OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Audit Report

Mobile Device Security

A-14-14-14051 | September 2014

OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

MEMORANDUM

Date: September 26, 2014 Refer To:

To: The Commissioner

From: Inspector General

Subject: Mobile Device Security (A-14-14-14051)

The attached final report presents the results of our audit. Our objective was to determine whether the Social Security Administration's mobile device security conformed with Federal standards and business best practices to mitigate unauthorized access to the Agency's sensitive information.

If you wish to discuss the final report, please call me or have your staff contact Steven L. Schaeffer, Assistant Inspector General for Audit, at (410) 965-9700.

Patrick P. O'Carroll, Jr.

Attachment

Mobile Device Security
A-14-14-14051

SOCIAL SECURITY ADMINISTRATION
OIG

September 2014 **Office of Audit Report Summary**

Objective

To determine whether the Social Security Administration's (SSA) mobile device security conformed with Federal standards and business best practices to mitigate unauthorized access to the Agency's sensitive information.

Background

While mobile devices allow employees to work from various locations, their mobility makes them susceptible to loss and theft. Recent data indicate that mobile devices are under increasing attack by cyber-criminals exposing them to such risks as theft and introduction of malicious software, potentially disclosing sensitive information.

Given these vulnerabilities, the National Institute of Standards and Technology recommends agencies fully secure each mobile device before allowing a user to access it. Further, organizations should have a mobile device security policy to define what information employees can access with these devices.

Our Findings

We determined that SSA's security of mobile devices did not always conform with Federal standards and business best practices to mitigate unauthorized access to Agency sensitive information. Specifically, we found the Agency lacked a comprehensive, consolidated mobile device policy, did not secure all mobile devices, and provided minimal mobile device security training.

Our Recommendations

We recommend the Agency:

1. Develop a comprehensive, consolidated mobile device policy.
2. Develop and apply standard security configurations for all Agency-issued mobile devices.
3. Enhance annual information technology security awareness training to remind individuals who use mobile devices of their responsibilities, acceptable behavior, and specific risks when using Agency-issued mobile devices.

The Agency agreed with our recommendations.

TABLE OF CONTENTS

ABBREVIATIONS

CIO	Chief Information Officer
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
SP	Special Publication
SSA	Social Security Administration

OBJECTIVE

Our objective was to determine whether the Social Security Administration's (SSA) mobile device security conformed with Federal standards and business best practices to mitigate unauthorized access to the Agency's sensitive information.

BACKGROUND

Mobile devices allow employees to work in various locations.[1] Additionally, mobile devices can access and store large volumes of data. However, the same features that make mobile devices desirable also make them a security challenge. For example, the portable nature of these devices makes them vulnerable to loss or theft.[2] According to recent data, mobile devices are under increasing attack by cyber-criminals. This can expose users and organizations to additional risks, such as theft and malicious software, and potentially disclose sensitive information either on the device or by allowing someone to use the device to remotely access Agency resources.[3] Individuals are using mobile devices for an increasing number of activities and often store sensitive data, such as email, calendars, contact information, and passwords. Moreover, mobile applications for social networking maintain personal information.

Cyber-criminals steal, publicly reveal, or sell personal information extracted from mobile devices. Cyber-criminals also search for information that will improve their chances of social engineering.[4] Cyber-criminals can use personal information, such as contact data for friends and business associates, as a launching pad to access Agency information or resources. [5]

Besides theft, cyber-criminals use malicious software and weaknesses in integrated mobile device features to gain knowledge or access.[6] According to a global leader in information

---

[1] For this review, we considered a mobile device to be a device that is handheld; has at least one wireless network interface for network access; has built-in data storage; and uses an operating system that is not a full-fledged desktop or laptop operating system. This included smartphones, tablets, and feature cellular telephones. We did not include non-feature cellular telephones, laptops, or portable mass storage devices in our review.

[2] According to Symantec, 36 percent of U.S. consumers' mobile devices was lost or stolen in 2010.

[3] According to Symantec, the amount of malicious mobile software continues to rise; there was a 58-percent increase in 2012 compared to 2011; and in 2013, 38 percent of mobile device users had experienced mobile cybercrime.

[4] Social engineering is a technique to trick people into divulging private information to gain unauthorized access to computer systems. Cyber-criminals must learn about the user to create a successful attack. They will research and compile email addresses, professional interests, conferences attended, and websites visited. The cyber-criminal's tools are designed to pull as much data as possible on the mobile device.

[5] Many people do not think a cyber-criminal would target them because they do not have an important enough position within an organization; however, their actions could help attackers. Cyber-criminals start by targeting low-level employees, but as the social network grows, the attack can target technical people, security people and even executives. Lucian Constantin, *Fake social media ID duped security-aware IT guys,* PCWorld, October 31, 2013.

[6] Integrated mobile device features include Bluetooth, camera, Internet access, location services, and text messaging.

security, 50 percent of mobile malicious software created in 2012 attempted to steal information or track movements.[7] A cyber-criminal can also infect a mobile device with a virus. Viruses can spread from infected desktops and laptops to a mobile device when connected through a Universal Serial Bus (USB) port — putting the device and any data it contains at risk.

According to the National Institute of Standards and Technology (NIST), organizations should fully secure each agency-issued mobile device before they allow a user access.[8] Additionally, the Federal Chief Information Officers Council, in conjunction with the Department of Homeland Security, recommends agencies have appropriate protection on agency-issued mobile devices.[9]

SSA's Blackberry smartphones access the Agency's email system and Intranet. Information from the email system may be stored on the Blackberry devices. Non-Blackberry mobile devices can connect to desktop computers. Users can store Agency data on, and move data from, a mobile device by dragging and dropping or by entering the data directly onto the device (for example, using the device's contacts or notes applications).

To accomplish our objective, we tested Blackberry and non-Blackberry mobile devices, and we interviewed device owners to determine whether SSA configured their devices appropriately to mitigate possible threats. We based our configuration checks on Federal standards and business best practices.[10] See Appendix A for additional information about our scope and methodology.

RESULTS OF REVIEW

We determined that SSA's mobile device security did not always conform with Federal standards and business best practices to mitigate unauthorized access to the Agency's sensitive information.[11] SSA did not adequately secure all of its mobile devices, potentially putting Agency data at risk. For example, while SSA stated it had mitigating controls to encrypt files copied to a device, we successfully copied a file to a mobile device without encryption occurring. We believe this occurred because SSA did not have a comprehensive, consolidated

---

[7] Symantec, *Internet Security Threat Report 2013*, April 2013, p. 4.

[8] NIST Special Publication (SP) 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, June 2013, p. vii.

[9] Federal CIO Council and Department of Homeland Security, *Mobile Security Reference Architecture*, May 23, 2013, p. 32.

[10] Federal standards include NIST SP 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, issued June 2013; and NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, issued August 2009. Business best practices include the Chief Information Officers Council's *Government Mobile and Wireless Security Baseline*, issued May 2013.

[11] For the purposes of this review, we considered the following to be sensitive Agency information: personally identifiable information (of the public and SSA staff), staff contact and location information, technology information such as login identifications, passwords, and network data.

policy on mobile devices, lacked configuration guides for all mobile devices, and provided minimal mobile device security training.

Comprehensive, Consolidated Mobile Device Policy

Federal guidelines acknowledge that developing a mobile device policy is a critical task an Agency should perform before it begins using mobile devices.[12] A mobile device security policy should define which types of organizational information can be accessed via mobile devices, which types of mobile devices are permitted to access the organizational information, and how much access mobile devices may have.[13] Furthermore, the Mobile Work Exchange recommends agencies have clearly written policies that provide workers the guidance to use mobile devices safely.[14]

SSA did not have a comprehensive, consolidated mobile device policy. SSA staff stated mobile devices were covered under the Agency's information technology policies. However, these policies did not define the types of Agency information accessible by mobile devices, the types of mobile devices permitted to access agency information, or access level by mobile device users. It is important that SSA define these levels of access, as it allows the Agency to limit the risk it incurs by permitting the most-controlled devices to have the most access and the least-controlled devices to have only minimal access.

Additionally, without clear guidance, employees may not know which policies apply to mobile devices. Although about half of the 17 mobile device users we interviewed stated the devices should only be used for official Government business, none could identify existing information technology policies that applied to mobile devices. We believe this is because SSA inconsistently categorized mobile devices in multiple Agency policies.[15] We believe SSA should develop a comprehensive, consolidated mobile device policy that, at a minimum, includes a definition of mobile devices and uses consistent terminology.[16]

---

[12] NIST SP 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, June 2013, p. 10.

[13] Id.

[14] The Mobile Work Exchange is a public-private partnership focused on demonstrating the value of mobility and telework and serving the emerging educational and communication requirements of the Federal mobile/telework community.

[15] In various policies, SSA categorized mobile devices as telecommunications equipment, personal property, and office equipment. Additionally, the policies used different terminology (for example, they used the terms cell phone, Blackberry, or mobile computing device).

[16] Since the Agency has different brands of mobile devices, we recommend that policy not be brand-specific.

Mobile Device Configuration

A baseline configuration is a documented set of specifications and provides device-specific settings. These settings are intended to mitigate certain risks with mobile devices.

- **Third-Party Applications.** There are Websites that provide third-party applications to download onto a mobile device.[17] These applications could contain malicious code.[18] Federal standards recommend that organizations view unknown third-party mobile device applications as untrustworthy.[19]

- **Location Services.** Location services map devices' physical locations. Mobile devices with location services enabled are at increased risk of targeted attacks. It is easier for attackers to determine where the user and the mobile device are and correlate information about other sources with whom the user associates and the kinds of activities they perform in particular locations.

- **Authentication.** Authentication, such as requiring a passcode before accessing the mobile device, can mitigate risk. If the device does not require authentication, unauthorized users could access Agency data that may be stored on, or accessed by, the mobile device. Agencies should consider requiring that employees establish passcodes on mobile devices.

- **Automatic Wipe.** Devices should automatically wipe after unsuccessful attempts to unlock them.[20] Configuring a mobile device to wipe itself after a specified number of failed attempts at entering a passcode will erase the data and reinitialize the settings to factory defaults.

- **Locked Security Settings.** If users can circumvent mobile devices' established security settings, they may leave the device exposed to vulnerabilities and weaknesses that attackers could exploit.[21] Agencies should assume mobile devices are untrusted unless properly secured and monitored.[22]

---

[17] A third-party application is software provided by someone other than the manufacturer of the device.

[18] There is malicious software online, most of which looks like legitimate applications. One example is a fake storefront for applications that lure users into downloading malicious software. Some malicious software can allow attackers to seize complete control of a mobile device. Last year, there was a steady growth in malicious mobile software.

[19] NIST SP 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, June 2013, p. 5.

[20] Id. at p. 9.

[21] Some users may bypass operating system lockout features to install applications (known as jailbreaking).

[22] NIST SP 800-124 Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, June 2013, p. 4.

Blackberry Devices

SSA centrally manages the Blackberry devices that connect to its network. Through this system, SSA can erase the data and restore the device to factory settings if a Blackberry smartphone is lost or stolen.[23]

SSA's baseline Blackberry configuration disables users' ability to download third-party applications. Of the 4,393 Blackberry mobile devices SSA was managing as of June 2014, 4,097 should have had SSA's baseline configuration.[24] However, we found that 1,234 (about 30 percent) did not. As a result, the devices permitted users to download third-party applications. In addition, the baseline configuration did not disable location services. SSA personnel informed us they are working to change the configuration for these Blackberry devices and expect to complete these changes by the end of Calendar Year 2014.

Non-Blackberry Devices

According to SSA's inventory system, the Agency had approximately 251 non-Blackberry mobile devices—such as smartphones, tablets, and feature cellular telephones[25] —in service as of September 2013.[26] SSA did not have baseline configurations for these mobile devices and could not centrally enforce security controls on them. In addition, SSA could not remotely wipe non-Blackberry mobile devices if they are lost or stolen. We tested 10 non-Blackberry devices and found the following.

- None of the devices had passcodes.
- Only 2 of the 10 devices automatically locked after they were idle for a period.
- None of the devices was configured to wipe data after a certain number of incorrect password attempts.
- One smartphone had a number of third-party applications.
- Location services were not disabled on two feature cellular telephones.
- All the feature cellular telephones allowed users to circumvent security features.
- SSA did not review and configure device settings on eight mobile devices.

---

[23] We did not review the centralized Blackberry management process and therefore cannot conclude on its effectiveness.

[24] The Office of the Inspector General (OIG) had a customized, SSA-approved configuration in use on 296 Blackberry devices. We excluded the OIG from our formal analysis since it is an independent organization within the Agency.

[25] A feature telephone is a cellular telephone with functions above voice calling. For our review, the selected feature telephones had Bluetooth capability and the ability to access the Internet.

[26] The mobile devices had at least one wireless network interface, built-in data storage, and an operating system that was not a full-fledged desktop or laptop operating system.

While the number of non-Blackberry mobile devices is small compared to the number of Blackberry devices, we believe the number of non-Blackberry mobile devices in use at SSA will likely increase.[27] To ensure adequate security and mitigate risks, we believe SSA should develop standard security configuration guides for each type of mobile device the Agency uses.

SSA's Office of Systems, as the primary purchaser of Blackberry smartphones for the Agency, distributed the devices throughout SSA and centrally managed them. However, any component in the Agency could purchase mobile devices (including Blackberry and non-Blackberry devices). By permitting this decentralized procurement, the Agency relied on non-technical staff to configure mobile devices procured outside the Office of Systems.[28] When components procure and deploy mobile devices without the Office of Systems' knowledge or involvement, they could introduce security risks. The unsupported hard- and software were not subject to the same security measures applied to the technologies the Office of Systems supported.

Information Security Awareness Training

SSA's mandatory, annual information security awareness training includes minimal training for mobile devices. To enhance security, the Agency may not be able to enforce directly, SSA should educate mobile device users on the importance of specific mobile device security measures. Additionally, SSA should define in policy and mobile device agreements users' responsibilities for implementing these measures. Rules of behavior specific to mobile devices would strengthen employee awareness of appropriate usage.[29]

CONCLUSIONS

We determined that SSA's mobile device security did not always conform with Federal standards and business best practices to mitigate unauthorized access to the Agency's sensitive information. Specifically, SSA did not have a comprehensive, consolidated mobile device policy or secure all mobile devices, and provided minimal mobile device security training.

[27] SSA has purchased over half of its tablets in the last 2 years.

[28] SSA has decentralized procurement for mobile devices with decentralized responsibility for the security of those devices. SSA does not restrict the types of mobile devices components can procure.

[29] Other Federal agencies – including the Federal Emergency Management Agency, Transportation Security Administration, and U.S. Coast Guard – have developed specific rules of behavior for mobile devices, and provided specific training on acceptable use of mobile devices in addition to general information technology security awareness.

RECOMMENDATIONS

We recommend the Agency:

1. Develop a comprehensive, consolidated mobile device policy.

2. Develop and apply standard security configurations for all Agency-issued mobile devices.

3. Enhance annual information technology security awareness training to remind individuals who use mobile devices of their responsibilities, acceptable behavior, and specific risks when using Agency-issued mobile devices.

AGENCY COMMENTS

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

OTHER MATTERS

To conduct our review, we relied on a mobile device inventory from SSA. During our assessment of the inventory's reliability, we found that SSA's Sunflower Assets Property System contained inaccurate and incomplete information.[30]

SSA policy requires that staff enter sensitive items into the Agency's property management system.[31] The policy specifically identifies cellular telephones and Blackberry smartphones. Additionally, Agency policy requires that custodial officers inventory sensitive property every 3 years.[32] Finally, SSA policy includes a list of sensitive items to be inventoried. This list is specific in brand (Blackberry) and only includes cellular telephones and laptops. SSA does not require that staff inventory all types of mobile devices.

We obtained Blackberry data from SSA's Sunflower Assets Property System as well as the Agency's Blackberry Enterprise System.

---

[30] While the data were incomplete and inaccurate, we found them to be sufficiently reliable for the limited purposes of this review. We did not perform further analysis of the inventory discrepancies as we plan to review the information technology inventory process in the future.

[31] SSA, Administrative Instructions Manual System, M0404 Material Resources, Chapter 04 *Property Management*, Instruction Number 04 *Physical Inventory of Personal Property*, §04.04.02B.

[32] Id. at §04.04.05B.

Table 1: Blackberry Devices Reported in Service

System	Blackberry Devices Reported as in Service
Sunflower Asset Management System (September 2013)	6,615
Blackberry Enterprise System (February 2014)	4,273

We compared the data in the two systems using the devices' serial numbers. We found that only 1,023 of the Blackberry devices recorded in Sunflower as "in service" as of September 2013 were actually connected to SSA's network as of February 2014. Therefore, it appears that

- just over 5,000 Blackberry devices that had actually been taken out of service were incorrectly reported as in service in Sunflower, and
- more than 3,000 Blackberry devices were actually in service but may not have been properly recorded in Sunflower.[33]

[33] We compared data from the two systems using the devices' serial numbers. The serial number was not included in the data we obtained from the Blackberry Enterprise System for 110 devices; therefore, we were unable to determine whether the devices were included in Sunflower.

APPENDICES

Appendix A – SCOPE AND METHODOLOGY

Our objective was to determine whether the Social Security Administration's (SSA) mobile device security conformed with Federal standards and business best practices to mitigate unauthorized access to the Agency's sensitive information.

To accomplish the audit objective we:

- Reviewed applicable Federal guidelines, and standards.
- Reviewed the Chief Information Officers Council and Department of Homeland Security's, *Mobile Security Reference Architecture,* and *Mobile Computing Decision Framework.*
- Reviewed SSA policy and the Information Systems Security Handbook.
- Interviewed SSA subject matter experts including mobile device support staff, custodial officers, and owners of the sampled mobile devices.
- Tested 17 mobile devices and interviewed the users.
- Analyzed Blackberry Enterprise policy data.

We obtained a sufficient understanding of information systems controls as they related to this review. We assessed the completeness, accuracy, and validity of the data from the asset management software. Through our testing, we found that key data elements of the asset management system were inconsistent, inaccurate, and possibly incomplete. Despite these limitations, we believe SSA's asset management system data were sufficiently reliable for the limited use of sampling mobile devices in the Agency.

We conducted our work from September 2013 through May 2014 in Baltimore, Maryland. The entities reviewed were the Offices of Budget, Finance, Quality and Management; Disability Adjudication and Review; Human Resources; Operations; and Systems. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Scope of the Review

The scope of the review was the confidentiality of Agency data.[1] For our review, we considered a mobile device to be hand-held and to have

1. at least one wireless network interface for network access;
2. built-in data storage; and
3. an operating system that is not a full-fledged desktop or laptop operating system.

This included smartphones, tablets, and feature cellular telephones. We did not include non-feature cellular telephones, laptops, or portable mass storage devices in our review.

Blackberry Mobile Device Sample

We selected 50 Blackberry mobile devices from SSA's property management system. Of the 50 "in service" Blackberry mobile devices we sampled, 45 were no longer in use. Because of the inaccuracy of SSA's Sunflower Assets Property system, we could physically test only seven Blackberry mobile devices.[2] We tested a subset of the mobile devices' controls basing our tests on National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 *Recommended Security Controls for Federal Information Systems and Organizations*, NIST SP 800-124 *Guidelines for Managing the Security of Mobile Devices in the Enterprise* and the Chief Information Officers Council's *Mobile Security Reference Architecture*. This testing provided assurance that the data from the Blackberry management software accurately reflected the configuration on the mobile device.

Using the data from the Agency's Blackberry management software, we reviewed the configuration for all Blackberry mobile devices registered. SSA's Blackberry management software registered about 4,100 Blackberry mobile devices in service as of May 2014 that were applicable to our review.

[1] NIST SP 800-124 (page 3). According to NIST, confidentiality is ensuring transmitted and stored data cannot be read by unauthorized parties.

[2] We tested four of the five remaining sampled Blackberry mobile devices. We also tested replacement devices for 3 of the 45 employees whose inventoried device was no longer in use.

Non-Blackberry Mobile Device Sample

The population from which we sampled included Agency-inventoried, non-Blackberry mobile devices within the scope of this review. SSA's asset management software had 251 non-Blackberry mobile devices in service as of September 2013 that were applicable to our review. We categorized the mobile devices into one of the following: non-Blackberry smartphones; feature cellular telephones (have Internet access or Bluetooth capability); and tablet computers.

Table A–1: SSA Mobile Device Inventory as of September 2013[3]

Device	Count	Tested
Non-Blackberry Smartphones	56	3
Feature Cellular Telephones[4]	173	3
Tablet Computers	22	4
TOTAL	251	**10**

We tested 10 non-Blackberry mobile devices. We tested a subset of the mobile devices' controls basing our tests on NIST SP 800-53 *Recommended Security Controls for Federal Information Systems and Organizations*, NIST SP 800-124 *Guidelines for Managing the Security of Mobile Devices in the Enterprise* and the Chief Information Officers Council's *Mobile Security Reference Architecture*.

[3] This inventory did not include mobile devices in the OIG.

[4] A feature telephone is a cellular telephone with functions above voice calling. For our review, the selected feature telephones had Bluetooth capability and the ability to access the Internet.

Appendix B – AGENCY COMMENTS

SOCIAL SECURITY

MEMORANDUM

Date: August 29, 2014 Refer To: S1J-3

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

From: James A. Kissko /s/
Chief of Staff

Subject: Office of the Inspector General Draft Report, "Mobile Device Security" (A-14-14-14051) - INFORMATION

Thank you for the opportunity to review the draft report. Please see our attached comments.

Please let me know if we can be of further assistance. You may direct staff inquiries to Gary S. Hatcher at (410) 965-0680.

Attachment

COMMENTS ON THE OFFICE OF THE INSPECTOR GENERAL DRAFT REPORT, "MOBILE DEVICE SECURITY" (A-14-14-14051)

Recommendation 1

Develop a comprehensive, consolidated mobile device policy.

Response

We agree. While we believe that we address many aspects of mobile device security in various sections of our Information Systems Security Handbook, we will review the relevant sections to determine how best to present this information in a consolidated format. We plan to complete our review no later than December 2014.

Recommendation 2

Develop and apply standard security configurations for all Agency-issued mobile devices.

Response

We agree. We anticipate completing the development of standard security configurations for all agency-issued mobile devices by December 31, 2014. As for non-network mobile devices (i.e., those devices purchased with agency funds, but which are un-managed and restricted from connecting to our network), there are inherent technical limitations. Developing standard security configuration baselines for non-network mobile devices would be cost-prohibitive, and ultimately ineffective because these devices cannot connect to the network to deploy a baseline configuration. We plan to develop guidance for agency purchasers of non-network mobile devices to assist in configuring these devices with minimum mobile safeguards as recommended. We anticipate starting the development of this guidance in September 2014.

Recommendation 3

Enhance annual information technology security awareness training to remind individuals who use mobile devices of their responsibilities, acceptable behavior, and specific risks when using Agency-issued mobile devices.

Response

We agree. We recently released our annual security and awareness training for fiscal year (FY) 2014. We will incorporate mobile device security training in our annual awareness training for FY 2015.

Appendix C – Major Contributors

Jeffrey Brown, Director

Mary Ellen Moyer, Audit Manager

Jan Kowalewski, Auditor in Charge

MISSION

By conducting independent and objective audits, evaluations, and investigations, the Office of the Inspector General (OIG) inspires public confidence in the integrity and security of the Social Security Administration's (SSA) programs and operations and protects them against fraud, waste, and abuse. We provide timely, useful, and reliable information and advice to Administration officials, Congress, and the public.

CONNECT WITH US

The OIG Website (http://oig.ssa.gov/) gives you access to a wealth of information about OIG. On our Website, you can report fraud as well as find the following.

- OIG news
- audit reports
- investigative summaries
- Semiannual Reports to Congress
- fraud advisories
- press releases
- congressional testimony
- an interactive blog, "Beyond The Numbers" where we welcome your comments

In addition, we provide these avenues of communication through our social media channels.


Watch us on YouTube


Like us on Facebook


Follow us on Twitter


Subscribe to our RSS feeds or email updates

OBTAIN COPIES OF AUDIT REPORTS

To obtain copies of our reports, visit our Website at http://oig.ssa.gov/audits-and-investigations/audit-reports/all. For notification of newly released reports, sign up for e-updates at http://oig.ssa.gov/e-updates.

REPORT FRAUD, WASTE, AND ABUSE

To report fraud, waste, and abuse, contact the Office of the Inspector General via

Website:	http://oig.ssa.gov/report-fraud-waste-or-abuse
Mail:	Social Security Fraud Hotline P.O. Box 17785 Baltimore, Maryland 21235
FAX:	410-597-0118
Telephone:	1-800-269-0271 from 10:00 a.m. to 4:00 p.m. Eastern Standard Time
TTY:	1-866-501-2101 for the deaf or hard of hearing