor, Health and Human Services, Education and Related Agencies, Committee on Appropriations, U.S. Senate

Chairman and Ranking Minority Member, Committee on Finance

Chairman and Ranking Minority Member, Subcommittee on Social Security and Family Policy

Chairman and Ranking Minority Member, Senate Special Committee on Aging

Social Security Advisory Board

# Overview of the Office of the Inspector General

The Office of the Inspector General (OIG) is comprised of our Office of Investigations (OI), Office of Audit (OA), Office of the Chief Counsel to the Inspector General (OCCIG), and Office of Resource Management (ORM). To ensure compliance with policies and procedures, internal controls, and professional standards, we also have a comprehensive Professional Responsibility and Quality Assurance program.

## Office of Audit

OA conducts and/or supervises financial and performance audits of the Social Security Administration's (SSA) programs and operations and makes recommendations to ensure program objectives are achieved effectively and efficiently. Financial audits assess whether SSA's financial statements fairly present SSA's financial position, results of operations, and cash flow. Performance audits review the economy, efficiency, and effectiveness of SSA's programs and operations. OA also conducts short-term management and program evaluations and projects on issues of concern to SSA, Congress, and the general public.

## Office of Investigations

OI conducts and coordinates investigative activity related to fraud, waste, abuse, and mismanagement in SSA programs and operations. This includes wrongdoing by applicants, beneficiaries, contractors, third parties, or SSA employees performing their official duties. This office serves as OIG liaison to the Department of Justice on all matters relating to the investigations of SSA programs and personnel. OI also conducts joint investigations with other Federal, State, and local law enforcement agencies.

## Office of the Chief Counsel to the Inspector General

OCCIG provides independent legal advice and counsel to the IG on various matters, including statutes, regulations, legislation, and policy directives. OCCIG also advises the IG on investigative procedures and techniques, as well as on legal implications and conclusions to be drawn from audit and investigative material. Finally, OCCIG administers the Civil Monetary Penalty program.

## Office of Resource Management

ORM supports OIG by providing information resource management and systems security. ORM also coordinates OIG's budget, procurement, telecommunications, facilities, and human resources. In addition, ORM is the focal point for OIG's strategic planning function and the development and implementation of performance measures required by the Government Performance and Results Act of 1993.