OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

Congressional Response Report

The Social Security Administration's Compliance with Congressional Requests and Electronic Message Requirements

A-01-18-50599 | August 2017

OIG Office of the Inspector General
SOCIAL SECURITY ADMINISTRATION

August 8, 2017

The Honorable Claire McCaskill
Ranking Member, Committee on
Homeland Security and Governmental Affairs
United States Senate
Washington, DC 20515

The Honorable Tom Carper
Member, Committee on
Homeland Security and Governmental Affairs
United States Senate
Washington, DC 20515

Dear Ms. McCaskill and Mr. Carper:

In a June 8, 2017 letter, you asked that we answer six questions related to the Social Security Administration's compliance with congressional requests and electronic message requirements. This report answers the six questions.

To ensure the Agency is aware of the information provided to your office, we are forwarding a copy of this report to the Agency. If you have any questions concerning this matter, please call me or have your staff contact Walter Bayer, Congressional and Intragovernmental Liaison, at (202) 358-6319.

Sincerely,

Gale Stallworth Stone

Gale Stallworth Stone
Acting Inspector General

Enclosure

cc:
Nancy A. Berryhill, Acting Commissioner of Social Security
Ron Johnson, Chairman, Committee on Homeland Security and Governmental Affairs

The Social Security Administration's Compliance with Congressional Requests and Electronic Message Requirements A-01-18-50599

Objective

To answer six questions related to the Social Security Administration's (SSA) compliance with congressional requests and electronic message requirements.

Background

On June 8, 2017, Senators McCaskill and Carper of the Committee on Homeland Security and Governmental Affairs, requested we answer six questions related to SSA's compliance with congressional requests and electronic message requirements.

To answer these questions, on June 21, 2017, we sent a survey to 186 SSA employees—with a request for a response by June 27, 2017. We reviewed the responses sent by 111 employees (60 percent). We also reviewed SSA's policies and procedures, prior Office of the Inspector General reports, and allegations made to our Hotline.

Results of Review

None of the responders to our survey indicated they delayed or withheld information to Congress or used unauthorized software to automatically delete electronic messages. Also, our review of allegations to our Hotline did not identify any issues. Furthermore, SSA has policies and procedures in place related to responding to congressional requests and capturing and retaining electronic messages in accordance with Federal law.

TABLE OF CONTENTS

ABBREVIATIONS

AIMS	Administrative Instructions Manual System
CY	Calendar Year
GAO	Government Accountability Office
NARA	National Archives and Records Administration
OIG	Office of the Inspector General
SSA	Social Security Administration

OBJECTIVE

Our objective was to answer six questions related to the Social Security Administration's (SSA) compliance with congressional requests and electronic message requirements.

BACKGROUND

On June 8, 2017, Senators McCaskill and Carper, Committee on Homeland Security and Governmental Affairs, requested that we answer six questions related to SSA's compliance with congressional requests and electronic message requirements. See Appendix A for the request.

The U.S. National Archives and Records Administration (NARA) is authorized to promulgate regulations for Federal records (which can include electronic messages). Federal agencies—such as SSA—are required to institute records management programs.

On July 29, 2015, NARA provided Federal agencies guidance[1] on how to comply with Federal law[2] regarding the preservation of electronic messages. Additionally, on March 15, 2017, NARA issued a memorandum to Federal agencies that addressed, among other things, electronic messaging and encrypted messages. The memorandum stated that, "Agencies are responsible for properly managing electronic messages that are Federal records, whether they are SMS [short message services] texts, encrypted communications, direct messages on social media platforms, email, or created on any other type of electronic messaging system or account."[3]

To answer the Senators' questions, we sent a survey to 186 employees—148 senior executive service officials at SSA and 38 staff in the Agency's Office of Legislation and Congressional Affairs. Of the 186 employees who received the survey, 111 responded—a 60-percent response rate.[4] See Appendix B for the survey.

---

[1] NARA, *Guidance on Managing Electronic Records*, Bulletin 2015-02, (July 29, 2015).

[2] The *Federal Records Act* defines Federal records as any material that is recorded, made, or received during Federal business, regardless of its form or characteristics, and is preserved or worthy of preservation because it evidences ". . . the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of data in them . . . ." *Federal Records Act*, 44 U.S.C. § 3301(a) (2014). Also, see 44 U.S.C. § 2911(a) (2014) regarding the use of non-official electronic messaging accounts for official business. A record using non-official electronic messaging accounts needs to be copied or forwarded to an official electronic message account no later than 20 days after the original creation or transmission of the record.

[3] NARA, *Records Management Priorities for 2017*, p. 2 (March 15, 2017).

[4] According to Government Accountability Office (GAO) guidelines, to make plausible generalizations, the effective response rate should usually be at least 75 percent. GAO, *Developing and Using Questionnaires*, GAO-PEMD -10.1.7, p. 185 (October 1993). Because of the short time frame to respond to the congressional request, we did not follow-up with the non-responders to obtain a 75-percent response rate. Also, since the survey was only open for 5 workdays, employees may not have been able to respond because they were out of the office. Employees may have also chosen to not respond to the survey since it was not anonymous or for some other reason.

We also reviewed SSA's policies and procedures, prior Office of the Inspector General (OIG) reports, and allegations made to our Hotline. See Appendix C for additional information on our scope and methodology.

RESULTS OF REVIEW

The answers to the Committee's questions are below.

Question 1: Since January 20, 2017, has any Administration official directed or advised any agency employee to delay or withhold a response to a Congressional request for information?

We did not identify any allegations to our Hotline—from January to June 2017—indicating that officials directed or advised SSA employees to delay or withhold a response to a congressional request for information. Furthermore, the list of outstanding requests[5] referenced in the congressional letter did not identify any related to SSA. Also, none of the 111 employees who responded to our survey said anyone had directed them to delay or withhold a response to a congressional request for information since January 2017. We also asked about delaying or withholding responses in Calendar Year (CY) 2016, and again, no employees who responded to the survey said they had been told to delay or withhold information to Congress.

It is SSA's policy to answer all congressional requests promptly.[6] Each SSA component is responsible for managing its own activities related to congressional inquiries. Furthermore, SSA does not have a system that tracks the progress of *all* congressional requests.

Although SSA's handling of congressional inquiries is decentralized, its Office of Legislation and Congressional Affairs has Agency-wide responsibility for

- establishing and maintaining effective relations with Congress,
- providing support services to individual members of Congress and their staffs in Washington, D.C.,
- responding to congressional inquiries concerning legislative policy and issues, and
- providing guidance and assistance to other SSA offices and components in all aspects of maintaining an effective congressional relations program.[7]

[5] See Appendix A, page A-3, for the Senators reference to this list.

[6] SSA, AIMS, Administrative Management Communications, Ch. 01.03, sec. 01.03.03-04(A) (September 2, 2016).

[7] SSA, AIMS, Administrative Management Communications, Ch. 09.14, sec. 09.14.03(C)-(D) (April 18, 2008).

Question 2: Since January 20, 2017, has any Administration official directed or advised any agency employee or Congressional staff member that the agency will only provide requested documents or information to a Committee chair?

We did not identify any allegations to our Hotline—from January to June 2017—indicating that officials directed or advised SSA employees to only provide requested documents or information to a Committee Chair. Also, none of the 111 employees who responded to our survey indicated this was an issue. We also asked about any instances in CY 2016 where employees were told to only provide information to a Committee Chair, and, again, no employees who responded to the survey said they had been told to do this.

Question 3: Since January 20, 2017, has the Administration issued any guidance related to the use of smartphone applications that support encryption or the ability to automatically delete messages after they are read or sent for work related communications?

None of the 111 responders to our survey indicated they had received guidance from the Administration related to the use of smartphone applications that support the ability to automatically delete messages after they are read or sent for work-related communications. Also, we did not identify any allegations to our Hotline related to this.

SSA policy requires that data on mobile computers/devices and removable media be encrypted unless the data are deemed to be non-sensitive by the SSA Deputy Commissioner, or their designee, in writing.[8] Furthermore, the encryption method employed must meet acceptable encryption standards designated by the National Institute of Standards & Technology.[9]

[8] SSA, Office of Information Security, *Information Security Policy for the Social Security Administration*, version 6.5, sec. 6.3.1 (July 17, 2017).

[9] SSA, Office of Information Security, *Information Security Policy for the Social Security Administration*, version 6.5, sec. 6.3.1 (July 17, 2017).

SSA policy also includes guidance on the different types of electronic messages—including messages sent using smartphones. For example, SSA's policy states that, if an employee uses Agency equipment, such as a BlackBerry, to create a Federal record while text messaging, the employee is required to copy the conversation into an email and send it to his/her SSA email account within 20 days after the original creation or transmission of the record to comply with the requirements in the *Presidential and Federal Records Act Amendments of 2014*.[10] The policy also states

> Although employees should only use agency email and other agency issued electronic messaging devices to conduct agency business, should you, in the rarest of circumstances or emergencies have to use a personal device or account to conduct agency business, or when an employee is initially contacted through a personal account, you must follow the requirements in the *Presidential and Federal Records Act Amendments of 2014*.[11]

Additionally, SSA policy states that, if an employee uses instant messages to create a Federal record, the employee must copy the entire conversation into an email and send the email to his/her SSA email account before closing the conversation. If the employee fails to follow instructions and creates a Federal record using a personal instant message service, the employee must forward the entire conversation to his/her SSA email account within 20 days after the original creation or transmission of the record.[12] Furthermore, the policy states

> Generally, electronic messages, such as chat (instant messaging software), text messages, social media communications, and voicemails mostly contain transitory information or information of value for a short period. SSA must manage any Federal records created while using electronic messaging systems in compliance with Federal records management laws, regulations, and policies.[13]

SSA implemented a new system that captures and retains all emails based on an employee's position. At SSA, for certain positions, emails are captured and retained for 7 years and then deleted. For other positions, emails are captured and retained for 15 years and then transferred to NARA for permanent preservation.[14] The system is designed to comply with Federal law and NARA guidance. However, the system only relates to emails sent and received from ssa.gov accounts and does not automatically capture and retain text or instant messages. Therefore, SSA relies on employees to follow its policy to forward electronic messages that are considered Federal records to their SSA email accounts so these types of messages will then be automatically captured and retained for the appropriate period of time. However, in July 2017,

---

[10] 44 U.S.C. § 2911(a); SSA, AIMS, Records Management, Ch. 7.02, sec. 07.02.04(2) (March 29, 2016).

[11] SSA, AIMS, Records Management, Ch. 7.02, sec. 07.02.04(1)(C) (March 29, 2016).

[12] SSA, AIMS, Records Management, Ch. 7.02, sec. 07.02.04(3) (March 29, 2016).

[13] SSA, AIMS, Records Management, Ch. 7.02, sec. 07.02.03 (March 29, 2016).

[14] SSA, AIMS, Records Management, Ch. 7.07 (December 16, 2016).

SSA informed us it was developing a system to automatically manage instant messages and was planning to develop similar systems for other non-email type electronic messages.

Question 4: Since January 20, 2017, has any Administration official used, for work-related communications, a smartphone app, including, but not limited to, WhatsApp, Signal, Confide, and others that support encryption or the ability to automatically deleted messages after they are read or sent?

None of the 111 responders to our survey indicated they had used unauthorized software—such as WhatsApp, Signal, or Confide—to automatically delete electronic messages after they are read or sent for work related communications. Also, we did not identify any allegations to our Hotline related to this.

Mobile devices SSA issues to employees are configured with an authorized encryption application and certain authorized applications, which do not include WhatsApp, Signal, Confide, or other applications that would automatically delete electronic messages after they are read.

In an October 2013 report,[15] we noted that some of the hardware devices connected to SSA's network were not appropriately configured. We recommended SSA ensure only approved and properly configured hardware devices connect to its network, revise its policy, and ensure hardware devices identified in that audit had proper configurations. SSA agreed with the recommendations and informed us it took steps to implement them.

In a September 2014 report,[16] we noted that SSA did not properly configure all its mobile devices. Specifically, we found

- unauthorized applications and a restricted feature (location services) enabled on 1,234 (30 percent) of 4,097 Blackberry devices, and
- none of the 251 non-Blackberry devices (such as smartphones and tablets) had policy-compliant configurations. We tested 10 of the 251 non-Blackberry devices, and 1 had various unauthorized applications.

At the time of that audit, SSA did not have a comprehensive, consolidated mobile device policy and provided minimal mobile device security training. Additionally, SSA did not have standard configurations for non-Blackberry devices. Therefore, we recommended SSA develop its mobile device policy, update its annual training on information security awareness to include information on mobile device policy, and develop and apply standard security configurations for all Agency mobile devices. SSA agreed with these recommendations.

---

[15] SSA, OIG, *The Social Security Administration's Process to Identify and Monitor the Security of Hardware Devices Connected to its Network, A-14-13-13050* (October 2013).

[16] SSA, OIG, *Mobile Device Security, A-14-14-14051* (September 2014).

SSA informed us that as of 2015 the Agency had fully implemented the first two recommendations. However, for the third recommendation, it had *only* developed and applied standard security configurations for the Blackberry devices. SSA explained it could not develop and apply standard security configurations for the non-Blackberry devices because it would be cost-prohibitive and ultimately ineffective since these devices could not connect to the network to deploy the baseline configuration. Furthermore, during our current audit, SSA informed us that it checked its Blackberry device settings and discovered it had inadvertently turned the location services feature back on in these devices during a system's upgrade. In July 2017, the Agency was reviewing its procedures to ensure they required staff to check whether the location services feature in its Blackberry devices was still turned off after a systems upgrade.

Question 5: Since January 20, 2017, has any Administration official failed to abide by federal law and/or NARA or Departmental guidance regarding preservation of electronic records related to official business, including, but not limited to, text messages, chats, instant messages, social media messages, or emails created on non-government accounts?

None of the 111 responders to our survey indicated they failed to abide by Federal law and/or NARA or SSA guidance regarding preserving electronic records related to official business. Also, we did not identify any allegations to our Hotline related to this.

SSA must retain and dispose of these records in accordance with the appropriate NARA-approved records schedule that mandates the retention period for a particular group of records.[17] It also mandates whether the Agency is to destroy those records or transfer them to NARA for permanent preservation after the retention period. See answers to Questions 3 and 4 related to SSA policies and procedures for capturing and retaining electronic records related to Agency business.

Question 6: Has the OIG previously provided recommendations to the Administration regarding its management of the preservation of electronic records and compliance with Congressional document requests? If so, please provide a list of any OIG recommendations that remain outstanding.

In February 2016,[18] we made six recommendations to SSA related to its management of electronic messages. In December 2016, SSA considered all the recommendations to have been implemented. Table 1 lists the recommendations and their status as of June 2017.

---

[17] SSA, AIMS, Records Management, Ch. 7.02, sec. 07.02.03(8)-(9) (March 29, 2016).

[18] SSA, OIG, *The Social Security Administration's Management of Electronic Message Records, A-14-15-25025* (February 2016).

Table 1: OIG Recommendations

Recommendation	Status
Revise Agency policies and procedures to ensure they reflect Federal law, regulations, and official guidance on the proper identification, capture, retention, and disposition of all types of electronic message records.	SSA updated its policy and procedures in March 2016.[19]
Clarify Agency policies and procedures related to the acceptable use of personal email accounts to conduct official business.	SSA updated its policy and procedures in March 2016.[20]
Develop and implement standards for storing and backing up Federal email records to protect them from loss and ensure they may be recovered if deleted.	SSA implemented a new system between June and December 2016 that captures and retains all emails based on an employee's position. For certain positions, emails are captured and retained for 7 years at SSA and then deleted. For other positions, emails are captured and retained for 15 years at SSA and then transferred to NARA.[21]
Retain the emails of at least the high-level officials who are most likely to create permanent records.	SSA implemented a new system between June and December 2016. Phase 1 of the system's implementation was in June 2016 when the Agency started automatically capturing and retaining all emails for high-level SSA officials. Emails for high-level officials are automatically captured and retained for 15 years at SSA and then transferred to NARA.[22]
Strengthen the Records Management Coordinators' oversight activities to ensure SSA complies with Federal requirements.	SSA updated the Record Management Coordinators' roles and responsibilities to include oversight activities. SSA also updated policies and procedures and implemented a system to capture and retain emails.[23]
Develop comprehensive Agency-wide records management training specific to electronic messages (including email messages and instant messages).	SSA updated the mandatory records management training video to include information about electronic messaging. SSA made the training available to staff on May 16, 2016. An updated training video, *Records Management Training for Employees*, was released in June 2017.

[19] SSA, AIMS, Records Management, Ch. 7.02 (March 29, 2016).

[20] SSA, AIMS, Records Management, Ch. 7.02 (March 29, 2016).

[21] SSA, AIMS, Records Management, Ch. 7.07 (December 16, 2016).

[22] SSA, AIMS, Records Management, Ch. 7.07 (December 16, 2016).

[23] SSA, AIMS, Records Management, Ch. 7.01 (August 23, 2016).

CONCLUSIONS

None of the responders to our survey indicated they delayed or withheld information to Congress or used unauthorized software to automatically delete electronic messages. Also, our review of allegations to our Hotline did not identify any issues. Furthermore, SSA has policies and procedures in place related to responding to congressional requests and capturing and retaining electronic messages in accordance with Federal law.

AGENCY COMMENTS

SSA has policies and procedures in place related to responding to congressional requests and capturing and retaining electronic messages in accordance with Federal law; see Appendix D.

Rona Lawson
Assistant Inspector General for Audit

APPENDICES

Appendix A – Letter From Congress

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS
WASHINGTON, DC 20510–6250

June 8, 2017

Ms. Gale Stallworth Stone
Acting Inspector General
Social Security Administration
6401 Security Boulevard
Baltimore, MD 21235

Dear Acting Inspector General Stallworth Stone:

We write today to request that the Office of the Inspector General (OIG) conduct a review of the Social Security Administration's processes and compliance with applicable legal standards for preserving certain electronic records as federal records, and cooperation with Congressional document requests.

Preservation of Electronic Records

In 2014, Congress amended the Presidential Records Act and the Federal Records Act (FRA) regarding the preservation, storage, and management of federal records. The National Archives and Records Administration (NARA) also provided federal agencies with specific guidance on how to comply with federal law regarding the preservation of electronic messages in Bulletin 2015-02, "Guidance on Managing Electronic Records".[1] Pursuant to 44 U.S.C. § 2911, agencies have additional requirements to manage records created or received in nonofficial and personal electronic messaging accounts.[2] NARA plays an essential role in preserving our history as the nation's federal record-keeper, and the Archivist of the United States, as head of NARA, has final authority on how agencies must preserve electronic records as federal records.[3] NARA recently surveyed the FRA compliance of federal agencies, and noted that many agencies "reported having difficulty identifying electronic messages that are records."[4]

---

[1] U.S. National Archives and Records Administration, Electronic Messages White Paper (Aug. 2016) (online at https://www.archives.gov/files/records-mgmt/resources/emessageswp.pdf).

[2] 44 U.S.C. § 2911.

[3] Presidential and Federal Records Act Amendments of 2014, Pub. L. No. 113-187, 128 Stat. 2203.

[4] U.S. National Archives and Records Administration, Electronic Messages White Paper (Aug. 2016) (online at https://www.archives.gov/files/records-mgmt/resources/emessageswp.pdf).

Although NARA has confirmed that the capture of electronic messages creates unique challenges throughout government, various public reports raise questions about whether Trump Administration officials are intentionally skirting compliance with federal record keeping requirements. For example, *The Independent* recently reported that White House staffers are using a "confidential messenger" app called "Confide" that deletes messages once they have been opened, leaving no record of them or their content thereafter.[5] Confide messages cannot be printed or archived and the company indicates that "Even we at Confide cannot decrypt or see any messages."[6] The app allows users to transmit text messages, photos, documents, and voice messages, and provides two forms of screenshot protection, which prevents recipients of an image from taking a screenshot of it. Use by federal employees of private messenger applications, such as Confide, to conduct official business flies in the face of federal recordkeeping laws and the principles of government transparency.

In response to these reports, on March 7, 2017, we wrote to the Archivist of the United States seeking information regarding any guidance NARA has provided to Trump Administration officials, as well as the Trump Administration's compliance with records preservation laws.[7] Archivist David Ferriero provided a detailed response to our letter and included copies of Presidential Records Act (PRA) guidance provided by NARA to the Office of the White House Counsel in a February 2, 2017 briefing on PRA compliance.[8] According to the Archivist's response letter, NARA was not in a position to answer our questions regarding whether officials at federal agencies used any smartphone apps, such as Confide, for work-related communications, or whether any government official at federal agencies have been instructed to avoid using email as a method of work-related communication.

Following the transmittal of our letter to Archivist Ferriero, NARA issued a memo on March 15, 2017, "to all Senior Agency Officials for Records Management that addresses, among other things, 'Electronic Messaging and Encrypted Messages.'"[9] Archivist Ferriero's memo reiterates that "agencies are responsible for properly managing electronic messages that are Federal records whether they are SMS texts, encrypted communications, direct messages on social media platforms, email or created on any other type of electronic messaging system or

---

[5] *Donald Trump's White House Staff 'Communicate Through App Which Automatically Deletes Messages'*, The Independent (Feb. 15, 2017) (online at http://www.independent.co.uk/news/world/americas/us-politics/donald-trump-white-house-staff-confide-communicate-app-auto-delete-messages-leaks-russia-us-a7581046.html).

[6] Frequently Asked Questions, Confide (online https://getconfide.com/faq) (accessed on Feb. 17, 2017).

[7] Letter from Sen. Claire McCaskill, Ranking Member, Senate Committee on Homeland Security and Governmental Affairs and Sen. Tom Carper to David Ferriero, Archivist of the United States (Mar. 7, 2017).

[8] Letter from David Ferriero, Archivist of the United States to Sen. Claire McCaskill, Ranking Member, Senate Committee on Homeland Security and Governmental Affairs and Sen. Tom Carper (Mar. 30, 2017).

[9] *Id.*

account."[10] The Archivist's memo also addressed the recent "news stories referring to the possible use by government employees of non-official, commercial communication applications such as WhatsApp, Signal, Confide, and others that support encryption or the ability to automatically delete messages after they are read or sent."[11] Archivist Ferriero advised federal agencies that:

> Any use of such communication applications requires coordination with your legal counsel and records management officials to ensure compliance with the Federal Records Act and related regulations. Agencies are responsible for setting policies that govern the use of these applications prior to their deployment and must take steps to manage and preserve records created through their use for as long as required.[12]

Cooperation with Congressional Requests

Reports that Trump Administration officials have used practices that undermine transparency of public records are also unfortunately consistent with this Administration's problematic pattern of delaying or ignoring requests from minority Members of Congress. For example, on March 15, 2017, Senate Democrats released a list of more than 100 oversight request letters that Trump Administration officials had not answered.[13] Among those unanswered requests was a letter we sent to Donald McGahn, Counsel to the President, regarding White House officials' use of private email accounts.[14] The list also included outstanding requests to a range of Trump Administration officials at various federal agencies, including Attorney General Sessions, Secretary of State Tillerson, Environmental Protection Agency Administrator Pruitt, Secretary of Defense Mattis, and Secretary of Commerce Ross, among others.

While it might be reasonable to attribute some delay in responding to Congressional requests to the presidential transition process, recent reports suggest that the Trump Administration's lack of transparency and responsiveness may be by design. For example, a January 20, 2017, memo from the Acting Secretary of Health and Human Services (HHS) to agency staff prohibit the dissemination of any "correspondence to public officials (e.g., Members of Congress, Governors) or containing interpretation or statements of Department regulations or

---

[10] Memorandum from David Ferriero, Archivist of the United States to Senior Agency Officials for Records Management re: Records Management Priorities for 2017 (March 15, 2017).

[11] *Id.*

[12] *Id.*

[13] Sen. Sheldon Whitehouse, *Senate Democrats Release List of Over 100 Oversight Letters President Trump Refuses to Answer* (Mar. 15, 2017) (online at https://www.whitehouse.senate.gov/news/release/senate-democrats-release-list-of-over-100-oversight-letters-president-trump-refuses-to-answer).

[14] *Id.*

policy, unless specifically authorized by me [the Acting Secretary]" or a designee.[15] Most recently, Senator Carper noted, regarding GSA's lack of responsiveness to congressional requests for information on the Trump Organization's lease with the General Services Administration (GSA) to redevelop and manage the Old Post Office building, that, effective January 20, 2017, the Trump Administration appeared to have changed GSA's "long-standing practice of providing certain documents requested by minority members of congress, including the ranking member of the committee of jurisdiction with direct oversight."[16] During a recent bipartisan briefing with GSA, "agency personnel stated that its new practice only assures that [requested] documents will be provided to the committee's chairman."[17] Additionally, *Politico* recently reported that during meetings this spring with senior officials for various federal agencies, a Deputy Counsel and Special Assistant to the President, "told agencies not to cooperate" with congressional oversight requests from Democrats.[18] These newly-implemented policies are deeply troubling and may also run afoul of several laws that prohibit interference with federal employees' ability to communicate with Congress, including, but not limited to the Whistleblower Protection Enhancement Act, Section 713 of the Consolidated Appropriations Act of 2016, as well as 5 U.S.C.§ 7211.

In order to better understand the Administration's compliance with federal laws governing records retention and compliance with Congressional requests and federal recordkeeping requirements for electronic messages, we ask that you conduct a review and provide a written response not later than July 6, 2017, which addresses the following questions:

1. Since January 20, 2017, has any Administration official directed or advised any agency employee to delay or withhold a response to a Congressional request for information? If any such directive is in writing, please provide a copy.

2. Since January 20, 2017, has any Administration official directed or advised any agency employee or Congressional staff member that the agency will only provide requested documents or information to a Committee chair? If any such directive is in writing, please provide a copy.

3. Since January 20, 2017, has the Administration issued any guidance related to the use of smartphone applications that support encryption or the ability to automatically delete messages after they are read or sent for work related communications?

---

[15] Memorandum from Acting Secretary, U.S. Department of Health and Human Services to HHS OPDIVHeads and StaffDiv Heads (Jan. 20, 2017).

[16] Senator Tom Carper, *Carper Statement on Trump Hotel Lease* (Mar. 31, 2017) (online at https://www.carper.senate.gov/public/index.cfm/pressreleases?ID=77B68657-FD23-4902-9A64-AE1314F64EAF).

[17] *Id.*

[18] *White House Orders Agencies to Ignore Democrats' Oversight Requests*, Politico (June 2, 2017) (online http://www.politico.com/story/2017/06/02/federal-agencies-oversight-requests-democrats-white-house-239034).

4. Since January 20, 2017, has any Administration official used, for work-related communications, a smartphone app, including, but not limited to, WhatsApp, Signal, Confide, and others that support encryption or the ability to automatically delete messages after they are read or sent?

5. Since January 20, 2017, has any Administration official failed to abide by federal law and/or NARA or Departmental guidance regarding preservation of electronic records related to official business, including, but not limited to, text messages, chats, instant messages, social media messages, or emails created on non-government accounts?

6. Has the OIG previously provided recommendations to the Administration regarding its management of the preservation of electronic records and compliance with Congressional document requests? If so, please provide a list of any OIG recommendations that remain outstanding.

If you or members of your staff have any questions about this request, please feel free to ask your staff to contact Donald Sherman with Ranking Member McCaskill's office at 202-224-2627 or Roberto Berrios with Senator Carper's office at 202-224-2441. Please send any official correspondence relating to this request to Amanda_Trosen@hsgac.senate.gov. Thank you very much for your attention to this matter.

Sincerely,

Claire McCaskill
Ranking Member

Tom Carper
United States Senator

cc: The Honorable Ron Johnson
Chairman

Appendix B – Office of the Inspector General Survey

On June 21, 2017, we issued a survey with the questions below to the Social Security Administration (SSA) senior executive service officials as well as staff in SSA's Office of Legislation and Congressional Affairs—with a request for responses by June 27, 2017.[1]

- In Calendar Year (CY) 2016, did anyone direct you to delay a response to a congressional request for information? Yes or No.
- In CY 2017, did anyone direct you to delay a response to a congressional request for information? Yes or No.
- In CY 2016, did anyone direct you to withhold a response to a congressional request for information? Yes or No.
- In CY 2017, did anyone direct you to withhold a response to a congressional request for information? Yes or No.
- In CY 2016, did anyone direct you to only provide requested documents or information to a congressional committee chairperson? Yes or No
- In CY 2017, did anyone direct you to only provide requested documents or information to a congressional committee chairperson? Yes or No
- Since January 20, 2017, has anyone directed you to use WhatsApp, Signal, Confide, or any other application to circumvent SSA's normal procedures for sending or retaining electronic messages? Yes or No
- Since January 20, 2017, have you used WhatsApp, Signal, Confide, or any other application to circumvent SSA's normal procedures for sending or retaining electronic messages? Yes or No.
- Since January 20, 2017, have you followed the Federal laws regarding retention of work-related electronic records, such as text messages, chats, instant messages, social media messages, or emails created on non-government accounts? Yes or No.
- Since January 20, 2017, have you followed the National Archives and Records Administration requirements regarding retention of work-related electronic records, such as text messages, chats, instant messages, social media messages, or emails created on non-government accounts? Yes or No.
- Since January 20, 2017, have you followed SSA guidance regarding retention of work-related electronic records, such as text messages, chats, instant messages, social media messages, or emails created on non-government accounts? Yes or No.
- Please provide any comments.

[1] We only held the survey open for 5 days because of the short timeframe for a response to the congressional request.

Appendix C – SCOPE AND METHODOLOGY

To answer the congressional questions, we:

- Reviewed Social Security Administration (SSA) policies and procedures.
- Reviewed National Archives and Records Administration policies.
- Reviewed prior Office of the Inspector General (OIG) reports.
- Reviewed the OIG Hotline allegations from January 20 through June 2017 for allegations related to electronic messages, records retention policies, or not responding to congressional requests.
- Obtained and/or confirmed information with SSA regarding its procedures for congressional requests, configuring mobile devices, and capturing and retaining non-email type electronic messages (such as instant messages and texts) that may be considered Federal records.
- Conducted an online survey with SSA senior executive service officials and staff in SSA's Office of Legislation and Congressional Affairs. (See Appendix B for the survey questions.)
    - On June 21, 2017, we sent the survey by email to SSA's e-mail distribution list for senior executive service officials[1] as well as 38 staff in the Office of Legislation and Congressional Affairs with a request for a reply by June 27, 2017. The survey was not anonymous since we wanted to be able to follow-up on responses, if necessary. Also, we did not send any follow- up emails to encourage employees to respond since the survey was only open for 5 work days.
    - We summarized the survey results and concluded there were no issues. We adjusted 7 of the 111 responses[2] based on the responders comments or our follow- up contact with them. For example, a responder answered "yes" to questions about delaying responses to Congress. However, the responder included comments that the delay was caused by the need to (a) obtain and verify data, (b) review the response for accuracy, and (c) ensure the release of the information was in compliance with *Privacy Act* restrictions related to the release of personal beneficiary information to Congress. Since the survey responder had a reasonable explanation for the delayed response to Congress, we concluded there was no issue with this response to our survey.

[1] As of June 2017, SSA had 148 senior executive service officials.

[2] The 111 responses represented a 60-percent response rate. However, because of the short time frame to respond to the congressional request, we did not follow-up with the non-responders to obtain a 75-percent response rate—which is generally considered the response rate needed to make plausible generalizations. GAO, *Developing and Using Questionnaires*, GAO-PEMD -10-1.7, p. 185 (October 1993). Because the survey was only open for 5 workdays, employees may not have been able to respond because they were out of the office. Employees may have also chosen to not respond to the survey since it was not anonymous or for some other reason.

Because of the limited timeframe to respond to the congressional request, we did not conduct any testing to determine whether employees used unauthorized electronic messaging applications. Instead we relied on the work completed from the two audits listed below.

1. *The Social Security Administration's Process to Identify and Monitor the Security of Hardware Devices Connected to its Network*, *A-14-13-13*050 (October 2013).

2. *Mobile Device Security*, *A-14-14-14051* (September 2014).

Additionally, because of the limited timeframe to conduct this review and SSA's decentralized structure for responding to congressional requests, we did not sample and review SSA responses to congressional requests to determine whether responses were delayed or withheld. We relied on our review of SSA's policies and procedures, the survey responses, answers to questions we provided to SSA, and our review of the list of pending requests cited in the congressional letter.[3]

We conducted our review between June and July 2017. Other than the limitations noted in this Appendix, 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 findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

[3] See Appendix A, page A-3, for the Senators reference to this list.

Appendix D– AGENCY COMMENTS

SOCIAL SECURITY

MEMORANDUM

Date: August 3, 2017 Refer To: S1J-3

To: Rona Lawson
Assistant Inspector General for Audit

From: Stephanie Hall
Acting Deputy Chief of Staff

Subject: Office of the Inspector General Draft Congressional Response Report, "The Social Security Administration's Compliance with Congressional Requests and Electronic Message Requirements" (A-01-18-50599)--INFORMATION

Thank you for the opportunity to review the draft report. We have policies and procedures in place related to responding to congressional requests and capturing and retaining electronic messages in accordance with Federal law. We have no further comment.

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

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 (https://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 https://oig.ssa.gov/audits-and-investigations/audit-reports/all. For notification of newly released reports, sign up for e-updates at https://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:	https://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