



UNITED STATES DEPARTMENT OF EDUCATION  
OFFICE OF INSPECTOR GENERAL

THE INSPECTOR GENERAL

July 14, 2017

The Honorable Claire McCaskill  
Ranking Member  
Committee on Homeland Security  
and Governmental Affairs  
United States Senate  
340 Dirksen Senate Office Building  
Washington, D.C. 20510

The Honorable Tom Carper  
Committee on Homeland Security  
and Governmental Affairs  
United States Senate  
340 Dirksen Senate Office Building  
Washington, D.C. 20510

Dear Ranking Member McCaskill and Senator Carper:

Thank you for your June 8, 2017, letter requesting that the U.S. Department of Education (Department) Office of Inspector General conduct a review of the Department's processes and compliance with applicable legal standards for preserving certain electronic records as Federal records, and cooperation with Congressional information requests. Enclosed with this letter you will find the results of our analysis.

If you have any questions or if you need any additional information, please do not hesitate to contact me directly at (202) 245-6900 or have a member of your staff contact our Congressional Liaison, Catherine Grant, at (202) 245-7023.

Sincerely,

Kathleen S. Tighe  
Inspector General

Enclosure

cc: The Honorable Ron Johnson, Chairman, Committee on Homeland Security and  
Governmental Affairs, United States Senate  
The Honorable Betsy DeVos, Secretary, U.S. Department of Education

**U.S. Department of Education Office of Inspector General**

**Response to Request for Information on Federal Electronic Records and Responses to  
Congressional Requests**

**July 14, 2017**

On June 8, 2017, Senators McCaskill and Carper requested that the U.S. Department of Education (Department) Office of Inspector General (OIG) conduct a review of the Department's processes and compliance with applicable legal standards for preserving electronic messages as Federal records, and cooperation with Congressional information requests. The Senators specifically requested that the OIG conduct a review addressing the following questions:

1. Since January 20, 2017, has any Department official directed or advised any agency employee to delay or withhold a response to a Congressional request for information?
2. Since January 20, 2017, has any Department 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?
3. Since January 20, 2017, has the Department 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?
4. Since January 20, 2017, has any Department official used, for work-related communications, a smartphone application, 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 Department official failed to abide by Federal law and/or National Archives and Records Administration (NARA) or Department 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 using non-government account?

6. Has the OIG previously provided recommendations to the Department regarding its management of the preservation of electronic records and compliance with Congressional document requests?

### ***Work Performed***

To respond to this request, we:

1. Interviewed officials from the Office of the Secretary, the Office of Management, the Office of Legislation and Congressional Affairs (OLCA), and the Office of the Chief Information Officer (OCIO) who are responsible for Congressional correspondence, records management, and smartphone applications.
2. Reviewed and analyzed 294 summary reports of the status of all Congressional correspondence received from January 20, 2017, through June 15, 2017, that were addressed to the Secretary and controlled by the Executive Secretariat in the Office of the Secretary.<sup>1</sup>
3. Conducted follow-up reviews on all 6 Congressional requests that the Department did not respond to in writing and a judgmental sample of 10 requests that took over 30 days to respond to, or that remained open after 30 days. We judgmentally selected requests focused on issues of policy or regulation that included five requests from Democrats, three from Republicans, and two joint requests.
4. Reviewed the Department's policies and procedures on the use of smartphone applications.
5. Identified approved smartphone applications that allow for automatic deletion or encryption, and identified all users who had downloaded those applications that allow for automatic deletion on their Department-issued phone.
6. Conducted a follow-up interview with all four users who downloaded Snapchat or WhatsApp onto their Department-issued smartphone to determine how those applications were used and whether any Federal records were created or preserved.

---

<sup>1</sup> We reviewed only the summary information related to the status of these requests, and did not review the contents of the requests or replies. Also, we did not quantify, verify, or review responses to Congressional requests that were handled by OLCA. According to the Legislative Affairs Director, constituent requests dominate this correspondence and it is their policy to respond to all Congressional requests.

7. Reviewed the Department's policies and procedures for ensuring compliance with Federal records management laws and policies.
8. Identified all politically appointed officials on board as of June 26, 2017, and requested documentation that they had received training on Federal records management requirements.

### ***Summary of Results***

According to the Secretary's Chief of Staff and other Department officials responsible for coordinating responses to Congressional correspondence, it is the Department's policy to respond to all Congressional correspondence, including requests for information, regardless of political party. Of the 294 Congressional requests that we reviewed, we identified a total of six instances where the Executive Secretariat closed the requests without response, either at the direction of, or based on information received from, the Chief of Staff.<sup>2</sup> The Chief of Staff indicated that three requests were closed either because the information had been provided during the confirmation process (two requests) or the Secretary had telephoned the member (one request). The Chief of Staff directed that one request related to the Presidential Executive Order banning travel from certain countries not be responded to because it was not appropriate for a response from the Secretary as she had not yet been confirmed, and the Presidential Transition office had received and responded to similar letters. For the two remaining requests, the Department decided, as a result of our review, that the requests had been closed in error and is now working to respond.

We found that the Department's efforts to ensure compliance with Federal records management laws and requirements focused on training Department employees of their responsibilities for maintaining government records. According to the Chief Privacy Officer, she has trained all but 4 of the 41 newly appointed political officials on records management requirements, and these remaining 4 officials are being scheduled for training. We determined that the Department has approved for use on its Department-issued smartphones two applications—Snapchat and WhatsApp—that allow for the encryption or automatic deletion of information. However, according to OCIO and Office of Communications and Outreach (OCO) officials, these applications have only been approved for use by a limited number of employees

---

<sup>2</sup> As previously noted, we did not review the contents of the correspondence and thus did not confirm whether each requested information from the Department. For ease of reference, we refer to the correspondence as requests.

who have requested access. Of this group, only four employees have downloaded either of the applications, and they told us their use of these applications was limited.

### ***Background***

The Office of the Director of Executive Secretariat (commonly referred to as Exec Sec) serves as the central coordinating point for documents needing review by the Secretary. The Exec Sec is responsible for coordinating all decision documents and information memoranda in response to information requests, including requests from Congress. The Exec Sec logs all such requests, directs them to the appropriate office, tracks and monitors the progress of the response, and prepares the final response for signature. The Office of the Chief Privacy Officer (OCPO) is responsible for overseeing the Department's records management program and ensuring the Department's compliance with Federal records management laws and related Department policies. OCIO governs and manages the network infrastructure and operations of the Department. Among its responsibilities, the OCIO is responsible for administering the Department's Mobile Devices program and approving smartphone applications for use on Department-issued smartphones.

The Federal Records Act of 1950 (Act) requires Federal agencies to make and preserve records containing adequate and proper documentation of its organization, function, policies, decisions, procedures, and essential transactions. It defines a Federal record as any information made or received by a Federal agency while conducting official business. In November 2014, the Act was amended to prohibit using nonofficial electronic messaging accounts to create or send a record, unless those messages are forwarded to an official electronic messaging account.<sup>3</sup> It also expanded the definition of a Federal record to include electronic messages.

In July 2015, the NARA also issued guidance<sup>4</sup> to provide Federal agencies with additional records management guidance for electronic messages and assist agencies in developing strategies for managing such messages.

The Department has issued two directives to establish its overall policies and procedures for compliance with the Act and its amendments, specific to the Department's records retention and disposition schedules<sup>5</sup> and records and information management program.<sup>6</sup> The directive states that it is the policy of the Department to create, preserve, maintain, use, and dispose of

---

<sup>3</sup> 44 U.S.C § 2911(a).

<sup>4</sup> Bulletin 2015-02, "Guidance on Managing Electronic Records," dated July 29, 2015.

<sup>5</sup> Office of Management (OM): 6-106 "Administrative Communications System Department Directive – Records Retention and Disposition Schedule," dated December 10, 2013.

<sup>6</sup> OM: 6-103, "Administrative Communications System Departmental Directive – Records and Information Management Program," dated April 14, 2017.

Federal records in accordance with Federal records management laws. It also prohibits the use of personal accounts to conduct government business. However, the policy states that if a personal account is used to create or send a record, an employee must forward the message to the Department's email system or print a copy for preservation within 20 days. Department training materials further state that personal accounts should be used only in exceptional circumstances when official accounts are unavailable.

### ***Results of Review***

1. Since January 20, 2017, has any Department official directed or advised any agency employee to delay or withhold a response to a Congressional request for Information?

According to the Secretary's Chief of Staff, it is the Department's policy to respond to all Congressional requests for information. Of the 294 Congressional requests that we reviewed, we identified a total of six instances where the Executive Secretariat closed the requests without response, either at the direction of, or based on information from, the Chief of Staff. The Chief of Staff indicated that three of the requests were closed either because the information has been provided during the Secretary's confirmation process (two requests) or the Secretary had telephoned the member (one request). The Chief of Staff directed that one request related to the Presidential Executive Order banning travel from certain countries not be responded to because it was not appropriate for a response from the Secretary as she had not yet been confirmed, and the Presidential Transition office had received and responded to similar letters. For the two remaining requests, the Department decided, as a result of our review, that the requests had been closed in error and is now working to respond. (See Table 1)

**Table 1: Congressional Requests for Information Closed with No Response**

<b>Requestor</b>	<b>Subject of Letter</b>	<b>Reason Declined</b>
Senator Patty Murray	Requesting then Secretary-designate's position on President's Executive Order banning travel from certain countries.	Request received prior to Secretary's confirmation and Presidential Transition office had responded to similar letters.
Senator Patty Murray	Requesting 3 years of tax returns as part of the Senate vetting process.	Information was provided during confirmation process.
Senator Patty Murray	Seeks answers to additional questions from then Secretary-designate on additional investments after submitting a more detailed financial disclosure form.	Information was provided during confirmation process.
Senator Patty Murray and Representative Robert C. Scott	Expressing concerns about the Secretary's recent comments about restructuring the Department and conducting an audit of the Department's programs	Closed per Chief of Staff instruction. Department subsequently decided closure was erroneous and is now developing a response.
Representative Luke Messer	Requesting the reestablishment of the National Research and Development Center on school choice.	Secretary placed a phone call with the Representative.
Senator Patty Murray	Seeking clarification concerning the Secretary's comments about Department of Education employees	Closed per Chief of Staff instruction. Department subsequently decided closure was erroneous and is now developing a response.

2. Since January 20, 2017, has any Department 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?

The Director of the Executive Secretariat and the Director of Legislative Affairs both said that they have not been directed to only provide requested documents or information to a Committee chair. Our review of summary information on the status of responses to Congressional requests addressed to the Secretary shows that the Department has been responding to Congressional requests from both parties. Of the 294 Congressional requests that we reviewed, 130 were from Republicans, 129 were from Democrats, and 35 were joint

requests. As of June 19, 2017, 93, or nearly one third of these requests, remained open, including 51 that have been pending for more than 30 days. Our follow up of 10 cases that were delayed longer than 30 days revealed no instances where the response was delayed at the direction of any senior official. The Exec Sec explained that this Administration has received an unusually high volume of requests, and that they are working to respond as quickly as possible. OLCA also receives and responds to Congressional requests, and works with the Exec Sec to coordinate responses to requests of the Secretary. We did not quantify, verify, or review these requests as we were informed that many of them involved constituent issues. The Director of Legislative Affairs for OLCA informed us that it is OLCA's policy to respond to all Congressional requests.

3. Since January 20, 2017, has the Department 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?

The Department has not issued any specific guidance on the use of smartphone applications that support encryption or the ability to automatically delete messages. (See answer to question 5 below on the guidance and training employees receive on the preservation of Federal records created on Department provided electronic messaging services and personal email or other messaging accounts.)

4. Since January 20, 2017, has any Department 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?

The Department manages the use of smartphone applications on Department-issued smartphones through the AirWatch mobile device solution, which allows for the use and download of only specific Department-approved applications. No applications in AirWatch that are available to all users allow for encryption or automatic deletion of messages. According to OCIO and OCO officials, they approved WhatsApp and Snapchat for use by a small group of employees who have requested access to these or other applications. Specifically, OCIO provided us with a list of 18 current career employees authorized to use these applications. According to OCIO officials, only four of these employees have downloaded these two applications. We interviewed each of these employees, and they reported limited use of these applications. One employee used WhatsApp to call a rural school official, another employee used the Department's official Snapchat account to promote a conference in December, 2016,

and a third employee, who requested WhatsApp as an accommodation for a disability, used it to communicate with work colleagues via their private WhatsApp accounts. The other employee reported only personal use.

According to the Senior Official Delegated the Duties and Functions of the Deputy Secretary, the Department intends to issue guidance prohibiting the use, except for disability accommodations, of software that allows for the automatic deletion of information.

5. Since January 20, 2017, has any Department official failed to abide by Federal law and/or NARA or Department 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 using non-government account?

All Department employees are required to take records management training annually in which they are informed of their responsibilities for preserving electronic messages that are created outside of official accounts that automatically capture employee communications. In addition, all new political appointees to the Department receive this training after arrival directly from the Chief Privacy Officer. According to the Chief Privacy Officer, she has trained all but 4 of the 41 newly appointed political officials on records management requirements, and these remaining 4 officials are being scheduled for training. We requested but have not received records corroborating that the 37 officials received the training.

This training instructs employees that it is Department policy to create, preserve, maintain, use, and dispose of Federal records in accordance with Federal records management laws and policies. The training also states that employees are prohibited from using personal messaging accounts to conduct official government business. However, if a Federal record is created or received in a personal account, the employee must forward the message to the Department's email system within 20 days.

We reviewed OIG hotline and investigative records and noted no complaints or investigations related to compliance with Federal records management requirements since January 20, 2017. The Chief Privacy Officer told us that she was not aware of any employee failing to comply with Federal records requirements related to electronic records. In the absence of allegations being brought to the attention of responsible officials, the Department would have limited ability to detect violations of the policy on use of personal messaging accounts since those accounts are, by definition, outside of the Department's information systems.

6. Has the OIG previously provided recommendations to the Department 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.

The OIG's last report on records management was completed in 2001, and we have no outstanding recommendations.

### ***Conclusion***

We found no evidence that the Department is directing employees to not respond to Congressional requests for information or that it is responding to only requests from a Committee chair. Although this Administration has experienced a high volume of written Congressional requests, it is working to respond to virtually every request it has received. We also found that there is very limited use on Department-issued smartphones of applications that allow for encryption or automatic deletion of messages. The Department relies primarily on its training of employees to inform them of Federal records requirements. The Department has limited ability to detect if Federal records are created using personal accounts and has not issued specific guidance on how to capture and preserve records created on these types of smartphone applications.