United States Senate
WASHINGTON, DC 20510

March 12, 2015

U.S. Department of State
Office of Inspector General
Room 8100, SA-3
2201 C Street, N.W.
Washington, DC 20520-0308

Dear Inspector General Linick:

We write to you today concerning the recent revelations that former Secretary of State Hillary Clinton and other top aides used non-State Department email addresses and servers to conduct official U.S. Government business. We are concerned that diplomatically sensitive, and possibly classified, information may have been transmitted and stored in an insecure manner.

Foreign intelligence organizations and malicious actors continuously probe our government's information systems for weaknesses and attempt targeted intrusions. As you know, the federal government has experienced a number of sophisticated intrusions in recent years, and the threat is only growing. The use of privately maintained information systems that are not protected by federal government experts and key technical capabilities raises serious concerns as those networks may be less secure. Moreover, if a non-government server was known to be a repository for the Secretary's emails, it would almost certainly become—if it is not already—a priority target for foreign intelligence services and others.

To ensure appropriate security protections for sensitive but unclassified information the State Department's Foreign Affairs Manual policy, in place since 2005, requires that "normal day-to-day operations be conducted on an authorized AIS [Automated Information System], which has the proper level of security control to provide nonrepudiation, authentication and encryption, to ensure confidentiality, integrity, and availability of the resident information." The policy also states that "employees are expected to use approved secure methods to transmit SBU [sensitive but unclassified] information when available and practical." Furthermore, it is our understanding that the State Department has specifically instructed its employees, ostensibly during Secretary Clinton's tenure, to avoid conducting official Department business from personal e-mail accounts.

In addition, there are serious questions about the use of such non-government accounts on federal recordkeeping and transparency, particularly if it results in non-compliance with the Federal Records Act and National Archives and Records Administration (NARA)

regulations. Potential noncompliance with these requirements, many of which are imposed by federal law, is a serious matter.

We ask that your office, in coordination with the Inspector General for the Intelligence Community, and any other appropriate Federal entities, conduct a thorough audit related to electronic communications by State Department employees, including former senior officials, that were principally carried out on non-government-owned, or non-government-protected, information networks. Further, we ask that you provide a written report to the relevant congressional committees detailing your findings and any recommendations. The report should include the following:

1. The names and positions of State Department officials who regularly used non-official email to conduct official government business.

2. A specific description of the non-government information networks or systems that were used to transmit such email, to include:
    a. the network security measures in place on such networks and systems from 2009 to 2013;
    b. the means, if any, by which the network's security incorporated classified cyber security threat information controlled by the U.S. government;
    c. the type of wireless communication devices that connected to the systems;
    d. the location and ownership of the servers and other components of such networks or systems;
    e. the names of individuals and entities that had authorized access to such networks or systems, including specifically those with authorized administrative access; and
    f. the funding source for the system, its maintenance, upkeep, and administration.

3. An assessment of whether any of the State Department or other U.S. or foreign government information transmitted or received on such networks or systems contained classified, sensitive but unclassified, diplomatically sensitive, or otherwise nonpublic material.

4. A determination of whether any non-government emails used to conduct official government business or other government information has been deleted from these information networks or systems or altered from their original content, and, if applicable, an estimate of the number of emails or material that was deleted or altered.

5. A determination of whether all emails and other information that was required to be archived pursuant to the Federal Records Act or other legal or regulatory requirements were provided to the State Department or other government agencies for archiving, and whether the timing and nature of these actions was consistent with State Department policy, as well as applicable federal law and regulations.

We ask that this be an unclassified report, and that a classified annex be provided if necessary. Thank you for your time, and we look forward to working with you on this important matter of national security.

Sincerely,

Chairman Bob Corker
Senate Foreign Relations Committee

Chairman Richard Burr
Senate Select Committee on Intelligence

Chairman Ron Johnson
Senate Homeland Security and
Governmental Affairs Committee

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

March 18, 2015

The Honorable Steve A. Linick
Inspector General
U.S. Department of State
2201 C Street, N.W.
Washington, DC 20520

Dear Mr. Linick:

On March 2, 2015, the *New York Times* reported that former Secretary of State, Hillary Clinton, exclusively used a non-State Department email account to conduct business while Secretary of State.[1] The *Times* reported that the State Department "took no action to have her personal emails preserved on department servers at the time, as required by the Federal Records Act."[2] Secretary Clinton's actions may violate federal regulations promulgated in October of 2009, which read "Agencies that allow employees to send and receive official electronic mail messages using a system not operated by the agency must ensure that Federal records sent or received on such systems are preserved in the appropriate agency recordkeeping system."[3] The Homeland Security and Government Affairs Committee requests that you examine this matter.

On March 10, 2015, Secretary Clinton admitted publicly that she exclusively used a non-State Department email account created on a private email server located in her home for official State Department business.[4] Secretary Clinton argued that she complied with federal rules because she sent emails to other officials on their State Department email accounts, which would be preserved under federal record-keeping rules.[5] However, communications of great public interest, such as emails to foreign leaders, individuals in the private sector, or government officials outside the State Department, may not be preserved because those individuals do not possess an official State Department account. As such, the use of a non-State Department email account to conduct official government business may have affected congressional oversight and limited citizen access to information under the Freedom of Information Act (FOIA) for records during Secretary Clinton's time at the State Department.[6]

---

[1] Michael S. Schmidt, *Hillary Clinton Used Personal Email Account at State Dept., Possibly Breaking Rules*, THE NEW YORK TIMES, March 2, 2015.
[2] *Id.*
[3] 36 CFR 1236.22.
[4] Press Conference with Hillary Clinton, CNN (March 10, 2015).
[5] *Id.*
[6] Michael S. Schmidt and Amy Chozick, *Using Private Email, Hillary Clinton Thwarted Record Requests*, THE NEW YORK TIMES, March 3, 2015.

Secretary Clinton also admitted that she operated her own internet server within her home to host her non-State Department email account.[7] This practice further limits access to non-State Department email accounts used to conduct official government business, and potentially gives unknown third parties sole control over the information contained in those emails, which should rightfully be in the public domain under federal record-keeping laws and regulations.

The exclusive use of a non-State Department email account by the leading diplomat in the United States also raises national security concerns. In her position, Secretary Clinton had access to sensitive and classified diplomatic information on a daily basis. Although Secretary Clinton asserted that she put safeguards in place to protect her non-State Department email server, it is unknown what precautionary security measures existed, and whether those safeguards were consistent with best practices used by the federal government to protect email communications.[8]

To address these concerns, we request that your office initiate an investigation into the exclusive use of a non-State Department email account by Secretary Clinton, including taking all necessary steps to immediately preserve and retain all emails on the non-State Department email server used for official business. Specifically, the Committee would like your investigation to answer to the following questions:

1. What are the State Department's email and record retention policies and procedures?
    a. Do State Department officials receive training on the Department's record retention policies and procedures?
    b. What policies does the Department have in place to ensure information transmitted over its networks is secure?
    c. Are the State Department's email and record retention policies and procedures sufficient?
    d. Were the State Department's email and record retention policies applied to Secretary Clinton? If not, please provide an explanation.

2. Did any federal employee or official authorize Secretary Clinton to use a non-State Department e-mail for official e-mails? If so, who?
    a. Who configured, managed, and administered Secretary Clinton's non-State Department e-mail address and associated software and hardware during her tenure at the State Department?
    b. Who paid for domain registration, equipment, software licenses, and associated maintenance for the non-State Department e-mail system?

3. What is the State Department's policy regarding assessing security of information technology systems used for official State Department business?

---

[7] Jack Gillum and Ted Bridis, *Clinton ran own computer system for her official emails*, THE ASSOCIATED PRESS, March 4, 2015.
[8] Press Conference with Hillary Clinton, CNN (March 10, 2015).

a. Did the State Department conduct a security assessment of Secretary Clinton's non-State Department e-mail system? If so, what was the result of that assessment? If not, why not?
b. Was Secretary Clinton's non-State Department e-mail system securely configured and compliant with the Federal Information Security Management Act?
c. Were any mobile devices connected or linked with the non-State Department e-mail system ever taken into foreign countries? If so, what security processes were in place to ensure the device, the data on the device(s), and the data on the non-State Department e-mail system were not compromised?

4. What motivated the State Department to send a letter to all former secretaries of state, including Secretary Clinton, in October 2014 seeking emails and other documents in their possession relating to official government business?
   a. When did other State Department employees become aware of Secretary Clinton's exclusive use of a non-State Department email account?
   b. How did the State Department become aware of the need to request emails sent through Secretary Clinton's non-State Department email account?
   c. Was the State Department's October 2014 request sufficiently expansive?
   d. How did Secretary Clinton respond to the request?
   e. What search terms and/or filters did Secretary Clinton apply when gathering her non-State Department emails?
   f. Did the Department and OIG's lack of access to Secretary Clinton's emails impede any reviews, investigations, inspections, evaluations, or audits conducted by the Department, OIG, or a third party?
   g. Who applied search terms and/or filters to gather Secretary Clinton's emails?
   h. How did the State Department maintain or preserve these emails after Secretary Clinton provided them to the Department?

5. After the State Department became aware of Secretary Clinton's use of a non-State Department email account to conduct official business, what entities or individuals did the Department notify about Secretary Clinton's use of a non-State Department email account?
   a. When did the Department notify these entities or individuals?
   b. What did the Department tell these entities or individuals?
   c. Did the Department receive instructions from any entities or individuals on what to tell those that it notified?
   d. Did any State Department officials inform the National Archives and Records Administration (NARA) of Secretary Clinton's exclusive use of a non-State Department email account? When?
   e. Did the Department notify your office about Secretary Clinton's use of a non-State Department email account?
   f. Was there any discussion between Department officials about whether the Department should notify your office, NARA, Congress, and/or the public about Secretary Clinton's use of a non-State Department email account?

g. Since the news of Secretary Clinton's non-State Department email server became public, have any federal government entities requested that Secretary Clinton preserve and retain all documents created on that email server during her tenure as Secretary of State?

6. Did State Department officials, including Secretary Clinton, take any steps to produce emails sent through Secretary Clinton's non-State Department email account in response to FOIA requests or requests from Congress? If so, what steps were taken for each specific request, from January 2009 to the present?

7. What steps is the Department taking to investigate Secretary Clinton's email practices?

8. What steps is the Department taking to recover emails sent through Secretary Clinton's non-State Department email account?
   a. Has the State Department attempted to recover emails sent through Secretary Clinton's non-State Department email account through other federal agencies, foreign governments, or the White House?
   b. What steps is the State Department taking to ensure it has access to the entire universe of Secretary Clinton's emails used to conduct official government business?

9. Did any of the e-mails sent to or from Secretary Clinton's non-State Department email account contain classified information?

10. Does Secretary Clinton have exclusive control over which documents she chooses to turn over to the federal government as responsive to FOIA and other requests? Who has physical possession and control of Secretary Clinton's emails at present?

If, during your investigation, you discover that other State Department employees used non-official email accounts to conduct official business, please answer these questions with respect to these other employees and accounts as well. We ask that you produce a report to the Committee with your findings related to this request. Please keep Committee staff apprised of your progress in conducting this report and contact Emily Martin or Caroline Ingram of the Committee staff at (202) 224-4751 with any questions. Your assistance in this matter is greatly appreciated.

Sincerely,

Ron Johnson
Chairman

Cc: The Honorable Thomas R. Carper
Ranking Member

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

July 9, 2015

The Honorable John F. Kerry
Secretary
U.S. Department of State
2201 C Street, NW
Washington, DC 20520

Dear Secretary Kerry:

The Committee on Homeland Security and Governmental Affairs is examining the Department of State's efforts to process and release electronic documents provided to the Department by former Secretary of State Hillary Clinton. I understand that the Department's Freedom of Information Act (FOIA) staff is working to review electronic documents provided by Secretary Clinton and I hope that Department officials are carefully processing, redacting, and classifying documents in accordance with federal law. In light of information obtained by the Committee that the Department publicly released a classified document and failed to adequately consult with the Intelligence Community (IC) prior to releasing some of Secretary Clinton's e-mails,[1] the Committee wants to confirm that Department officials charged with processing Secretary Clinton's electronic documents are sufficiently scrutinizing the documents and consulting with the appropriate classification experts, rather than relying upon any assurances made by Secretary Clinton regarding the absence of classified material.

In December 2014, following a request from the Department made to all former Secretaries of State for official documents,[2] Secretary Clinton provided 55,000 pages of electronic documents exchanged during her tenure as Secretary of State using her personal communications hardware and software.[3] Following a March 2015 report in the *New York Times* that Secretary Clinton had exclusively used a non-State Department e-mail account and server to conduct business during her tenure as Secretary of State, Secretary Clinton appeared at a press conference to address her personal e-mail use. During the press conference, she insisted that she did not exchange classified information.[4] She said: "I did not e-mail any classified material to

---

[1] Memorandum from I. Charles McCullough, III, Inspector Gen., Intelligence Community, *Update to IC IG Support to State Department IG* (Jun. 19, 2015).
[2] Michael S. Schmidt, *Hillary Clinton Used Personal Email Account at State Dept., Possibly Breaking Rules*, N.Y. TIMES, March 2, 2015, *available at* http://www.nytimes.com/2015/03/03/us/politics/hillary-clintons-use-of-private-email-at-state-department-raises-flags.html?_r=0 (last visited Jul. 9, 2015).
[3] *Id.*
[4] Zeke J. Miller, *Transcript: Everything Hillary Clinton Said on the Email Controversy*, TIME, Mar. 10, 2015, *available at* http://time.com/3739541/transcript-hillary-clinton-email-press-conference/ (last visited Jul. 9, 2015).

anyone on my e-mail. **There is no classified material**. So, I'm certainly well-aware of the classification requirements and did not send classified material."[5]

According to media reports, the Department organized a team of Department officials to sort, review, and redact the electronic documents.[6] The Department reportedly tasked a full-time staff made up of one project manager, two case analysts, nine FOIA reviewers, and additional information analysts to review Secretary Clinton's electronic documents.[7] The team reportedly began reviewing the 55,000 pages in April and is continuing to do so.[8] The team implemented a five-step process for review involving "barcodes," "separator sheets," "manually input bibliographic coding," and other data entry tasks.[9] It is unclear whether the Department's review team was tasked with analyzing the potential appearance of classified material in Secretary Clinton's emails, whether the team was instructed to consult with classification experts in the Intelligence Community, or whether the team simply relied upon the statements of Secretary Clinton that there is no classified material in the e-mails.

On May 22, 2015, the Department released its first round of 296 of Secretary Clinton's e-mails, spanning 896 pages of the 55,000 pages of documents that she had turned over to the Department.[10] According to a review conducted by the Intelligence Community Inspector General (IC IG) of this first set of 896 pages of e-mails released by the Department, Department officials failed to mark one classified document as classified. According to the IC IG, Department officials culling Secretary Clinton's electronic documents for potential public release disseminated at least one document publicly in an unclassified and unredacted form that should have been marked as classified. Department officials apparently did not coordinate with the appropriate Intelligence Community officials prior to releasing the document in question. The disclosure made by the Department raises serious national security concerns and could implicate a violation of federal law concerning the unauthorized disclosure of classified information. Accordingly, the IC IG made a series of recommendations that were provided to the Department to improve its review process to better protect potentially classified information.

Further, the reported disclosure of just one of 296 e-mails, which span 896 pages of the 55,000 total pages of documents Secretary Clinton provided to the Department, raises additional questions as to whether the Department has or will inadvertently release additional classified

---

[5] *Id.* (emphasis added).
[6] *See, e.g.*, Justin Fishel, *How the State Department is Tackling 55,000 Pages of Hillary Clinton Emails*, ABC NEWS, May 19, 2015, *available at* http://abcnews.go.com/US/state-department-tackling-55000-hillary-clinton-emails/story?id=31160021 (last visited Jul. 9, 2015).
[7] *Id.*
[8] *Id.*
[9] *Id.*
[10] Alexandra Jaffe, *First Round of Hillary Clinton State Department Emails Released*, CNN, May 26, 2015, *available at* http://www.cnn.com/2015/05/22/politics/hillary-clinton-emails-release-benghazi/ (last visited Jul. 9, 2015) [hereinafter Jaffe, *First Round of Hillary Clinton Emails*]; Michael S. Schmidt, *First Batch of Hillary Clinton Emails Captures Concerns Over Libya*, N.Y. TIMES, May 21, 2015, *available at* http://www.nytimes.com/2015/05/22/us/politics/first-batch-of-hillary-clinton-emails-captures-concerns-over-libya.html (last visited Jul. 9, 2015); The Assoc. Press, *Highlights of Clinton Emails on Benghazi*, N.Y. TIMES, May 22, 2015, *available at* http://www.nytimes.com/aponline/2015/05/22/us/politics/ap-us-dem-2016-clinton-emails-glance.html (last visited Jul. 9, 2015).

material, as well as the adequacy of the Department's review process. Based on the appearance of classified material in the small fraction of Secretary Clinton's emails publicly released thus far, it is quite possible that there is considerably more classified material in the entirety of Secretary Clinton's e-mails provided to the Department. In the most recently released set of approximately 3,000 pages of e-mails—publicly disseminated on June 30, 2015—the Department redacted 25 e-mails for the presence of (b)(1), or classified information.[11] Thus, the Department must ensure that it works quickly with the IC and IC IG to implement changes to its review process before any additional classified material is publicly released.

As the Department works to review and process Secretary Clinton's electronic documents, the Committee seeks to ensure that the Department is carefully assessing the documents to discern whether the documents contained classified information. In order to assist the Committees' oversight obligations, I request that you provide the following information:

1. Please explain what guidance, instruction, and training have been communicated and provided to Department FOIA staff, including all Department officials who are assisting with reviewing and processing Secretary Clinton's electronic documents, on how to review and process Secretary Clinton's electronic documents for potential public release and properly identify potentially classified information.

2. Please explain what procedures Department FOIA staff, including all Department officials who are assisting with reviewing and processing Secretary Clinton's electronic documents, are using to review and process Secretary Clinton's electronic documents for potential public release and properly identify potentially classified information.

3. Please explain whether the directives and procedures used to review and process Secretary Clinton's electronic documents for potential public release and properly identify potentially classified information have changed since the IC IG submitted its June 19, 2015 letter.

4. Please explain what steps the Department is taking to implement the IC IG's recommendations to improve its review of Secretary Clinton's electronic documents for the presence of classified information, as well as what safeguards the Department has implemented to protect other potentially classified information from public release.

5. Please explain what steps the Department is taking with the IC and IC IG to address Secretary Clinton's transfer of classified information over an unclassified network.

---

[11] Peter Baker & Steve Eder, *Trove of Hillary Clinton's Emails Highlights Workaday Tasks at State Department*, N.Y. TIMES, Jun. 30, 2015, *available at* http://www.nytimes.com/2015/07/01/us/politics/new-trove-of-hillary-clintons-emails-highlight-workaday-tasks-at-the-state-department.html?_r=0 (last visited Jul. 9, 2015); *State Dept. Withholds 'Classified' Info from Clinton Emails, Despite Claim of 'No Classified Material'*, FOX NEWS, Jul. 1, 2015, *available at* http://www.foxnews.com/politics/2015/07/01/state-dept-withholds-classified-clinton-emails-despite-claim-there-is-no/ (last visited Jul. 9, 2015).

6. Please explain whether Department officials have consulted with Secretary Clinton, her staff, or her representatives directly regarding the presence of classified information within the 55,000 pages of documents provided to the Department. If so, please provide all documents and communications referring or relating to the potential presence of classified information within the 55,000 pages of documents.

7. Please explain whether Department officials have relied on representations or statements made by Secretary Clinton, her staff, her representatives, or any media reports concerning the potential presence of classified information within the 55,000 pages of documents provided by Secretary Clinton to the Department. If so, please explain to what extent Department officials have relied on these representations or statements.

Please produce this material as soon as possible, but by no later than 5:00 p.m. on July 23, 2015. To the extent possible, please provide unclassified responses to these questions. Should a complete response require transmission of classified information, please send such information under separate cover, via the Office of Senate Security.

If you have any questions about this request, please contact me or have your staff contact Caroline Ingram or Emily Martin of Senator Johnson's staff at (202) 224-4751. Thank you for your attention to this matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

July 29, 2015

Mr. David E. Kendall
Williams & Connolly LLP
725 Twelfth Street NW
Washington, DC 20005

Dear Mr. Kendall:

The Inspector General of the Intelligence Community (IC IG) recently notified Congress that you possess a thumb drive containing 30,000 emails from your client, former Secretary of State Hillary Clinton, which may contain classified information sent or received by Secretary Clinton.[1] I write to inquire what protections you have implemented to access, store, and safeguard the classified material in your possession.

On March 12, 2015, I joined with Chairmen Bob Corker and Richard Burr in asking the Inspector General of the State Department to examine whether State Department employees sent or received classified information in an insecure manner.[2] We asked that the State Department IG coordinate with the IC IG in this review.[3] On March 18, 2015, I wrote separately to the State Department IG to inquire, among other things, whether Secretary Clinton's emails included any classified information.[4] On July 23, 2015, the IC IG notified Congress that State Department Freedom of Information Act (FOIA) officials informed him "that there are potentially hundreds of classified emails within the approximately 30,000 provided by former Secretary Clinton."[5] The IC IG stated:

> We note that none of the emails we reviewed had classification or dissemination markings, but some included IC-derived classified information and should have been handled as classified, appropriately marked, and transmitted via a secure network. **Further, my office's limited sampling of 40 of the emails revealed four contained classified IC information which should have been marked and handled at the SECRET level.**[6]

---

[1] Memorandum for Sen. Richard Burr et al. from I. Charles McCullough, III, Update to IC IG support to State Department IG (July 23, 2015).
[2] *See* Letter from Senator Bob Corker et al., to U.S. Dep't of State, Office of Inspector Gen. (Mar. 12, 2015).
[3] *Id.*
[4] Letter from Senator Ron Johnson, S. Comm. on Homeland Sec. & Gov't Affairs, to Steve A. Linick, U.S. Dep't of State Office of Inspector Gen. (Mar. 18, 2015).
[5] Memorandum, *supra* note 1, at 2.
[6] *Id.* (emphasis added).

The memorandum further stated that "the 30,000 emails in question are purported to have been copied to a thumb drive in the possession of former Secretary Clinton's personal counsel, Williams and Connelly [*sic*] attorney David Kendall."[7]

On July 24, 2015—after suggestions that the information in Secretary Clinton's emails had been classified retroactively[8]—the IC IG and the State Department IG issued a joint statement. They wrote:

> The IC IG found four emails containing classified IC-derived information in a limited sample of 40 emails of the 30,000 emails provided by former Secretary Clinton. The four emails, which have not been released through the State FOIA process, did not contain classification markings and/or dissemination controls. **These emails were not retroactively classified by the State Department; rather these emails contained classified information when they were generated and, according to IC classification officials, that information remains classified today.** This classified information should never have been transmitted via an unclassified personal system.[9]

The IC IG and State Department IG concluded that "classified information may exist on at least one private server and thumb drive that are not in the government's possession."[10]

As you know, Directive No. 1 of the National Archives' Information Security Oversight Office (ISOO) requires holders of classified information to "protect[] it from persons without authorized access to that information, to include securing it in approved equipment or facilities . . . ."[11] The ISOO Directive mandates that "[c]lassified information shall be stored only under conditions designed to deter and detect unauthorized access to the information," and prescribes storage requirements according to the classification level.[12] The Directive also prescribes requirements for the transmission of classified information and requires the implementation of information controls to "assure that access to classified information is provided to authorized persons."[13] Further, the State Department's *Foreign Affairs Manual* requires classified information to be stored in an "approved locked container" under particular conditions.[14]

Based on the IC IG's memorandum, it is unclear what actions, if any, you have taken to safeguard the classified information contained on the thumb drive in your possession. The lax

---

[7] *Id.*
[8] *See* Josh Gerstein & Hanna Trudo, *Hillary Clinton on email scandal: Everybody calm down*, Politico, June 24, 2015 (statement of Rep. Elijah E. Cummings).
[9] I. Charles McCullough, III, & Steve Linick, Statement from the Inspectors General of the Intelligence Community and the Department of State Regarding the Review of Former Secretary Clinton's Emails (July 24, 2015) (emphasis added).
[10] *Id.*
[11] 32 C.F.R. § 2001.41.
[12] *Id.* § 2001.43.
[13] *Id.* § 2001.45, 2001.46.
[14] Storing and Safeguarding Classified Material, 12 F.A.M. 530.

storage and safeguarding of this information could have serious consequences to national security. Accordingly, I ask that you provide the following information:

1. Please explain how you have secured the thumb drive in your possession that apparently contains Secretary Clinton's emails, including emails with classified information ("the thumb drive").

2. Please identify the manufacturer and model of the thumb drive.

3. Please identify all individuals who have had or currently have access to the thumb drive.

4. Please identify the computer system(s) you and/or your colleagues utilize or have utilized to access the data on the thumb drive.

5. Please provide a list of every individual who has accessed or had possession of the thumb drive since it came to be in your possession.

6. Please explain the controls you have established for storing, transporting, and accessing the thumb drive and the basis for those controls in Federal policies and procedures regarding storage of and access to classified information.

7. Please identify any partners or employees of Williams & Connolly, including yourself, who possess personal security clearances for the possession of and access to classified information issued by the Federal Government; any partners or employees of Williams & Connolly with formal authorizations to courier classified information; and any facility clearances issued to Williams & Connolly or to which individuals at Williams & Connolly have access for storage purposes.

8. Please explain how you have secured the server used by Secretary Clinton to send and receive emails during her time as Secretary of State, including emails that may contain classified information.

In addition, I ask that you take all appropriate steps on behalf of Secretary Clinton to preserve all devices and data on those devices—including the thumb drive in your possession and the private server used by Secretary Clinton—that may contain classified information. I ask that you provide responses to the requests above and a certification that you have preserved this material as soon as possible but no later than 5:00 p.m. on August 12, 2015.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of the Government."[15] Additionally, S. Res. 73 (114th Congress) authorizes the Committee to examine "the efficiency and economy of all branches and functions of the Government with particular reference to—the effectiveness of

[15] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).

present national security methods, staffing, and process . . . ."[16] For purposes of this request, please refer to the definitions and instructions in the enclosure.

If you have any questions about this request, please contact David Brewer or Liam McKenna of the Committee staff at (202) 224-4751. Thank you for your cooperation.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

Enclosure

[16] S. Res. 73 § 12, 114th Cong. (2015).

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

August 11, 2015

Mr. Treve Suazo
CEO
Platte River Networks
5700 Washington Street
Denver, CO 80216

Dear Mr. Suazo:

The Committee on Homeland Security and Governmental Affairs is examining Platte River Networks' role in maintaining former Secretary of State Hillary Clinton's private server during her time leading the State Department. A *Washington Post* article reported that Secretary Clinton hired Platte River Networks in 2013 to maintain the data stored on her non-official server.[1] Given that the server was used to conduct official State Department business, questions have been raised regarding whether classified information was stored on the private server,[2] if that data was secured, who had access to that material, and whether all official documents were appropriately preserved pursuant to the Federal Records Act of 1950.[3]

In order to address these security and preservation concerns and to better understand Platte River Networks' role in maintaining Secretary Clinton's private server, I ask that you please provide the following information and materials:

1. Please produce all documents and communications between or among employees or contractors of Platte River Networks and employees of the State Department referring or relating to Platte River Networks' work related to Secretary Clinton's private server.

2. Please produce all documents and communications between or among employees or contractors of Platte River Networks and Secretary Clinton or any representative of the Clinton family or Clinton Foundation referring or relating to Secretary Clinton's private server.

3. Please produce all contracts between Platte River Networks, Secretary Clinton, the State Department, or any other party referring or relating to Platte River Networks' work related to Secretary Clinton's private server.

---

[1] *See, e.g.*, Carol D. Leonnig, Rosalind S. Helderman, and Tom Hamburger, *FBI Looking Into the Security of Hillary Clinton's Private E-Mail Setup*, THE WASHINGTON POST (Aug. 4, 2015), http://www.washingtonpost.com/politics/fbi-looks-into-security-of-clintons-private-e-mail-setup/2015/08/04/2bdd85ec-3aae-11e5-8e98-115a3cf7d7ae_story.html.

[2] *See* Letter from Ron Johnson, S. Comm. on Homeland Sec. & Gov't Affairs, to David E. Kendall, Williams & Connolly (July 29, 2015).

[3] Federal Records Act, 44 U.S.C. Chapter 31 (2015).

4. Please produce all invoices, bills, and receipts prepared by Platte River Networks or its representatives or agents regarding Platte River Networks' work related to Secretary Clinton's private server.

5. Was Platte River Networks ever made aware that the information on Secretary Clinton's private server may contain classified or sensitive security data? If so, how did Platte River Networks learn about the classified or sensitive information? Please explain.

6. Is Platte River Networks authorized to maintain or access classified information? Please explain.

7. Did any employee of Platte River Networks receive training in the handling of classified information as it relates to Platte River Networks' work on Secretary Clinton's private server?

8. Did any employee of Platte River Networks receive training on preserving federal records pursuant to the Federal Records Act of 1950[4] as it relates to Platte River Networks' work on Secretary Clinton's private server?

Please provide this information and material as soon as possible, but no later than 5:00 p.m. on August 25, 2015. Additionally, I ask that you please provide the Committee with a staff-level briefing to discuss Platte River Networks' role in maintaining the server.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of the Government."[5] Additionally, S. Res. 73 (114th Congress) authorizes the Committee to examine "the efficiency and economy of operations of all branches and functions of the Government with particular reference to (i) the effectiveness of present national security methods, staffing, and processes . . . ."[6] For purposes of this request, please refer to the definitions and instructions in the enclosure.

---

[4] Federal Records Act, 44 U.S.C. Chapter 31 (2015).
[5] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[6] S. Res. 73 § 12, 114th Cong. (2015).

If you have any questions about this request, or concerns about the instructions or requirements in the enclosure, please contact Scott Wittmann of the Committee staff at (202) 224-4751. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

Enclosure

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

August 26, 2015

Mr. David L. Brown
Chief Executive Officer
Web.com Group, Inc.
12808 Gran Bay Parkway West
Jacksonville, FL 32258

Dear Mr. Brown:

The Committee on Homeland Security and Governmental Affairs is examining former Secretary of State Hillary Clinton's use of a private email account and server during her time leading the State Department. According to the Inspector General for the Intelligence Community (IC IG), emails contained on the account and transmitted on the server include national security information collaterally classified as high as Top Secret and subject to Sensitive Compartmented Information control systems, which are reserved for the country's most sensitive intelligence.[1] I write to request your assistance in understanding the role of Web.com Group, Inc. and its subsidiaries, Perfect Privacy, LLC and Network Solutions, LLC, in managing Secretary Clinton's clintonemail.com domain.

On March 12, 2015, I joined Chairman Bob Corker and Chairman Richard Burr in asking the Inspector General of the State Department to examine whether State Department employees sent or received classified manner in an insecure manner.[2] We asked that the State Department IG coordinate with the IC IG in this review.[3] On March 18, 2015, I wrote separately to the State Department IG to inquire whether Secretary Clinton's personal emails included any classified information.[4] On July 23, 2015, the IC IG notified Congress that its limited sampling of a portion of Secretary Clinton's emails had revealed the presence of classified information.[5] On August 11, 2015, the IC IG notified Congress that Secretary Clinton's emails included "information classified up to 'TOP SECRET//SI//TK//NOFORN.'"[6] The presence of such

---

[1] Memorandum for Sen. Richard Burr et al. from I. Charles McCullough, III, Update Classified Material on Personal Electronic Storage Devices (Aug. 11, 2015).
[2] *See* Letter from Senator Bob Corker et al., to U.S. Dep't of State, Office of Inspector Gen. (Mar. 12, 2015).
[3] *Id.*
[4] Letter from Senator Ron Johnson, S. Comm. on Homeland Sec. & Gov't Affairs, to Steve A. Linick, U.S. Dep't of State Office of Inspector Gen. (Mar. 18, 2015).
[5] Memorandum for Sen. Richard Burr et al. from I. Charles McCullough, III, Update to IC IG support to State Department IG (July 23, 2015). The IC IG and State Department IG later clarified that the "emails contained classified information when they were generated and, according to IC classification officials, that information remains classified today." I. Charles McCullough, III, & Steve Linick, Statement from the Inspectors General of the Intelligence Community and the Department of State Regarding the Review of Former Secretary Clinton's Emails (July 24, 2015).
[6] Memorandum for Sen. Richard Burr et al. from I. Charles McCullough, III, Update to IC IG support to State Department IG (Aug. 11, 2015), *available at http://www.grassley.senate.gov/sites/default/files/judiciary/upload/*

sensitive information on a private email system raises concerns about the security and preservation of Secretary Clinton's records.

According to the Internet Corporation for Assigned Names and Numbers (ICANN), the clintonemail.com domain was registered on January 13, 2009.[7] Perfect Privacy, LLC is listed as the registrant for the clintonemail.com domain and Network Solutions, LLC is listed as the registrar for the domain, according to ICANN.[8] The registration for the clintonemail.com domain runs through January 13, 2017.[9] Both Perfect Privacy and Network Solutions are subsidiaries of Web.com Group, Inc.[10] In addition to offering domain name registration and services, Web.com provides file hosting and email services.[11] Perfect Privacy, likewise, offers Internet anonymity by acting as the public registrant of the domain registration rather than the actual domain owner.[12] While it appears that Perfect Privacy, Network Solutions, and Web.com played some role relating to Secretary Clinton's clintonemail.com domain, the nature and extent of this relationship is unknown.

To assist the Committee in better understanding the role of Web.com and its subsidiaries in managing Secretary Clinton's clintonemail.com domain, and to help assess the decision-process culminating in the use of the clintonemail.com domain and the consequences for the security and preservation of federal records, I ask that you provide the following information and materials:

1. Please provide all documents and communications associated with the clintonemail.com domain.

2. Please provide all contact information, including registrant, administrative, technical, and billing information, associated with the clintonemail.com domain for the period January 13, 2009, to the present.

3. Please identify all employees or agents of Web.com Group, Inc., Perfect Privacy, LLC, Network Solutions, LLC, or other subsidiary or affiliated entities with access to the clintonemail.com domain for the period January 13, 2009, to the present.

4. Please provide all log files of activity associated with the clintonemail.com domain for the period January 13, 2009, to the present.

5. Please provide all receipts, invoices, bills, and other payment information associated with the clintonemail.com domain for the period January 13, 2009, to the present.

Classified%20docs%2C%2008-11-15%2C%20ICIG%20CN%20-%20Update%20on%20Classified%20Materials%20on%20Personal%20thumb%20drive.%20Clinton%20server.pdf.

[7] *See* ICANN WHOIS, http://whois.icann.org/en (search for "clintonemail.com") (last accessed Aug. 26, 2015).

[8] *Id.*

[9] *Id.*

[10] Web.com Group, Inc., Annual Report (Form 10-K), at ex. 21.1 (Feb. 28, 2014) [hereinafter "Web.com 10-K"]; Conn. Sec. of State, Business Inquiry (search for "Perfect Privacy LLC") (last accessed Aug. 18, 2015).

[11] Web.com 10-K, *supra* note 12; *see* also Web.com (last accessed Aug. 26, 2015).

[12] Perfect Privacy, perfectprivacy.com (last accessed Aug. 26, 2015).

6. Please produce all communications sent or received by employees of Web.com Group, Inc., Perfect Privacy, LLC, Network Solutions, LLC, or any other subsidiary or affiliated entity referring or relating to the clintonemail.com domain for the period January 13, 2009, to the present.

7. Did Web.com Group, Inc., Perfect Privacy, LLC, Network Solutions, LLC, or any other subsidiary or affiliated entity have access to files, emails, or other content associated with the clintonemail.com domain for the period January 13, 2009, to the present? If so, please produce this material.

8. Was Web.com Group, Inc., Perfect Privacy, LLC, Network Solutions, LLC, or any other subsidiary or affiliated entity ever made aware that the information associated with the clintonemail.com domain may contain classified or sensitive security data? Please explain.

9. Is Web.com Group, Inc., Perfect Privacy, LLC, Network Solutions, LLC, or any other subsidiary or affiliated entity authorized to maintain or access classified information? Please explain.

10. Did any employee of Web.com Group, Inc., Perfect Privacy, LLC, Network Solutions, LLC, or any other subsidiary or affiliated entity receive training in the handling of classified information associated with the clintonemail.com domain?

11. Did any employee of Web.com Group, Inc., Perfect Privacy, LLC, Network Solutions, LLC, or any other subsidiary or affiliated entity receive training on preserving federal records pursuant to the Federal Records Act of 1950[13] as it relates to information associated with the clintonemail.com domain?

Please provide this information as soon as possible but no later than 5:00 p.m. on September 9, 2015. To the extent possible, please provide unclassified responses to these questions. Should a complete response require transmission of classified information, please send such information under separate cover, via the Office of Senate Security

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of the Government."[14] Additionally, S. Res. 73 (114th Congress) authorizes the Committee to examine "the efficiency and economy of operations of all branches and functions of the Government with particular reference to (i) the effectiveness of present national security methods, staffing, and processes . . . ."[15] The

[13] Federal Records Act, 44 U.S.C. Chapter 31 (2015).
[14] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[15] S. Res. 73 § 12, 114th Cong. (2015).

Committee also has specific jurisdiction over federal records and government information.[16] For purposes of this request, please refer to the definitions and instructions in the enclosure.

If you have any questions about this request, please ask your staff to contact David Brewer or Liam McKenna of the Committee staff at (202) 224-4751. Thank you for your attention to this important matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

Enclosure

[16] S. Rule XXV(k).

United States Senate

WASHINGTON, DC 20510

September 4, 2015

VIA ELECTRONIC TRANSMISSION

Mr. Bryan M. Pagliano
c/o Mark MacDougall, Esq.
Constance O'Connor, Esq.
Connor Mullin, Esq.
Sean D'Arcy, Esq.
Akin Gump Strauss Hauer & Feld
1333 New Hampshire Ave NW,
Washington, DC 20036

Dear Mr. Pagliano,

According to federal campaign finance records, you "[were] paid by Clinton's Senate leadership PAC through April of 2009," where you served as the campaign's IT director.[1] According to news reports, the following month, you began working for the State Department as an IT Specialist and continued to act as the lead specialist responsible for Secretary Clinton's private server in New York.[2] From 2010-2012, you were compensated at the GS-15 level by the Department.[3] You reportedly worked for the Department as an IT Specialist and were tasked with overseeing the maintenance and operability of Secretary Clinton's non-government server. Her use of that server substantially hindered the ability of State Department personnel to fully comply with Freedom of Information Act (FOIA) requests, which has generated substantial related litigation with FOIA requestors. In addition, according to the Inspector General for the Intelligence Community, Secretary Clinton's email records included "information classified up to 'TOP SECRET//SI//TK//NOFORN.'"[4]

---

[1] Carol D. Leonnig, Rosalind S. Helderman, Tom Hamburger, "FBI looking into the security of Hillary Clinton's private email setup," The Washington Post (August 5, 2015). Accessible at http://www.washingtonpost.com/politics/fbi-looks-into-security-of-clintons-private-e-mail-setup/2015/08/04/2bdd85ec-3aae-11e5-8e98-115a3cf7d7ae_story.html.

[2] *Id.*

[3] FedsDataCenter. Bryan Pagliano Salary Search 2012; Bryan Pagliano Salary Search 2011. Bryan Pagliano Salary Search 2010. Accessible at http://www.fedsdatacenter.com/federal-pay-rates/index.php?n=pagliano&l=&a=&o=&y=2010.

[4] Memorandum for Sen. Richard Burr et al. from I. Charles McCullough, III, Update Classified Material on Personal Electronic Storage Devices (Aug 11, 2015), *available at* *http://www.grassley.senate.gov/sites/default/files/judiciary/upload/Classified%20docs%2C%2008-11 15%2C%20ICIG%20CN%20-%20Update%20on%20Classified%20Materials%20on%20Personal%20thumb%20drive.%20Clinton%20server.pdf.*

Accordingly, the Judiciary Committee, which has jurisdiction over FOIA, and the Homeland Security and Governmental Affairs Committee, which has jurisdiction over national security procedures and federal records, are investigating the circumstances surrounding the use of that non-government email server. It appears likely that you have unique information relevant to the Committees' inquiry.

On August 19, 2015, staff of the Homeland Security and Governmental Affairs Committee contacted you to inquire whether you would speak with the Committee. On your behalf, your attorney declined and subsequently indicated that you would avail yourself of constitutional protections.

On August 28, 2015, staff of the Judiciary Committee reached out to you in an attempt to schedule an interview to discuss those matters. On September 1, 2015, in response to a question about whether you were paid by any outside entity during your tenure at the State Department, your attorneys notified Judiciary Committee staff unequivocally that they will not be "answering questions or providing any information on [your] behalf." In addition, your attorneys stated that "[i]f any effort is made to compel our client's testimony, Mr. Pagliano will decline to answer such questions in reliance on his right under the 5th Amendment."

Your right under the Fifth Amendment to avoid being compelled to provide testimony that might be used to prosecute you is a fundamental individual right. The Committees will certainly respect and defer to any legitimate assertion of an individual's constitutional rights.

With that being said, the Committees also need the unique information you likely have in order to exercise their oversight functions under the Constitution, which are unrelated to any potential prosecution or criminal inquiry. Thus, the Committees have the authority to obtain an immunity order, to acquire the information they need, while also protecting your right against self-incrimination.[5]

On behalf of the Committees, we write to request that you make yourself available to provide information. Given the issues raised by your attorney and in order for the Committees to assess whether it would be appropriate for either Committee to consider obtaining an immunity order in these circumstances, we ask that your attorneys meet with the Committees' staff to explore how to obtain the unique information you possess while respecting your constitutional rights, such as the possibility of a proffer session so that we can better understand what your testimony would be without any waiver of your rights.

---

[5] 18 U.S.C. §6005 Congressional proceedings; 18 U.S.C. § 6002. Immunity generally; 2 U.S.C. §288b(d) Immunity proceedings; 2 U.S.C. §288f Immunity proceedings.

Please respond no later than September 10, 2015. If you have questions, please have your attorney contact Josh Flynn-Brown of the Judiciary Committee staff at (202) 224-5225 or David Brewer of the Homeland Security and Governmental Affairs Committee staff at (202) 224-4751.

Sincerely,

Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs

Charles E. Grassley
Chairman
Committee on the Judiciary

cc: The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

United States Senate

WASHINGTON, DC 20510

September 11, 2015

VIA ELECTRONIC TRANSMISSION

The Honorable John F. Kerry
Secretary of State
Office of the Secretary
United States Department of State
2201 C Street, N.W.
Washington, D.C. 20520

Dear Secretary Kerry:

As you are aware, the Judiciary Committee and the Homeland Security and Governmental Affairs Committee are currently investigating Secretary Clinton's email practices and the potential that those practices caused interference with Freedom of Information Act (FOIA) requests and possibly interfered with congressional inquiries. As you also know, the Judiciary Committee has legislative jurisdiction over FOIA and the Homeland Security and Governmental Affairs Committee has jurisdiction over national security procedures and federal records.

The Clinton Campaign has stated that Mr. Bryan M. Pagliano was personally compensated by Secretary Clinton to manage and maintain the server she used for government business while he was also employed by the Department of State.[1] One of Mr. Pagliano's supervisors was Mr. Steven C. Taylor, current Chief Information Officer for the Department. Mr. Taylor likely has knowledge relevant to the Committee's investigation and Mr. Pagliano's role in information systems practices during Secretary Clinton's tenure. Accordingly, the Committees request that you make Mr. Taylor available for a transcribed interview with Committee staff.

In addition to an interview with Mr. Taylor, please provide the following information and materials:

1. Please identify Mr. Pagliano's supervisors other than Mr. Taylor.

2. All records relating to Mr. Pagliano's communications with Secretary Clinton.

3. All records relating to Mr. Pagliano's communications with Secretary Clinton's senior staff, including Huma Abedin, Cheryl Mills, and Jake Sullivan.

---

[1] Rosalind S. Helderman, Carol D. Leonnig, "Clintons personally paid State Department staffer to maintain server," THE WASHINGTON POST (September 5, 2015).

4. All records relating to Mr. Pagliano's communications regarding the server Secretary Clinton used for official government communications.

5. All records relating to Mr. Pagliano's hiring as a full-time employee at the State Department.

6. All records relating to Mr. Pagliano's communications regarding security measures employed for the server, evidence of breaches, or hacks of the server.

7. All records relating to Mr. Pagliano's communications regarding compliance with FOIA requests, congressional inquiries, or inquiries from the Office of Inspector General.

8. All records relating to Mr. Pagliano's communications regarding records retention practices or requirements relating to the server.

9. All personnel records for Mr. Pagliano including performance reports, all approved timesheets, leave requests, and all requests for paid or unpaid excused absences or administrative leave.

10. All records relating to any payments made by the Department or by Secretary Clinton or her senior staff to Mr. Pagliano for his services related to Secretary Clinton's server.

11. All records relating to communications between Mr. Pagliano and the Department's Designated Agency Ethics Official.

12. Please provide a description of Mr. Pagliano's position and responsibilities at the Department of State.

13. Was the Department of State aware that, in addition to getting paid as a full-time employee at the Department, Mr. Pagliano was also getting paid to manage Secretary Clinton's private server?
    a. If so, when was the Department of State made aware of this information?
    b. If so, who disclosed this information to the Department of State?
    c. If so, did the amount of Mr. Pagliano's second salary comply with Department of State or federal regulations regarding how much extra annual income full-time government employees can make?

14. Please identify other employees of the Bureau of Information Resource Management that may have knowledge of Mr. Pagliano's role in information systems practices at the State Department.

Please number your responses according to their corresponding questions. Please respond by September 24, 2015. To set up a mutually agreeable time for an interview please contact Josh Flynn-Brown of the Judiciary Committee staff at (202) 224-5225 or David Brewer of the Homeland Security and Governmental Affairs staff at (202) 224-4751. Thank you for your cooperation with the Committees' inquiry and for your prompt attention to this request.

Sincerely,

Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs

Charles E. Grassley
Chairman
Committee on the Judiciary

cc: The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

United States Senate

WASHINGTON, DC 20510

September 14, 2015

VIA ELECTRONIC TRANSMISSION

The Honorable Loretta Lynch
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Attorney General Lynch:

We are writing to you in regard to Fifth Amendment issues relating to Mr. Bryan Pagliano, the IT Specialist who was responsible for managing Secretary of State Hillary Clinton's non-government email server during her time leading the State Department. As you may already know, the Judiciary Committee, which has jurisdiction over the Freedom of Information Act (FOIA), as well as certain national security matters, and the Homeland Security and Governmental Affairs Committee, which has jurisdiction over national security procedures and federal records, are investigating the circumstances surrounding the use of that non-government email server. According to news reports, the FBI is also "looking into" the security of former Secretary Clinton's private email setup, although it unclear whether the FBI has opened a full field criminal investigation, and if so, who are the subjects of that investigation.[1]

Upon attempting to contact Mr. Pagliano, his attorneys informed us that "[i]f any effort is made to compel our client's testimony, Mr. Pagliano will decline to answer such questions in reliance on his right under the 5th Amendment." We subsequently replied to Mr. Pagliano's attorneys, writing that the Committees will certainly respect and defer to any legitimate assertion of an individual's constitutional rights, but also noting that the Committees have the authority to obtain an immunity order to acquire the information needed for oversight while also protecting Mr. Pagliano's right against self-incrimination. We requested that Mr. Pagliano's attorneys meet with the Committees' staff to explore the possibility of a proffer session in order to assess whether it might be appropriate to consider seeking an immunity order.

Mr. Pagliano's attorneys responded stating, among other things, that any proffer session on the part of Mr. Pagliano or his attorneys creates the risk that he will later be deemed to have waived his constitutional protections. Although we are seeking additional information from the State Department through requests to interview other witnesses who worked with Mr. Pagliano and requests for records of Mr. Pagliano's communications regarding former Secretary Clinton's

---

[1] Carol D. Leonnig, Rosalind S. Helderman, Tom Hamburger, *FBI Looking into the Security of Hillary Clinton's Private email setup*, THE WASHINGTON POST (Aug. 5, 2015), available at http://www.washingtonpost.com/politics/fbi-looks-into-security-of-clintons-private-e-mail-setup/2015/08/04/2bdd85ec-3aae-11e5-8e98-115a3cf7d7ae_story.html.

email server, the State Department has been extremely unresponsive to previous requests. This leaves the Committees with very little information on which to base a decision as important as whether to seek an immunity order to compel Mr. Pagliano's testimony.

Accordingly, we request that you provide us with responses to the following questions by September 21, 2015:

1. If Mr. Pagliano or his attorneys provide information to the Committees' counsel during a confidential proffer to assist the Committees in deciding whether to seek an immunity order, with the Committees' express agreement that the witness is not waiving his Fifth Amendment rights, would the Department of Justice consider the proffer to be a waiver of his Fifth Amendment rights? Please explain why or why not.

2. Does the FBI or any other component of the Department of Justice currently have a criminal investigation open relating to Secretary Clinton's private server? If so, is Mr. Pagliano a subject of that investigation?

3. Does the FBI or any other component of the Department of Justice currently have any other type of inquiry open relating to Secretary Clinton's private server? If so, please explain the nature and status of that inquiry and indicate whether Mr. Pagliano is a subject of that inquiry.

4. Does the FBI or any other component of the Department of Justice currently have a criminal investigation open relating to Mr. Pagliano, including any concerning his concurrent employment by the State Department and the Clintons, or concerning allegations that he failed to report to the government his outside income from the Clintons?

5. Does the FBI or any other component of the Department of Justice currently have any other type of inquiry open relating to Mr. Pagliano? If so, please explain the nature and status of that inquiry.

6. Has the FBI or any other component of the Justice Department engaged in negotiations with Mr. Pagliano regarding any potential proffer, plea, or immunity agreement? If so, please explain.

7. If the Department does enter into any proffer, plea, or immunity agreement with Mr. Pagliano, will you please ensure that such an agreement requires that Mr. Pagaliano cooperate fully with our Committees' investigations? If not, please explain why not.

Thank you for your attention to this matter. If you have any questions, please contact Patrick Davis of the Judiciary Committee staff at (202) 224-5225 or David Brewer of the Homeland Security and Governmental Affairs Committee staff at (202) 224-4751.

Sincerely,

Charles E. Grassley
Chairman
Committee on the Judiciary

Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs

Cc: The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

United States Senate
WASHINGTON, DC 20510

September 14, 2015

Mr. Bryan M. Pagliano
c/o Mark MacDougall, Esq.
Constance O'Connor, Esq.
Connor Mullin, Esq.
Sean D'Arcy, Esq.
Akin Gump Strauss Hauer & Feld LLP
1333 New Hampshire Ave NW
Washington, DC 20036

Dear Mr. Pagliano:

We were disappointed to receive a letter, dated September 9, 2015, from your attorneys indicating that you and your attorneys would "decline to participate in the explanatory discussions or proffer session with the Committees' staff . . . ."[1] We continue to believe that you possess information about former Secretary of State Hillary Clinton's use of a private email account and server that is unavailable elsewhere and that is relevant to the Committees' oversight duties. We respectfully request that you reconsider your decision and accept our offer to engage with the Committees on a path toward obtaining the pertinent information you possess.

As we noted in our initial letter, we respect your constitutional rights and we will defer to any legitimate personal assertion of your Fifth Amendment privilege against self-incrimination. We had hoped to explore options for obtaining your testimony while respecting your constitutional rights. As your attorneys assert, the applicable statute for obtaining an immunity order, 18 U.S.C. § 6005, does not require a proffer session as a prerequisite to the issuance of an order by a U.S. district court. Nonetheless, as former House Counsel and current Akin Gump Senior Counsel Stan Brand opined during the House Committee on Oversight and Government Reform's evaluation of former IRS executive Lois Lerner's assertion of the Fifth Amendment, a proffer session "is a practice that has developed to allow the government, or in this case the Committee, to determine whether it wishes to seek immunity for the witness through a formal application to the Court."[2] He continued:

> It is used by the government (again in this case the Committee) to evaluate the scope, value and content of a witnesses [*sic*] testimony to determine whether the committee should, in its judgment, seek an order pursuant to 18 U.S.C. § 6005, requiring such individual to testify.[3]

---

[1] Letter from Mark J. MacDougall et al., Akin Gump Strauss Hauer & Feld LLP, to Ron Johnson, S. Comm. on Homeland Sec. & Governmental Affairs, & Charles E. Grassley, S. Comm. on the Judiciary (Sept. 9, 2015).
[2] Letter from Stan Brand, Brand Law Group, to Democratic Staff, House Committee on Oversight and Government Reform (Feb. 28, 2014), *available at* http://democrats.oversight.house.gov/sites/democrats.oversight.house.gov/files/migrated/uploads/Democratic%20Staff%20House%20Committee%20on%20Oversight%20%20Gov't%20Reform%20re%20attorney%20proffers%20(2-28-14%20%20sbm).pdf.
[3] *Id.*

In this case, the Committees have no information about the nature of your potential criminal liability or whether the value of your testimony in advancing the Committee's oversight obligations would justify the steps necessary to immunize your testimony.

While your attorneys correctly noted that you have not asked for an immunity order, their unwillingness to engage in any discussions toward a mutual accommodation frustrates our ability to explore offering you protection from legal jeopardy for your testimony. It also frustrates our ability to carry out our constitutional oversight obligations. Therefore, we respectfully request that your attorneys meet with our staff to discuss these issues further, and ask that you respond to the Committees no later than Wednesday, September 16, 2015. Please know, however, that the Committees will continue to explore all options to obtain the unique information we believe that you possess.

Thank you for your attention to this important matter.

Sincerely,

Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs

Charles E. Grassley
Chairman
Committee on the Judiciary

cc: The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

September 16, 2015

The Honorable James R. Clapper
Director of National Intelligence
Office of the Director of National Intelligence
Washington, DC 20511

Dear Director Clapper:

The Committee on Homeland Security and Governmental Affairs is examining former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. According to Charles McCullough, Inspector General for the Intelligence Community (IC IG), emails contained on the account and transmitted on the server include national security information collaterally classified as high as Top Secret and subject to Sensitive Compartmented Information control systems, which are reserved for the country's most sensitive intelligence.[1] The use of a non-official and unsecured platform could leave sensitive State Department information and intelligence from other agencies vulnerable to intrusion and removal. I write to request your assistance in understanding the steps that the intelligence community is taking to assess and mitigate any potential security damage caused by Secretary Clinton's use of a personal email account and server.

On March 12, 2015, I joined Chairman Bob Corker and Chairman Richard Burr in asking the Inspector General of the State Department to examine whether State Department employees sent or received classified information in an insecure manner.[2] We asked that the State Department IG coordinate with the IC IG in this review.[3] On March 18, 2015, I wrote separately to the State Department IG to inquire whether Secretary Clinton's personal emails included any classified information.[4] On July 23, 2015, the IC IG notified Congress that its limited sampling of a portion of Secretary Clinton's emails had revealed the presence of classified material.[5] On August 11, 2015, the IC IG notified Congress that Secretary Clinton's emails included "information classified up to 'TOP SECRET//SI//TK//NOFORN.'"[6]

---

[1] Memorandum for Sen. Richard Burr et al. form I. Charles McCullough, III, Update Classified Material on Personal Electronic Storage Devices (Aug 11, 2015).

[2] *See* Letter from Senator Bob Corker et al., to U.S. Dep't of State, Office of Inspector Gen. (Mar. 12, 2015).

[3] *Id.*

[4] Letter from Senator Ron Johnson, S. Comm. on Homeland Sec. & Gov't Affairs, to Steve A. Linick, U.S. Dep't of State Office of Inspector Gen. (Mar. 18, 2015).

[5] Memorandum for Sen. Richard Burr et al. from I. Charles McCullough, III, Update to IC IG support to State Department IG (July 23, 2015). The IC IG and State Department IG later clarified that the "emails contained classified information when they were generated and, according to IC classification officials, that information remains classified today." I. Charles McCullough, III, & Steve Linick, Statement from the Inspectors General of the Intelligence Community and the Department of State Regarding the Review of Former Secretary Clinton's Emails (July 24, 2015).

[6] Memorandum for Sen. Richard Burr et al. form I. Charles McCullough, III, Update Classified Material on Personal

The existence of such sensitive information on an unofficial and unclassified server raises serious security concerns about whether that information was compromised. To date, reports indicate there are as many as 305 emails that potentially contained classified data that were once kept on Secretary Clinton's personal, unsecure server and transmitted on her personal email account.[7] Another report indicates that some of Secretary Clinton's emails may have been exposed in the March 2013 Sidney Blumenthal hack, but that the State Department took no action to "shore up the security of the former secretary of state's private computer server."[8] Given the recent cybersecurity breaches that have afflicted federal agencies, it is imperative that the State Department and the intelligence community continue to maintain stringent safeguards when receiving and transmitting classified data to ensure that our nation's most sensitive material remains secure.

In order to determine what actions the intelligence community is taking to assess and mitigate the potential security vulnerabilities relating to Secretary Clinton's use of a private email and server for official State Department business, I respectfully request the following information and materials:

1. What resources is the intelligence community putting into place to assess and mitigate the potential damage and security risks caused by Secretary Clinton's use of an unsecure sever to conduct official Department business? Please explain.

2. When did the intelligence community learn about the potential security vulnerabilities resulting from Secretary Clinton's use of an unsecure server and email account to conduct official State Department business? How soon did the intelligence community take action to begin to access and mitigate potential damage and security risks caused by the use of an unsecure server and email account?

3. Has the intelligence community conducted an assessment of the security vulnerabilities caused by Secretary Clinton's use of an unsecure server and email account to conduct official State Department business, including the transmission of classified and sensitive information over an unclassified email system? Please explain.
    a. If so, please produce all communications, analyses, or findings referring or relating to the intelligence community's assessment of the potential security vulnerabilities caused by Secretary Clinton's use of an unsecure server and email account.

Electronic Storage Devices (Aug 11, 2015), *available at http://www.grassley.senate.gov/sites/default/files/judiciary/upload/Classified%20docs%2C%2008-11 15%2C%20ICIG%20CN%20- %20Update%20on%20Classified%20Materials%20on%20Personal%20thumb%20drive.%20Clinton%20server.pdf.*

[7] Stephen Braun, *US: Up to 305 Clinton emails might have classified* data, THE WASHINGTON POST (Aug. 18, 2015), http://www.washingtonpost.com/politics/us-up-to-305-clinton-emails-might-have-classified-data/2015/08/17/123bc3e2-4517-11e5-9f53-d1e3ddfd0cda_story.html.

[8] Anita Kumar, Marisa Taylor, & Greg Gordon, *State Department did nothing to protect Clinton emails after hack*, MCCLATCHY (Aug. 20, 2015), http://www.mcclatchydc.com/news/politics-government/election/article31628900.html.

b. If the intelligence community has not conducted an assessment of the potential damage caused by Secretary Clinton's use of an unsecure server and email account, please explain why.

4. Please describe the potential physical security and cybersecurity vulnerabilities that could be exposed through the use of an unsecure server and email account to conduct official State Department business.

5. Is the intelligence community in the process of determining whether any information received or transmitted on Secretary Clinton's private server or email account was compromised by a hacker or foreign adversary? Please explain.

6. Is the intelligence community in the process of determining whether any classified information transmitted on Secretary Clinton's private server or email account was sent to a person, either directly or indirectly, without clearance to receive such information? Please explain.

7. Has the intelligence community changed or modified its sources, methods, or practices for intelligence gathering or review as a result of Secretary Clinton's use of a private server or email account? Please explain.

8. Is the intelligence community aware of whether any covert assets have been endangered as a result of classified information being transmitted on an unsecure server? Please explain.

9. What, if any, policies or procedures has the intelligence community changed or modified to ensure that all employees in the intelligence community receive or transmit classified information in a secure manner? Please explain.

Please provide this information and material as soon as possible, but no later than 5:00 p.m. on September 30, 2015. To the extent possible, please provide unclassified responses to these questions. Should a complete response require transmission of classified information, please send such information under separate cover, via the Office of Senate Security.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of the Government."[9] Additionally, S. Res. 73 (114th Congress) authorizes the Committee to examine "the efficiency and economy of operations of all branches and functions of the Government with particular reference to (i) the effectiveness of present national security methods, staffing, and processes . . . ."[10] For purposes of this request, please refer to the definitions and instructions in the enclosure.

[9] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[10] S. Res. 73 § 12, 114th Cong. (2015).

If you have any questions about this request, please ask your staff to contact Scott Wittmann of the Committee staff at (202) 224-4751. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

Enclosure

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

September 16, 2015

The Honorable John Kerry
Secretary of State
U.S. Department of State
2201 C Street, NW
Washington, DC 20520

Dear Secretary Kerry:

The Committee on Homeland Security and Governmental Affairs is examining former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. According to the Inspector General for the Intelligence Community (IC IG), emails contained on the account and transmitted on the server include national security information collaterally classified as high as Top Secret and subject to Sensitive Compartmented Information control systems, which are reserved for the country's most sensitive intelligence.[1] The use of a non-official and unsecured platform could leave sensitive State Department information and intelligence from other agencies vulnerable to intrusion and removal. I write to request your assistance in understanding the steps that the State Department is taking to assess and mitigate any potential security damage caused by Secretary Clinton's use of a personal email account and server.

On March 12, 2015, I joined Chairman Bob Corker and Chairman Richard Burr in asking the Inspector General of the State Department to examine whether State Department employees sent or received classified information in an insecure manner.[2] We asked that the State Department IG coordinate with the IC IG in this review.[3] On March 18, 2015, I wrote separately to the State Department IG to inquire whether Secretary Clinton's personal emails included any classified information.[4] On July 23, 2015, the IC IG notified Congress that its limited sampling of a portion of Secretary Clinton's emails had revealed the presence of classified material.[5] On

---

[1] Memorandum for Sen. Richard Burr et al. form I. Charles McCullough, III, Update Classified Material on Personal Electronic Storage Devices (Aug 11, 2015).
[2] *See* Letter from Senator Bob Corker et al., to U.S. Dep't of State, Office of Inspector Gen. (Mar. 12, 2015).
[3] *Id.*
[4] Letter from Senator Ron Johnson, S. Comm. on Homeland Sec. & Gov't Affairs, to Steve A. Linick, U.S. Dep't of State Office of Inspector Gen. (Mar. 18, 2015).
[5] Memorandum for Sen. Richard Burr et al. from I. Charles McCullough, III, Update to IC IG support to State Department IG (July 23, 2015). The IC IG and State Department IG later clarified that the "emails contained classified information when they were generated and, according to IC classification officials, that information remains classified today." I. Charles McCullough, III, & Steve Linick, Statement from the Inspectors General of the Intelligence Community and the Department of State Regarding the Review of Former Secretary Clinton's Emails (July 24, 2015).

August 11, 2015, the IC IG notified Congress that Secretary Clinton's emails included "information classified up to 'TOP SECRET//SI//TK//NOFORN.'"[6]

The existence of such sensitive information on an unclassified official and unofficial server raises serious security concerns about whether that information was compromised. To date, reports indicate there are as many as 305 emails that potentially contained classified data that were once kept on Secretary Clinton's personal, unsecure server and transmitted on her personal email account.[7] Another report indicates that some of Secretary Clinton's emails may have been exposed in the March 2013 Sidney Blumenthal hack, but that the State Department took no action to "shore up the security of the former secretary of state's private computer server."[8] Given the recent cybersecurity breaches that have afflicted federal agencies, it is imperative that the State Department and the intelligence community continue to maintain stringent safeguards when receiving and transmitting classified data to ensure that our nation's most sensitive material remains secure.

In order to determine what actions the State Department is taking to assess and mitigate the potential security vulnerabilities relating to Secretary Clinton's use of a private email and server for official State Department business, I respectfully request the following information and materials:

1. What resources is the State Department putting into place to assess and mitigate the potential damage and security risks caused by Secretary Clinton's use of an unsecure sever to conduct official Department business? Please explain.

2. Has the State Department conducted an assessment of the security vulnerabilities caused by Secretary Clinton's use of an unsecure server and email account to conduct official business, including the transmission of classified and sensitive information over an unclassified email system? Please explain.
    a. If so, please produce all communications, analyses, or findings referring or relating to the Department's assessment of the potential security vulnerabilities caused by Secretary Clinton's use of an unsecure server and email account.
    b. If the State Department has not conducted an assessment of the potential damage caused by Secretary Clinton's use of an unsecure server and email account, please explain why.

---

[6] Memorandum for Sen. Richard Burr et al. form I. Charles McCullough, III, Update Classified Material on Personal Electronic Storage Devices (Aug 11, 2015), *available at http://www.grassley.senate.gov/sites/default/files/judiciary/upload/Classified%20docs%2C%2008-11 15%2C%20ICIG%20CN%20-%20Update%20on%20Classified%20Materials%20on%20Personal%20thumb%20drive.%20Clinton%20server.pdf.*

[7] Stephen Braun, *US: Up to 305 Clinton emails might have classified* data, THE WASHINGTON POST (Aug. 18, 2015), http://www.washingtonpost.com/politics/us-up-to-305-clinton-emails-might-have-classified-data/2015/08/17/123bc3e2-4517-11e5-9f53-d1e3ddfd0cda_story.html.

[8] Anita Kumar, Marisa Taylor, & Greg Gordon, *State Department did nothing to protect Clinton emails after hack*, MCCLATCHY (Aug. 20, 2015), http://www.mcclatchydc.com/news/politics-government/election/article31628900.html.

3. Please describe the potential physical security and cybersecurity vulnerabilities that could be exposed through the use of an unsecure server and email account to conduct official State Department business.

4. Is the Department in the process of determining whether any information received or transmitted on Secretary Clinton's private server or email account was compromised by a hacker or foreign adversary? Please explain.

5. Is the Department in the process of determining whether any classified information transmitted on Secretary Clinton's private server or email account was sent to a person, either directly or indirectly, without clearance to receive such information? Please explain.

6. What, if any, policies or procedures has the State Department changed or modified to ensure that all of Department employees receive or transmit classified information in a secure manner? Please explain.

7. Has the State Department determined the number of emails that were transmitted from the unclassified official State Department email system to Secretary Clinton's private server or email account that contained classified or sensitive information? Please explain.

Please provide this information and material as soon as possible, but no later than 5:00 p.m. on September 30, 2015. To the extent possible, please provide unclassified responses to these questions. Should a complete response require transmission of classified information, please send such information under separate cover, via the Office of Senate Security.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of the Government."[9] Additionally, S. Res. 73 (114th Congress) authorizes the Committee to examine "the efficiency and economy of operations of all branches and functions of the Government with particular reference to (i) the effectiveness of present national security methods, staffing, and processes . . . ."[10] For purposes of this request, please refer to the definitions and instructions in the enclosure.

[9] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[10] S. Res. 73 § 12, 114th Cong. (2015).

If you have any questions about this request, please ask your staff to contact Scott Wittmann of the Committee staff at (202) 224-4751. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

Enclosure

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

September 18, 2015

Clinton Executive Services Corp.
c/o Ms. Rorrie Gregorio
Marcum LLP
750 Third Avenue
11th Floor
New York, NY 10017

Dear Ms. Gregorio:

The Committee on Homeland Security and Governmental Affairs is examining former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. The Committee has learned that Clinton Executive Services Corp. (CESC) contracted with Platte River Networks in 2013 to support and maintain Secretary Clinton's private server. While the exact nature and extent of CESC's involvement with Secretary Clinton's private email and server is unknown, you are named as the point of contact for CESC in its agreement with Platte River. You also are identified on monthly invoices issued by Platte River to CESC and an apparently related entity, ZFS Holdings, LLC. Accordingly, I request your assistance in better understanding the role of CESC and ZFS Holdings, LLC, relating to Secretary Clinton's private email account and server.

To help the Committee better understand the role of CESC and ZFS Holdings, LLC, relating to Secretary Clinton's private email account and server, and to help assess the decision-making process culminating in the use of the private email account and server and the consequences for the security and preservation of federal records, I ask that you provide the following information and materials:

1. Please provide the articles of incorporation and bylaws for Clinton Executive Services Corp.

2. Please provide the articles of incorporation and bylaws for ZFS Holdings, LLC.

3. Please identify all current and former officers and board members of Clinton Executive Services Corp.

4. Please identify all current and former officers and board members of ZFS Holdings, LLC.

5. Please produce all documents referring or relating to the clintonemail.com domain or the hardware or software on which clintonemail.com domain services, such as email, were hosted or otherwise supported.

6. Please produce all communications sent or received by officers, board members, employees, or agents of CESC referring or relating to the clintonemail.com domain or the hardware or software on which clintonemail.com domain services, such as email, were hosted or otherwise supported.

7. Please produce all communications sent or received by officers, board members, employees, or agents of CESC referring or relating to Secretary Clinton's use of private email account and server during her time as Secretary of State.

Please provide this information as soon as possible but no later than 5:00 p.m. on October 2, 2015. If you are not in possession of some or all of the information and materials requested above, please notify the Committee of the individuals or entities that are in possession of the information and materials to the best of your knowledge.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of the Government."[1] Additionally, S. Res. 73 (114th Congress) authorizes the Committee to examine "the efficiency and economy of operations of all branches and functions of the Government with particular reference to (i) the effectiveness of present national security methods, staffing, and processes . . . ."[2] The Committee also has specific jurisdiction over federal records and government information.[3] For purposes of this request, please refer to the definitions and instructions in the enclosure.

If you have any questions about this request, please ask your staff to contact David Brewer of the Committee staff at (202) 224-4751. Thank you for your attention to this important matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

Enclosure

---

[1] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[2] S. Res. 73 § 12, 114th Cong. (2015).
[3] S. Rule XXV(k).

United States Senate
WASHINGTON, DC 20510

September 21, 2015

The Honorable John Kerry
Secretary
U.S. Department of State
22201 C Street, NW
Washington, DC 20520

Dear Secretary Kerry:

The Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary are continuing to examine former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. On July 9, 2015, the Committee on Homeland Security and Governmental Affairs wrote to you about the Department's procedures regarding its compliance with Freedom of Information Act (FOIA) requests for Secretary Clinton's emails. On March 27, 2015, the Committee on the Judiciary wrote to you regarding concerns that Secretary Clinton's email practices may have interfered with State Department FOIA compliance. In addition, on August 19, 2015, the Judiciary Committee wrote to you about reports of disagreements between FOIA specialists and Office of the Legal Advisor attorneys that may have caused at least one classified email to be released publicly. The Committees write today to request clarification to better understand the Department's policies for employees who transmit or receive sensitive information on official and unofficial email systems when conducting State Department business.

In the State Department's response to the Committee on Homeland Security and Governmental Affairs' July 9 letter, Julia Frifield, the Department's Assistant Secretary for Legislative Affairs, wrote that "the Department's team of email reviewers is redacting and classifying [Secretary Clinton's emails] in accordance with the Freedom of Information Act and Executive Order 13526."[1] According to recent reports, however, the State Department publicly released at least one email that "contained intelligence from the Defense Intelligence Agency (DIA), the National Security Agency (NSA), and the National Geospatial-Intelligence Agency (NGA)."[2] The public release of this email appears to conflict with Executive Order 13526, which specifies that "information shall be declassified or downgraded by . . . the official who authorized the original classification."[3] Because the email contained sensitive information from other intelligence agencies, it appears that the State Department did not have proper authorization to declassify and release such information pursuant to Executive Order 13526.[4]

---

[1] See Letter from Julia Frifield, Assistant Secretary, Legislative Affairs, U.S. Dep't of State (Aug. 11, 2015) (on file with the Comm.).
[2] Catherine Herridge, *Exclusive: State Dept.-released Clinton email had classified intel from 3 agencies, in possible violation*, FOX NEWS (Aug. 26, 2015).
[3] Exec. Order No. 13526, 75 Fed. Reg. 707 (Jan. 5, 2010).
[4] Catherine Herridge, *Exclusive: State Dept.-released Clinton email had classified intel from 3 agencies, in possible violation*, FOX NEWS (Aug. 26, 2015).

In addition to the fact that the State Department has released classified information, this incident raises a number of additional concerns regarding the exchange of classified material between unclassified official State Department email systems and unsecure non-official email systems. According to the Inspector General for the Intelligence Community (IC IG), emails contained on Secretary Clinton's private account and transmitted on the server include national security information collaterally classified as high as Top Secret and subject to Sensitive Compartmented Information control systems, which are reserved for the country's most sensitive intelligence.[5] The use of an unsecured non-official platform could leave sensitive State Department information and intelligence from other agencies vulnerable to unauthorized intrusion and removal. Further, the use of unclassified official email systems to send and receive intelligence could also put sensitive information at risk, potentially jeopardizing national security.

As the Department works to review and process Secretary Clinton's email records, the Committees seek to ensure that the Department is carefully assessing those documents in order to prevent the public release of classified information. Further, we are deeply concerned by reports that former State Department employees, including Secretary Clinton, used official and unofficial unclassified email systems to transmit and receive classified information. In order to assist the Committee's oversight obligations, we request that you provide the following information:

1. Did the State Department ever evaluate Secretary Clinton's private server and email account to determine whether it complied with the State Department's requirements to receive and transmit classified information? Please explain.
    a. If so, what determination did the State Department make about whether Secretary Clinton's private server and email account complied with State Department's requirements to receive and transmit classified information? Please provide all legal analyses used by the State Department to make that determination.
    b. If the State Department evaluated Secretary Clinton's private server and email account, please provide the dates for which such an evaluation occurred and the official(s) who conducted the evaluation.

2. Did the State Department authorize Secretary Clinton to use her private server and email account to conduct official State Department business, including the exchange of classified information?
    a. If so, please provide all communications referring or relating to the Department's authorization of Secretary Clinton's private server and email account.
    b. Please include, if applicable:
        i. The date on which the State Department was notified about Secretary Clinton's use of a private server and email account to conduct official State Department business, and

[5] Memorandum for Sen. Richard Burr et al. from I. Charles McCullough, III, Update Classified Material on Personal Electronic Storage Devices (Aug 11, 2015).

ii. The date on which the State Department authorized Secretary Clinton's use of a private server and email account to conduct official State Department business.

c. Please identify the Department official who authorized Secretary Clinton's use of a private server and email account to conduct official State Department business.

3. Please produce all documents and communications referring or relating to legal analysis, opinions, or advice about any State Department employee's use of a private server or email account to conduct official State Department business for the time period January 1, 2009, to the present.

4. Please describe the State Department's policies and procedures for conferring with intelligence agencies prior to publicly releasing Secretary Clinton's emails pursuant to FOIA requests to ensure that sensitive material potentially contained in those emails is not shared publicly.

5. Did Secretary Clinton have an official State Department email account—such as JWICS or SIPRNet—assigned to her for accessing classified emails during her time at the State Department?
   a. If so, did Secretary Clinton ever use those classified email systems?
   b. If so, please provide all of Secretary Clinton's emails in unredacted format sent and received from her official classified email systems.

6. Please produce logs maintained by the Bureau of Intelligence and Research relating to Secretary Clinton's access to classified information.

7. On July 2, 2015, the Judiciary Committee received a response in regards to a March 27, 2015 letter to the Department. In the response, the Department noted that "staff from the Executive Secretariat briefed the former Secretary's staff (including Huma Abedin) about record practices on an annual basis and upon the Secretary's departure; the former Secretary's staff would then brief then-Secretary Clinton." Please list the date of each briefing and all individuals present including the date Secretary Clinton was briefed. In addition, please provide all records and communications relating to the briefing including all documents used at the briefing.

8. In the Department's July 2, 2015 response, it noted that, "[t]o assist employees in carrying out [responsibilities to preserve written and typed material], the Department makes available information regarding record-keeping responsibilities to all employees, including preservation of email communications and other documents throughout their tenure, including when they depart." Please provide all records relating to the information provided to employees during Secretary Clinton's tenure regarding employees' record keeping obligations while employed and at departure.

9. Please produce all records relating to communications sent or received by State Department employees to or from David Kendall, Secretary Clinton's attorney, in unredacted form for the period January 21, 2009, to February 1, 2013.

10. Please produce all records relating to communications sent or received by former State Department officials Huma Abedin, Jake Sullivan, Cheryl Mills, or Philippe Reines in the State Department's possession in unredacted form for the period January 21, 2009, to April 12, 2009; December 30, 2012 to February 1, 2013.

11. Please produce all records relating to communications sent or received by Huma Abedin in the State Department's possession in unredacted form for the period August 1, 2011 to October 1, 2011; December 1, 2012 to July 1, 2012.

Please provide this information and material as soon as possible, but no later than 5:00 p.m. on October 5, 2015. To the extent possible, please provide unclassified responses to these questions. For the transmission of responsive classified information, please send such information under separate cover, via the Office of Senate Security.

If you have any questions about this request, please contact Scott Wittmann of the Homeland Security and Governmental Affairs Committee staff at (202) 224-4751 or Josh Flynn-Brown of the Judiciary Committee staff at (202) 224-5225. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs

Charles E. Grassley
Chairman
Committee on the Judiciary

cc: The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

September 22, 2015

The Honorable Patrick F. Kennedy
Under Secretary
U.S. Department of State
Harry S. Truman Building
2201 C Street, NW
Washington, DC 20520

Dear Under Secretary Kennedy:

The Committee on Homeland Security and Governmental Affairs is examining former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department.

On October 28, 2014, the State Department issued a formal request to Secretary Clinton and three other former secretaries asking that they provide records of communications during their tenures leading the State Department.[1] Secretary Clinton's attorney, David Kendall, informed the Committee that on December 5, 2014, he provided 30,490 emails from the Secretary's private email account in response to the State Department's request.[2] However, based on information obtained by the Committee, it appears that Secretary Clinton's representatives were already in the process of gathering and reviewing Secretary Clinton's emails as early as February 2014—months before the State Department made its official request for the records. Accordingly, I write to better understand the timing of the State Department's official request and its reasoning for issuing that request in October 2014.

It appears that as early as February 2014—approximately eight months prior to the State Department's formal document request—Secretary Clinton's staff asked Platte River Networks (PRN) to begin importing Secretary Clinton's archived emails "into [a] separate archive email box."[3] Also in February 2014, PRN employees migrated Secretary Clinton's archived emails

---

[1] Letter from Patrick F. Kennedy, Under Secretary, U.S. Department of State, to Cheryl Mills (stamped Nov. 12, 2015) http://www.archives.gov/press/press-releases/2015/pdf/attachment4-clinton-letter.pdf; *see also* Letter from David E. Kendall, Williams & Connolly, LLP, to Senator Ron Johnson, S. Comm. On Homeland Sec. & Gov't Affairs (Aug. 12, 2015); Michelle Ye Hee Lee, *The misleading Democratic spin on Hillary Clinton's e-mails*, THE WASHINGTON POST (March 10, 2015) http://www.washingtonpost.com/blogs/fact-checker/wp/2015/03/10/the-misleading-democratic-spin-on-hillary-clintons-emails/.

[2] Letter from David E. Kendall, Williams & Connolly, LLP, to Senator Ron Johnson, S. Comm. On Homeland Sec. & Gov't Affairs (Aug. 12, 2015).

[3] Invoice from Platte River Networks to Marcum LLP, Rorrie Gregorio, on behalf of Clinton Executive Services Corp. (Feb. 15, 2014). Platte River Networks was hired by the Clinton Family to set up a new email server in June 2013.

into the new email system.[4] In July 2014, approximately three months prior to the State Department's formal document request, Secretary Clinton's staff asked PRN to make DVD copies of archived data related to Secretary Clinton's email account to be directly sent to Secretary Clinton's senior aide, Cheryl Mills, via overnight mail.[5] In September 2014, apparently at the direction of Cheryl Mills, PRN encrypted Secretary Clinton's email archive.[6]

Based on this information, it appears that Secretary Clinton's staff was in the process of reviewing her emails months before the State Department's October 28, 2014, formal request for her records. However, based on Secretary Clinton's statements regarding her response to the State Department's October 2014 request, it would appear as though Secretary Clinton began reviewing emails only after the State Department asked for her records. On March 10, 2015 Secretary Clinton said:

> "[A]fter I left office, the State Department asked former secretaries of state for our assistance in providing copies of work-related emails from our personal accounts. I responded right away and provided all my emails that could possibly be work-related, which totaled roughly 55,000 printed pages, even though I knew that the State Department already had the vast majority of them. We went through a thorough process to identify all of my work-related emails and deliver them to the State Department."[7]

According to former Secretary Clinton's statements, it took her staff a little over one month to review over 60,000 thousand emails, determine if each email was official or personal, produce approximately 55,000 hard-copy pages to the State Department, and then permanently delete the remaining emails.[8] However, from the information obtained by the Committee, it appears that Secretary Clinton's archiving and review of her emails were in fact aspects of a multi-month-long process that began as early as eight months prior to the State Department's formal request. Given this apparent discrepancy and the questions it raises about the rationale for and timing of the Department's request for official records, I ask the State Department to clarify the process that led to its formal records request on October 28, 2014, for Secretary Clinton's records.

In order to assist the Committee's oversight of this important matter, please provide the following information and materials:

1. Prior to the October 28, 2014 request, did the State Department communicate with Secretary Clinton or her representatives regarding the preservation and production of

---

[4] Invoice from Platte River Networks to Marcum LLP, Rorrie Gregorio, on behalf of Clinton Executive Services Corp. (Feb. 28, 2014).
[5] Email from Paul Combetta to Brenda Gies and Jill Milsom (July 23, 2014).
[6] Invoice from Platte River Networks to Marcum LLP, Rorrie Gregorio, on behalf of Clinton Executive Services Corp. (September 30, 2014) (the encrypted file was a PST Outlook file that stores copies of messages, calendar events, and other items (*see* Microsoft Outlook, *Introduction to Outlook Data Files*, https://support.office.com/en-za/article/Introduction-to-Outlook-Data-Files-pst-and-ost-6d4197ec-1304-4b81-a17d-66d4eef30b78)).
[7] Zeke J. Miller, *Transcript: Everything Hillary Clinton Said on the Email Controversy*, TIME (March 10, 2015) http://time.com/3739541/transcript-hillary-clinton-email-press-conference/.
[8] *Id.* (quoting Secretary Clinton's press conference: "At the end, I chose not to keep my private personal emails").

email records contained on Secretary Clinton's private email account and server? Please produce these communications.

2. Was the State Department aware of Secretary Clinton's review of the email records contained on her private email account and server prior to October 28, 2014? Please explain.

3. Please produce all documents and communications for the period January 1, 2014, to the present referring or relating to the State Department's request to four former Secretaries of State for federal records, including but not limited to all documents and communications referring or relating to the Department's decision-making process.

4. According to recent reports, there potentially exists a five month gap in Secretary Clinton's emails provided to the State Department.[9] When did the State Department become aware of this gap in emails? What is the State Department doing to locate the missing emails? Please explain.

I request you provide this information and material as soon as possible, but no later than 5:00 p.m. on October 6, 2015.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of the Government."[10] Additionally, S. Res. 73 (114th Congress) authorizes the Committee to examine "the efficiency and economy of operations of all branches of the Government including the possible existence of fraud, misfeasance, malfeasance, collusion, mismanagement, incompetence, corruption or unethical practices. . . ."[11] For purposes of this request, please refer to the definitions and instructions in the enclosure.

---

[9] Email from Eric Stein to Margaret Grafeld (Apr. 21, 2015) (Gaps in Secretary Clinton's emails include: messages received between January 21, 2009 to March 17, 2009, messages sent between January 21, 2009 and April 12, 2009, and messages sent between December 30, 2012 and February 1, 2013) found at http://www.judicialwatch.org/wp-content/uploads/2015/09/pp-20-21-Stein-gap-09-13-15-Hillary-email-gap-JW-v-DOS-687.pdf.
[10] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[11] S. Res. 73 § 12, 114th Cong. (2015).

If you have any questions about this request, please contact Michael Lueptow or Scott Wittmann of the Committee staff at (202) 224-4751. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

Enclosure

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

October 5, 2015

Mr. Austin McChord
Chief Executive Officer
Datto, Inc.
101 Merritt 7, 7th Floor
Norwalk, CT 06851

Dear Mr. McChord:

The Committee on Homeland Security and Governmental Affairs is examining former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. The Committee has learned that a product offered by Datto, Inc.—the Datto SIRIS S2000[1]—was purchased in 2013 for Secretary Clinton to provide on-site, immediate recovery of backup data in the event that the primary server failed.[2] The Committee is interested in the security and preservation of Secretary Clinton's official records, including whether this backup device was used to back up, recover, or store those records in any manner. I request your assistance with this important inquiry.

Datto, Inc. is "an innovative provider of comprehensive backup, recovery and business continuity solutions used by thousands of managed service providers worldwide," offering cloud, hardware, and software devices.[3] A Datto SIRIS device, like the one acquired for Secretary Clinton, "takes data directly from the server and converts it into virtual machines that can be booted instantly from a remote web interface."[4] Essentially, if the primary server fails, the Datto device acts as a virtual server to allow continued workflow while the primary server is fixed.[5] When acquiring a Datto SIRIS device, Datto offers its clients two options for storing the virtualized backups. The first option is to store the backups on-site on the Datto SIRIS S2000 product itself, creating a private cloud for the data that keeps the data within the customer's control only.[6] The second option is the data can be stored "remotely in Datto's secure cloud."[7]

---

[1] According to Datto's website, its SIRIS product supports "business continuity" with server backups, virtualization, and cloud-based accessibility. *See* Datto Siris 2, found at http://www.datto.com/siris.
[2] Platte River Networks Invoice #7942 (May 31, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).
[3] Datto, Inc., About Datto, http://www.datto.com/about.
[4] Datto SIRIS Brochure found at http://www.ableteк.com/productcatalog/datto/siris/pdf/DattoSIRISProductBrochure_r2.pdf.
[5] Instant Virtualization, Datto (last accessed on Sept. 23, 2015) http://www.datto.com/technologies/instant-virtualization.
[6] *Id.*
[7] *Id.*

According to information received by the Committee, Platte River Networks (PRN)[8] billed the Clinton Executive Service Corp. (CESC) on May 31, 2013, to acquire a Datto SIRIS S2000 device. CESC appears to be a Clinton family company. According to documents received by the Committee, CESC oversaw contracting for the hardware and software required for Secretary Clinton's private server and email.[9]

When Secretary Clinton's private server was moved from her private residence to the New Jersey-based data center, PRN set up the Datto SIRIS device at this new location.[10] When acquiring the Datto SIRIS product, it appears that CESC representatives worked with PRN employees to determine how the Datto device would back up data on Secretary Clinton's private server.[11] According to documents received by the Committee, CESC chose to only store the backup data on-site on the Datto SIRIS device, thus creating a private cloud managed by PRN.[12] CESC specifically requested that no data be stored on Datto's off-site cloud at any time.[13]

Although Secretary Clinton apparently wanted "Datto options *without* offsite backup," there was confusion among PRN employees when they noticed that data from Secretary Clinton's private server was potentially being sent to Datto's off-site backup location.[14] In

---

[8] Platte River Networks was hired by Secretary Clinton in 2013 to maintain the data stored on her private server.
[9] Email from Infograte to Platte River Networks (Apr. 17, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).
[10] Platte River Networks Invoice #33427 (June 15, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).
[11] *See* Email from Platte River Networks to Datto, Inc. (June 6, 2013) (on file with the Committee on Homeland Security and Governmental Affairs); Email from Platte River Networks to Platte River Networks (Jan. 26, 2015); Email from Platte River Networks to Platte River Networks (Jan. 26, 2015).
[12] Email from Platte River Networks to Datto, Inc. (June 6, 2013) (on file with the Committee on Homeland Security and Governmental Affairs). PRN billed for work installing the device in June 2013. For use of the private cloud capability, Datto charges a monthly fee. Each month beginning in July 2013, PRN billed CESC for "Datto Month of Private Cloud Service." This monthly service fee apparently allowed Secretary Clinton to continually have a backup on a private, virtual cloud on the SIRIS S2000 device. *See* Platte River Networks Invoice #33427 (June 15, 2013); Platte River Networks Invoice #33488 (June 17, 2013); Platte River Networks Invoice #IS.1307006 (July 1, 2013); Platte River Networks Invoice #IB.1308057 (Aug. 5, 2013); Platte River Networks Invoice #IB.1309050 (Sept. 4, 2013); Platte River Networks Invoice #IB.1310031 (Oct. 3, 2013); Platte River Networks Invoice #IB.1311027 (Nov. 5, 2013); Platte River Networks Invoice #IB.1312009 (Dec. 4, 2013); Platte River Networks Invoice #IB.1401012 (Jan. 6, 2014); Platte River Networks Invoice #IB.1402022 (Feb. 3, 2014); Platte River Networks Invoice #IB.1403010 (Mar. 3, 2014); Platte River Networks Invoice #IB.1404011 (Apr. 1, 2014); Platte River Networks Invoice #IB.1405011 (May 1, 2014); Platte River Networks Invoice #IB.1406011 (June 1, 2014); Platte River Networks Invoice #IB.1407012 (July 1, 2014); Platte River Networks Invoice #IB.1408012 (Aug. 4, 2014); Platte River Networks Invoice #IB.1409013 (Sept. 3, 2014); Platte River Networks Invoice #IB.1410015 (Oct. 1, 2014); Platte River Networks Invoice #IB.1411016 (Nov. 3, 2014); Platte River Networks Invoice #IB.1412015 (Dec. 2, 2013); Platte River Networks Invoice #IB.1501015 (Jan. 6, 2015); Platte River Networks Invoice #IB.1502014 (Feb. 2, 2015); Platte River Networks Invoice #IB.1503016 (Mar. 3, 2015); Platte River Networks Invoice #IB.1504014 (Apr. 1, 2015); Platte River Networks Invoice #IB.1505016 (May 1, 2015); Platte River Networks Invoice #IB.1506014 (June 1, 2015); Platte River Networks Invoice #IB.1507017 (July 1, 2015); Platte River Networks Invoice #IB.1508019 (Aug. 1, 2015) (all invoices mentioned on file with the Committee on Homeland Security and Governmental Affairs).
[13] Email from Platte River Networks to Datto, Inc. (June 6, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).
[14] Email from Platte River Networks to Platte River Networks (Aug. 1, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).

August 2015, employees at PRN discovered that Secretary Clinton's private server was syncing with "an offsite sync server . . . belonging to Datto."[15]

PRN employees reached out to Datto to determine if the server was actually sending data from the private server to Datto's off-site cloud for backup. One PRN employee wrote to Datto and stated, "[w]hen we made the purchase [of the SIRIS S2000], it was under the understanding that we didn't want to backup to Datto's [off-site] datacenter."[16] When a Datto employee determined that "for some reason this device [the SIRIS S2000] does appear to be syncing with the Datto Cloud,"[17] another PRN employee bluntly replied, "[t]his is a problem. This data should not be stored in the Datto Cloud . . . ."[18] Whereas CESC specifically requested that no data from Secretary Clinton's private server be backed up off-site, according to this information, it appears that Datto was providing backups for the server "from the beginning" of the contract.[19] Thus, as of August 2015, Datto apparently possessed a backup of the server's contents since June 2013.

In response to this finding, PRN employees directed Datto to not delete the saved data and worked with Datto to find a way to move the saved information on Datto's servers back to Secretary Clinton's private server.[20] According to documents received by the Committee, it appears that Datto and PRN employees discussed an option to save the data on a USB drive, send the USB drive to PRN, and "then wipe [the data] from the [Datto] cloud."[21] Despite these communications, it is unclear whether or not this course of action was followed. Additionally, questions still remain as to whether Datto actually transferred the data from its off-site datacenter to the on-site server, what data was backed up, and whether Datto wiped the data after it was transferred.

It also appears that PRN employees were directed by CESC to reduce how much data would be stored in each backup. In August 2015, a PRN employee raised the prospect that the length of the backups was reduced at some point during PRN's time managing the server. In an email to a colleague with the subject line "CESC Datto," the PRN employee asked if it is possible to use Mimecast,[22] PRN's email archiving system, to find an old email from CESC directing PRN to reduce the length of Datto's backups. He wrote:

---

[15] Email from Platte River Networks to Platte River Networks (Aug. 6, 2015) (on file with the Committee on Homeland Security and Governmental Affairs).
[16] Email from Platte River Networks to Datto, Inc. (Aug. 6, 2015) (on file with the Committee on Homeland Security and Governmental Affairs).
[17] *Id.*
[18] *Id.*
[19] Email from Platte River Networks to Platte River Networks (Aug. 7, 2015) (on file with the Committee on Homeland Security and Governmental Affairs).
[20] Email from Platte River Networks to Datto, Inc. (Aug. 6, 2015) (on file with the Committee on Homeland Security and Governmental Affairs).
[21] Email from Platte River Networks to Platte River Networks (Aug. 7, 2015) (on file with the Committee on Homeland Security and Governmental Affairs).
[22] PRN used a Mimecast product that allowed PRN to archive employee emails in a cloud-based server and search that archive as needed. *See* Mimecast, Archiving, Risk & Compliance (last accessed on Sept. 23, 2015) https://www.mimecast.com/solutions/email-archiving-compliance/.

> Any chance you found an old email with their directive to cut the backup back in Oct-Feb. I know they had you cut it once in Oct-Nov, then again to 30days [sic] in Feb-ish. If we had that email, we are golden. Would Mimecast have archived it by chance? Wondering how we can sneak an email in now after the fact asking them when they told us to cut the backups and have them confirm it for our records. Starting to think this whole thing really is covering up some shaddy shit.... I just think if we have it in writing that they told us to cut the backups, and that we can go public with our statement saying we have had backups since day one, then we were told to trim to 30days [sic], it would make us look a WHOLE LOT better.[23]

The State Department formally requested all of Secretary Clinton's records related to her time as Secretary of State on October 28, 2014.[24] It is unclear why Secretary Clinton's representatives apparently directed PRN to reduce the backup time period of her emails around the same time period or in the months following the State Department's request.

In order to better understand Datto's role relating to Secretary Clinton's private server, the backup and security capabilities of the private server, and any directives provided to Datto relating to the server, I ask that you please provide the following information and materials:

1. Please produce all documents and communications between or among employees or contractors of Datto and employees of Platte River Networks, Clinton Executive Services Corp. (CESC), or any other party referring or relating to Secretary Clinton's private server or any backup device.

2. Please produce all contracts between Datto and Platte River Networks, CESC, or any other party referring or relating to Secretary Clinton's private server or any backup device.

3. Please produce all invoices, bills, and receipts prepared by Datto or its representatives or agents regarding Secretary Clinton's private server or any backup device.

4. Please produce all helpdesk, service, or support tickets received by Datto from Platte River Networks, CESC, or any other party related to the Datto device used to backup Secretary Clinton's private server.

5. Is Datto authorized to store classified information? Were any Datto employees authorized to view classified information? Please explain. Did Datto's contract

---

[23] Email from Platte River Networks to Platte River Networks (Aug. 19, 2015) (emphasis added) (on file with the Committee on Homeland Security and Governmental Affairs); *see also* Email from Platte River Networks to Platte River Networks (Aug. 18, 2015) (PRN employee believes CESC direction to reduce the length of time backups were kept "was all phone comm[unication]s") (on file with the Committee on Homeland Security and Governmental Affairs).

[24] Letter from Patrick F. Kennedy, Under Secretary, U.S. Department of State, to Cheryl Mills (stamped Nov. 12, 2014) http://www.archives.gov/press/press-releases/2015/pdf/attachment4-clinton-letter.pdf.

regarding Secretary Clinton's private server include provisions related to the storing of classified information?

6. Has Datto been contacted by the Federal Bureau of Investigation (FBI) or any other law-enforcement entity regard Secretary Clinton's private server? Has Datto turned over any information, materials, or equipment to the FBI or any other law enforcement entity? Please explain.

7. Information obtained by the Committee suggests that PRN ordered a new Datto device in 2015 "to turn encryption on for the backups and then to power down the old device."[25] Please explain the measures taken to ensure the security of data stored on the SIRIS S2000 device, the private cloud, and the Datto Cloud.
    a. Was the backup data stored on the private cloud encrypted when the device was first installed in 2013?
    b. Was the backup data stored on the Datto Cloud encrypted?

8. Please explain the process for storing data in the Datto Cloud.
    a. How long is data retained in the cloud?
    b. What happens to the data once the required retention period is reached?
    c. Is the data deleted automatically?
    d. As mentioned above, CESC requested that the retention period for backups be reduced to 30 days. What information would be lost by reducing the backup retention period to 30 days? Please explain.

9. According to documents received by the Committee, Datto was providing off-site, cloud-based, back-up services for data contained on Secretary Clinton's private server.[26]
    a. How much data was stored on Datto's cloud? Please explain.
    b. Was this data eventually moved elsewhere? If so, where and how was this data moved? If the data was moved from Datto's servers, did Datto retain a copy of that data? If Datto retained a copy, please provide this material to the Committee.
    c. Please explain what security measures are in place to protect the data stored on Datto's cloud?
    d. During the time in which Secretary Clinton's private server was backed up on Datto's cloud, did Datto's cloud come under cyberattack? If so, please provide documentation that includes information about the time and date each attack occurred and whether any data was compromised.
    e. According to documents received by the Committee, Datto was not supposed to be storing data from Secretary Clinton's private server as part of the contract.[27] Please explain how and why data was stored on Datto's cloud.

---

[25] Email from Platte River Networks to Platte River Networks (Aug. 18, 2015) (on file with the Committee on Homeland Security and Governmental Affairs).
[26] Email from Channel Sales Executive, Datto, Inc., to Platte River Networks (Aug. 6, 2015) (on file with the Committee on Homeland Security and Governmental Affairs).

f. As mentioned above, Datto employees reviewed why backups to the Datto cloud were occurring.[28] Please provide any documentation or correspondence related to what these employees found.

Please provide this information and material as soon as possible, but no later than 5:00pm on October 19, 2015. Additionally, I ask that you please provide the Committee with a staff-level briefing to discuss Datto's role in backing up the server.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of Government."[29] Additionally, S. Res. 73 (114th Congress) authorizes the Committee to examine "the efficiency and economy of operations of all branches and functions of the Government with particular reference to (i) the effectiveness of present national security methods, staffing and processes...."[30] For purposes of this request, please refer to the definitions and instructions in the enclosure. To the maximum extent possible, please provide unclassified responses to my questions; should a complete response to any question require that you send me classified information, you may send me that information under separate cover, via the Office of Senate Security.

If you have any questions about this request, or concerns about the instructions or requirements in the enclosure, please contact Scott Wittmann or Mike Lueptow of the Committee staff at (202) 224-4751. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

Enclosure

---

[27] Email from Channel Sales Executive, Datto, Inc., to Platte River Networks (Aug. 6, 2015) (on file with the Committee on Homeland Security and Governmental Affairs).
[28] *Id.*
[29] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[30] S. Res. 73 § 12, 114th Cong. (2015).

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

October 5, 2015

Mr. Victor Nappe
Chief Executive Officer
SECNAP Network Security Corp.
Technology Research Park
3651 FAU Boulevard, Suite 400
Boca Raton, FL 33431

Dear Mr. Nappe:

The Committee on Homeland Security and Governmental Affairs is examining former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. The Committee has obtained information confirming that a product offered by SECNAP Network Security Corp. (SECNAP)—CloudJacket SMB—was purchased to perform threat monitoring of the network connected to Secretary Clinton's private server in June 2013.[1] Within a period of nine months following CloudJacket's activation in October of 2013, SECNAP identified cyberattacks originating in countries such as China, the Republic of Korea, and Germany on Secretary Clinton's private server.[2] Further, the Committee has learned that from June 2013 to October 2013, it appears that the device was not active, raising concerns about whether the private server was vulnerable to intrusions.[3] The Committee is examining, among other things, the security of Secretary Clinton's server and network. I write to respectfully request your assistance with this important inquiry.

It was recently reported that Russian hackers attempted to access Secretary Clinton's email in 2011 through the use of an email-phishing scam.[4] Although the attack originating in Russia took place nearly two years prior to SECNAP's involvement in securing Secretary

---

[1] Email from Infograte to SECNAP Network Solutions (June 26, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).

[2] Email from Infograte to SECNAP Network Solutions (June 26, 2013); *see also* Email from SECNAP Network Security to Platte River Networks (Feb. 8, 2014) (cyberattack allegedly originated from Internet Protocol (IP) address located in China); Email from SECNAP Network Security to Platte River Networks (Feb. 17, 2014) (cyberattack allegedly originated from IP address located in China); Email from SECNAP Network Security to Platte River Networks (March 4, 2014) (cyberattack allegedly originated from IP address located in "Korea, Republic of"); and Email from SECNAP Network Security to Platte River Networks (June 18, 2014) (cyberattack allegedly originated from IP address located in Germany) (all of the above emails are on file with the Committee on Homeland Security and Governmental Affairs).

[3] Email from Infograte to SECNAP Network Solutions (June 26, 2013); Email from SECNAP Network Security to Platte River Networks (Oct. 5, 2013) (confirming proper installation of CloudJacket for Secretary Clinton's private server) (both emails are on file with the Committee on Homeland Security and Governmental Affairs).

[4] Bradley Klapper, Jack Gillum, and Stephen Braun, *Russia-Linked Hackers Tried to Access Clinton Server, Emails Show*, ASSOCIATED PRESS (Sept. 30, 2015), *available at* http://abcnews.go.com/Politics/wireStory/6000-pages-clinton-emails-published-wednesday-34149824.

Clinton's private server, information received by the Committee suggests that cyberattacks originating in locations such as China, the Republic of Korea, and Germany occurred against the private server while SECNAP was monitoring threats to the network.[5] In one instance, the CloudJacket device discovered and automatically blocked malicious activity on the server.[6] According to one incident report, a SECNAP employee wrote that malicious activity based in "China was found running an attack against" Secretary Clinton's server.[7] While this specific attack was apparently detected and prevented, questions remain about whether the private server was vulnerable to cyberattacks prior to SECNAP's involvement, during the multi-month period between the purchase and activation of the CloudJacket device, and while the CloudJacket device was actively monitoring the server for malicious activity.

SECNAP delivers "unrivaled protection of network and information assets" using "next-generation information technology solutions that enable business to be conducted securely and privately on the Internet."[8] The CloudJacket device, like the one used on Secretary Clinton's network, is an intrusion prevention system that uses an "extensive and robust database of rules and signatures, and an expert experienced team of certified security engineers" to block network access to "even the most determined hackers."[9]

SECNAP provides two options for monitoring and supporting the CloudJacket device.[10] The first option is to pay a monthly fee for SECNAP Managed Service in which SECNAP expert Security Engineers will monitor the network around the clock. The second option is a "Do It Yourself Strategy" where the customer's own in-house staff monitors the network.[11] According to a document obtained by the Committee and titled, *CloudJacket Services Agreement*, it appears that Secretary Clinton's staff selected the first option, authorizing SECNAP to provide "real-time security incident response and forensics."[12]

---

[5] *See* Email from SECNAP Network Security to Platte River Networks (Feb. 8, 2014) (cyberattack allegedly originated from Internet Protocol (IP) address located in China); Email from SECNAP Network Security to Platte River Networks (Feb. 17, 2014) (cyberattack allegedly originated from IP address located in China); Email from SECNAP Network Security to Platte River Networks (March 4, 2014) (cyberattack allegedly originated from IP address located in "Korea, Republic of"); and Email from SECNAP Network Security to Platte River Networks (June 18, 2014) (cyberattack allegedly originated from IP address located in Germany) (all of the above emails are on file with the Committee on Homeland Security and Governmental Affairs).

[6] Email from SECNAP Network Security to Platte River Networks (Feb. 8, 2014) (on file with the Committee on Homeland Security and Governmental Affairs).

[7] *Id.*

[8] SECNAP Network Security Corp., Overview, http://www. secnap.com/overview/.

[9] SECNAP Network Security Corp., Patented Technology, https://www.secnap.com/products-services/cloudjacket/patented-technology/.

[10] SECNAP Network Security Corp., Managed Benefits, https://www.secnap.com/products-services/cloudjacket/managed-benefits/.

[11] *Id.*

[12] Contract between Clinton Executive Service Corp. (CESC) and SECNAP, CloudJacket Services Agreement (June 26, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).

According to additional information received by the Committee, SECNAP entered into a contract with the Clinton Executive Services Corp. (CESC) on June 26, 2013.[13] According to documents, CESC oversaw contracting for the hardware, software, and security required for Secretary Clinton's private server and email.[14] However, the CloudJacket device that was intended to prevent malicious intrusions onto the network was not activated until October 5, 2013—three months after the device was purchased.[15] This gap raises questions about the vulnerability of Secretary Clinton's private server during the multi-month period that the CloudJacket device and management service was unable to monitor the network. During this period in which the CloudJacket device was inactive, a consultant for CESC recognized the potential security vulnerabilities and strongly urged CESC's leadership to approve a time for activation of the CloudJacket device. The consultant wrote:

> We really really [*sic*] need to do this and get you on board. We are left in a bad state. 1- We want to add in this extra security. We are paying for it and no[t] using the security. 2- we need to get you all fully on board[] so they can service you properly in case you have an issue.[16]

This apparent lack of security is concerning, particularly given the cyberattacks identified by SECNAP as soon as twelve days after the CloudJacket device was activated.[17]

In order to better understand SECNAP's role relating to Secretary Clinton's private server, the security capabilities of the private server, and any directives provided to SECNAP relating to security of the server, I ask that you please provide the following information and materials:

1. Please produce all documents and communications between or among employees or contractors of SECNAP and employees of Platte River Networks, Clinton Executive Services Corp. (CESC), the U.S. State Department, the U.S. Department of Justice, or any other entity referring or relating to Secretary Clinton's private server or network for the period January 1, 2009 to the present.

---

[13] Email from Infograte to SECNAP Network Solutions (June 26, 2013) (on file with the Committee on Homeland Security and Governmental Affairs). The contract between SECNAP and Clinton Executive Service Corp. (CESC) indicates a prepaid, 24-month fee and includes "real-time security incident response and forensics." *Id.* The contract appears to have been renewed in August 2015. *See* Email from CESC to Infograte (Aug. 19, 2015) (on file with the Committee on Homeland Security and Governmental Affairs).

[14] Email from Infograte to Platte River Networks (Apr. 16, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).

[15] Email from Platte River Networks to Infograte (Sept. 27, 2013) (on file with the Committee on Homeland Security and Governmental Affairs); *see also* Email from SECNAP Network Security to Platte River Networks (Oct. 5, 2013) (confirming proper installation of CloudJacket for Secretary Clinton's private server).

[16] Email from CESC to Infograte (Aug. 19, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).

[17] Email from SECNAP Network Security to Platte River Networks (Oct. 17, 2013) (unauthorized traffic was found scanning the network and was subsequently blocked) (on file with the Committee on Homeland Security and Governmental Affairs).

2. Please produce all contracts between SECNAP and Platte River Networks, CESC, the U.S. State Department, the U.S. Department of Justice, or any other entity referring or relating to Secretary Clinton's private server or network.

3. Please produce all invoices, bills, and receipts prepared by SECNAP or its representatives or agents regarding Secretary Clinton's private server and network.

4. Please produce all helpdesk, service, or support tickets generated by SECNAP related to Platte River Networks, CESC, or any other entity connected to the SECNAP services provided to secure Secretary Clinton's private server and network.

5. Please explain how CloudJacket secures a private server and network. If a private server is targeted by a cyberattack, how does CloudJacket identify the threat and notify SECNAP employees of a potential breach?

6. According to documents received by the Committee, SECNAP detected cyberattacks originating in China, Germany, and the Republic of Korea on Secretary Clinton's server or network.[18] Were there any other attacks from inside or outside of the U.S. directed at Secretary Clinton's server or network? If so, please identify the country where the attack originated from and whether the network or data was compromised.

7. Is SECNAP aware of any cyberattacks or breaches of Secretary Clinton's private server or network prior to its engagement to provide security services? Please explain.

8. After SECNAP's services were activated for Secretary Clinton's private server, did SECNAP identify any malicious material that was already installed on the private server? If so, please explain what steps SECNAP took to report and mitigate the issue.

9. According to documents received by the Committee, SECNAP was providing "24x7x365 monitoring and escalation of network intrusion alarms and events" for Secretary Clinton's private server and network.[19]

    a. During the time in which Secretary Clinton's private server was protected by CloudJacket, how many intrusion alarms and events were reported? Was the network or data ever compromised? Please explain.
    b. Does SECNAP's CloudJacket service maintain a log of intrusion alarms and events? If so, please provide the log to the Committee.

---

[18] Email from SECNAP Network Security to Platte River Networks (Feb. 8, 2014) (on file with the Committee on Homeland Security and Governmental Affairs); *see also* Email from SECNAP Network Security to Platte River Networks (Feb. 17, 2014) (on file with the Committee on Homeland Security and Governmental Affairs).
[19] Email from Infograte to SECNAP Network Security (June 26, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).

c. Please explain the process used by SECNAP to notify the managers of Secretary Clinton's private server and network about a network intrusion.
d. According to documents received by the Committee, there was a delay in activating the CloudJacket device.[20] After activation, how many days passed before CloudJacket identified the first network threat?

10. Please identify the employees at SECNAP who were responsible for providing services for Secretary Clinton's private server.

    a. According to documents received by the Committee, SECNAP employees are required to undergo background checks.[21] What level of investigation was undertaken during the background check process?
    b. Were any SECNAP employees cleared to access classified information? If so, what clearance levels did these employees possess?

11. According to publicly available information, SECNAP provides an email encryption service.[22] Did CESC purchase SECNAP's email encryption service? If not, did CESC indicate that encryption services were already in use?

Please provide this information and material as soon as possible, but no later than 5:00pm on October 19, 2015. Additionally, I ask that you please provide the Committee with a staff-level briefing to discuss SECNAP Network Solution's role in backing up the server.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of Government."[23] Additionally, S. Res. 73 (114th Congress) authorizes the Committee to examine "the efficiency and economy of operations of all branches and functions of the Government with particular reference to (i) the effectiveness of present national security methods, staffing and processes...."[24] For purposes of this request, please refer to the definitions and instructions in the enclosure.

---

[20] Email from Platte River Networks, to Infograte (Sept. 27, 2013) (on file with the Committee on Homeland Security and Governmental Affairs); *see also* Email from SECNAP Network Security, to Platte River Networks (Oct. 5, 2013) (confirming proper installation of CloudJacket for Secretary Clinton's private server).
[21] Email from Infograte to CESC (June 17, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).
[22] SECNAP Network Security Corp., Email Encryption, https://www.secnap.com/products-services/spam-email-secuirty/email-encryption/.
[23] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[24] S. Res. 73 § 12, 114th Cong. (2015).

If you have any questions about this request, or concerns about the instructions or requirements in the enclosure, please contact Scott Wittmann or Mike Lueptow of the Committee staff at (202) 224-4751. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

Enclosure

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

October 5, 2015

The Honorable John Kerry
Secretary of State
U.S. Department of State
2201 C Street, NW
Washington, DC 20520

Dear Secretary Kerry:

The Committee on Homeland Security and Governmental Affairs is continuing to examine former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. On September 24, 2015, *The Wall Street Journal* noted that in response to a lawsuit from Citizens United, the State Department had turned over a "complete inventory and broad description of every document it has that pertains to" a Freedom of Information Act (FOIA) request, otherwise known as a *Vaughn* index.[1] To assist the Committee in better understanding the security and preservation of Secretary Clinton's records, I request that the State Department produce unredacted copies of all documents cited on the *Vaughn* index and withheld from production under FOIA.

As you know, FOIA and its exceptions do not apply to requests from Congress. According to Section 522(d) of the Freedom of Information Act, a federal agency cannot use FOIA as "authority to withhold information from Congress."[2] In addition, in *Murphy v. Department of the Army*, the D.C. Circuit reasoned that "Congress, whether as a body, through committees, or otherwise, must have the widest possible access to executive branch information. . . ."[3] Since the Department has searched for, gathered, and compiled these documents already, I ask that you produce the *Vaughn* index and all documents cited on the Vaughn index in unredacted form as soon as possible, but no later than 5:00pm on October 19, 2015.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and

---

[1] Kimberley A. Strassel, *Hillary Clinton vs. FOIA*, THE WALL STREET JOURNAL, (Sept. 24, 2015), http://www.wsj.com/articles/hillary-clinton-vs-foia-1443136818. Citizens United, a non-profit organization, filed a complaint in federal district court to compel the U.S. Department of State to comply with Citizen United's FOIA requests. *See Citizens United v. U.S. Dep't of State*, No. 15-cv-374-EGS (D.D.C. Cir. filed March 16, 2015). The term *Vaughn* index comes from a 1973 decision by the U.S. Court of Appeals for the District of Columbia. *See Vaughn v. Rosen*, 484 F.2d 820 (D.C. Cir. 1973), cert. denied, 415 U.S. 977 (1974).

[2] 5 U.S.C. § 552(d) (2006).

[3] *Murphy v. Dep't of the Army*, 613 F.2d 1151, 1155-56, 1158 (D.C. Cir. 1979); *see also McGrain v. Daugherty*, 273 U.S. 135, 174 (1927) (establishing congressional investigations are within Congress' legislative function and powers).

effectiveness of all agencies and departments of Government."[4] Additionally, S. Res. 73 (114th Congress) authorizes the Committee to examine "the efficiency and economy of operations of all branches and functions of the Government with particular reference to (i) the effectiveness of present national security methods, staffing and processes…."[5] For purposes of this request, please refer to the definitions and instructions in the enclosure. To the maximum extent possible, please provide unclassified responses to this request; should a complete response to any question require that you send me classified information, you may send me that information under separate cover, via the Office of Senate Security.

If you have any questions about this request, or concerns about the instructions or requirements in the enclosure, please contact Scott Wittmann or Mike Lueptow of the Committee staff at (202) 224-4751. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

Enclosure

[4] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[5] S. Res. 73 § 12, 114th Cong. (2015).

United States Senate

WASHINGTON, DC 20510

October 8, 2015

VIA ELECTRONIC TRANSMISSION

Mr. Bryan M. Pagliano
c/o Mark MacDougall, Esq.
Constance O'Connor, Esq.
Connor Mullin, Esq.
Sean D'Arcy, Esq.
Akin Gump Strauss Hauer & Feld LLP
1333 New Hampshire Ave NW
Washington, DC 20036

Dear Mr. Pagliano:

The Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary are continuing to examine former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. You possess information about this matter that is unavailable elsewhere and that is relevant to the Committees' oversight duties. Because you have declined our efforts to obtain your testimony, we hope you will assist the Committees by producing relevant documents and communications from your @pagliano.com email address in your possession.

The Committees have made several attempts to obtain your testimony about matters relating to Secretary Clinton's use of a private email account and server. On September 4, 2015, after your attorneys indicated that you would assert your right under the Fifth Amendment to decline to answer any questions before the Committees, we wrote you seeking a meeting with your attorneys to explore options—such as a proffer session to inform a possible grant of immunity—to obtain the unique information you possess while respecting your constitutional rights.[1] On September 9, 2015, your attorneys responded, "declin[ing] to participate in the explanatory discussions or proffer session with the Committees' staff . . . ."[2] On September 14, 2015, we wrote again to ask you to reconsider your decision not to engage with the Committees toward obtaining the pertinent information you possess.[3] On September 15, 2015, your attorneys again responded and once more declined "to enter into discussions with the staff of the Committees regarding Mr. Pagliano."[4]

---

[1] Letter from Ron Johnson, S. Comm. on Homeland Sec. & Governmental Affairs, & Charles E. Grassley, S. Comm. on the Judiciary, to Bryan M. Pagliano (Sept. 4, 2014).
[2] Letter from Mark J. MacDougall et al., Akin Gump Strauss Hauer & Feld LLP, to Ron Johnson, S. Comm. on Homeland Sec. & Governmental Affairs, & Charles E. Grassley, S. Comm. on the Judiciary (Sept. 9, 2015).
[3] Letter from Ron Johnson, S. Comm. on Homeland Sec. & Governmental Affairs, & Charles E. Grassley, S. Comm. on the Judiciary, to Bryan M. Pagliano (Sept. 14, 2014).
[4] Letter from Mark J. MacDougall et al., Akin Gump Strauss Hauer & Feld LLP, to Ron Johnson, S. Comm. on Homeland Sec. & Governmental Affairs, & Charles E. Grassley, S. Comm. on the Judiciary (Sept. 15, 2015).

As we have noted in our previous correspondence, we respect your constitutional rights and we will defer to any legitimate personal assertion of your Fifth Amendment privilege against self-incrimination. The Committees, however, have a legitimate need pursuant to our constitutional oversight authority for the information you possess in furtherance of the Committees' examination of Secretary Clinton's use of a private email account and server for official business. According to documents obtained by the Committee on Homeland Security and Governmental Affairs, you used an @pagliano.com email address to correspond with Secretary Clinton's chief of staff, Cheryl Mills; President Clinton's chief of staff, Tina Flournoy; representatives of Platte River Networks; and others about Secretary Clinton's private server.[5] We therefore believe you may possess documents relevant and necessary for the Committees' oversight.

As a further attempt to obtain information that is necessary for our constitutional oversight while respecting your constitutional right against providing self-incriminating testimony, we respectfully request that you produce documents and communications sent or received from your @pagliano.com email address referring or relating to Secretary Clinton's use of a private email account or server. We ask that you produce this material as soon as possible but no later than October 22, 2015.

We believe this accommodation will allow the Committees to obtain the information they require while respecting your constitutional rights. Thank you for your cooperation with this important matter.

Sincerely,

Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs

Charles E. Grassley
Chairman
Chairman on the Judiciary

cc: The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

---

[5] *See, e.g.*, email from Bryan Pagliano to Cheryl Mills et al. (Apr. 22, 2013) (on file with Comm. on Homeland Sec. & Governmental Affairs).

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

November 4, 2015

Mr. David E. Kendall
Williams & Connolly LLP
725 Twelfth Street NW
Washington, DC 20005

Dear Mr. Kendall:

The Committee on Homeland Security and Governmental Affairs is examining former Secretary of State Hillary Clinton's use of a private email account and server during her time leading the State Department. In the course of the Committee's work, two individuals have declined requests to assist the investigation on the bases of non-disclosure agreements that apparently have been executed that cover information that has been requested by the Committee. If the representations of these two individuals are accurate, I write to respectfully request your assistance in arranging for the appropriate authorization for their cooperation with the Committee's requests.

In particular, the Committee has learned that an entity called Clinton Executive Services Corp. (CESC) contracted with Platte River Networks (PRN) in 2013 to support and maintain Secretary Clinton's private server. On September 18, 2015, I wrote to Rorrie Gregorio, the individual named as the point of contact for CESC on its agreement with PRN and the PRN's monthly invoices, requesting information about the role of CESC relating to Secretary Clinton's private email and server.[1] On October 1, 2015, Ms. Gregorio informed the Committee that due to "our non-disclosure agreements," she was "not in a position to furnish the requested information."[2] Ms. Gregorio did not specify the nature of the non-disclosure agreements, and she did not respond to the Committee's request for clarification on whether she had asked for her client's consent to produce the requested information.

Similarly, the Committee has learned that Secretary Clinton used the services of InfoGrate, a technology consulting company, to identify and retain PRN. The Committee contacted Tania Neild, the Founder and CEO of InfoGrate, on September 9, 2015, to request that she speak with the Committee about her role relating to the private server. Ms. Neild responded the same day that she was willing to speak with the Committee but that her attorney, Ron Safer, would be in contact with Committee staff about Ms. Neild's non-disclosure agreement. During a subsequent phone conversation on September 14, at the request of Mr. Safer, Committee staff provided Mr. Safer with your name, so that you and Mr. Safer could discuss obtaining the

[1] Letter from Ron Johnson, S. Comm. on Homeland Sec. & Governmental Affairs, to Clinton Exec. Servs. Corp. (Sept. 18, 2015).
[2] E-mail from Rorrie Gregorio, Marcum LLP, to Comm. staff (Oct. 1, 2015, 11:59 a.m. EST).

appropriate consent for Ms. Neild to speak with the Committee. On October 2, 2015, Mr. Safer informed the Committee that Ms. Neild, too, had declined to speak with the Committee. Mr. Safer could not say whether Ms. Neild had sought or obtained her client's consent to speak with the Committee.

Secretary Clinton has said that she "want[s] to be as transparent as possible" about her use of a private email account and server,[3] and you have explained that Secretary Clinton is "actively cooperating" with the ongoing investigations.[4] The Committee is conducting an investigation under authority granted by Rule XXV of the Standing Rules of the Senate and pursuant to Section 12 of S. Res. 73, 114th Congress. The Committee is presently unable to obtain information relevant to the investigation due to the alleged existence of non-disclosure agreements. Although the parties to the agreements are unknown, the circumstances suggest that you may have the ability to facilitate the appropriate authorizations to enable Ms. Gregorio and Ms. Neild to cooperate with the Committee's inquiries.

Accordingly, I respectfully request that you arrange the appropriate authorization for Ms. Gregorio and Ms. Neild to cooperate with the Committee and produce relevant information. If you are unable to arrange this authorization, I ask that you explain the impediments and direct the Committee to the individual(s) with the authority to grant the appropriate authorizations.

I respectfully request that you respond by November 12, 2015. If you have any questions about this request, please contact Committee staff at 202-224-4751. Thank you for your assistance in this important matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

Clinton Executive Services Corp.
c/o Ms. Rorrie Gregorio

Ms. Tania Neild
c/o Ronald S. Safer
Schiff Hardin LLP

---

[3] Maggie Haberman, *Hillary Clinton takes 'responsibility' for email use, saying it 'wasn't the best choice,'* N.Y. TIMES, Aug. 26, 2015.
[4] Eric Tucker, *Lawyer: Gov't investigating device storage of Clinton emails*, Assoc. Press, Aug. 5, 2015.

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

November 5, 2015

Mr. Ken Xie
Chief Executive Officer
Fortinet, Inc.
899 Kifer Road
Sunnyvale, CA 94086

Dear Mr. Xie:

The Committee on Homeland Security and Governmental Affairs is examining former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. The Committee has learned that two firewalls offered by Fortinet, Inc.—the FortiGate 80C—were purchased for Secretary Clinton's private server in May 2013. Further, the Committee has learned that the Clinton server and network also had a subscription to Fortinet's 24x7 support package as of May 2013. The Committee is examining, among other things, the security of Secretary Clinton's server and network. I write to respectfully request your assistance with this important inquiry.

In order to better understand Fortinet's role relating to Secretary Clinton's private server, the security capabilities of the private server, and any directives provided to Fortinet relating to security of the server, I respectfully request that you provide the following information and materials:

1. Please produce all documents and communications between or among employees or contractors of Fortinet and employees of Platte River Networks, Clinton Executive Services Corp. (CESC), the U.S. State Department, the U.S. Department of Justice, or any other entity referring or relating to Secretary Clinton's private server or network for the period January 1, 2009 to the present.

2. Please produce all contracts between Fortinet and Platte River Networks, CESC, the U.S. State Department, or any other entity referring or relating to Secretary Clinton's private server or network.

3. Please produce all invoices, bills, and receipts prepared by Fortinet or its representatives or agents referring or relating to Secretary Clinton's private server and network.

4. Please produce all helpdesk, service, or support tickets generated by Fortinet related to Platte River Networks, CESC, or any other entity referring or relating to the Fortinet services concerning Secretary Clinton's private server and network.

5. Fortinet offers two-factor authentication using a FortiToken Mobile.[1]
    a. Did Fortinet provide FortiToken Mobile tokens to Platte River Networks? If so, how many? Does Fortinet know if the tokens were ever used?
    b. Generally, does Fortinet keep a log each time a FortiToken Mobile token is used to access a network? Please explain.

6. Fortinet offers a variety of firewall platforms and products, including the FortiGate 100D firewall and the FortiGate 80C firewalls.
    a. What security features do the FortiGate 80C firewall and the FortiGate 100D firewall provide and how do they differ?
    b. What advantages, if any, are there to upgrading from the FortiGate 80C firewall to the FortiGate 100D firewall?

7. One option for setting up a network is to use two firewalls—one firewall as the primary unit and a second firewall in case the primary firewall fails.[2] This is also known as redundancy.
    a. Is accounting for redundancy a standard industry practice? Please explain.
    b. Is the use of a single firewall sufficient to provide 24x7x365 protection to a server and network? Please explain.
    c. To Fortinet's knowledge, are there any complications when a Fortinet firewall device and a firewall device from another company are linked to the same network? If so, please explain.
    d. Is Fortinet aware of any additional security devices or services in place on Secretary Clinton's private network or connected to her server prior to May 2013?

8. In order to block unauthorized access to a network, firewalls, including the FortiGate 80C, generally filter content based on certain rules.[3]
    a. What are the main rules that most Fortinet customers use to filter content? Please explain.
    b. Generally speaking, what does creating an "open to the world rule" do?
    c. Are there rules for filtering content that leave a system more vulnerable to attack? If so, please explain.
    d. To Fortinet's knowledge, what rules were used to filter content on Secretary Clinton's private server and network? Please explain.

---

[1] Fortinet, Inc., Two-Factor Authentication & PKI Solutions – FortiToken (last accessed on Oct. 27, 2015) http://www.fortinet.com/products/fortitoken/index.html?webSyncID=d872ecc6-97cd-ab75-65aa-b4970be7d158&sessionGUID=3159e0b8-aade-8a77-8135-c5652493c17a.

[2] Fortinet, Inc., The Fortinet Cookbook: High Availability to Two Fortigates (Nov. 3, 2014) http://cookbook.fortinet.com/high-availability-two-fortigates/

[3] Symantec, *What does a firewall do?*, PCTOOLS, (last accessed on Oct. 27, 2015) http://www.pctools.com/security-news/what-does-a-firewall-do/.

9. Fortinet provides a number of services that work in conjunction with its firewall products.[4]
    a. During the time in which Secretary Clinton's private server was protected by FortiGate 80C firewalls, how many viruses or cyberattacks were detected and reported?
    b. Does Fortinet's FortiGate 80C firewall maintain a log of cyberattacks made against the server? If so, please provide the log to the Committee.
    c. Please explain the process used by Fortinet to notify the managers of Secretary Clinton's private server and network about any compromises to the network.
    d. Was Secretary Clinton's private network, server, or data ever compromised? Please explain. Did the FortiGate 80C firewall ever fail? If the FortiGate 80C firewall failed, please provide the date(s) when this occurred.
    e. Please describe this type of cyberattack: Attack ID 39294-Bash.Function.Definitions.Remote.Code.Execution.
        i. Please describe the impact of this particular type of attack registered multiple times on certain days on the FortiGate 80C firewall.
        ii. To Fortinet's knowledge, what or who is typically the source of this type of attack? Are these attacks typically from the same source?
    f. Please describe this type of cyberattack: Attack ID 31752-PHP.CGI.Argument.Injection.
    g. Please describe this type of cyberattack: Attack ID 38315-OpenSSL.Heartbleed.Attack.
    h. Please describe this type of cyberattack: Attack ID 18162-Adobe.XML.Entity.Injection.
    i. Please describe this type of cyberattack: Attack ID 13277-SSLv2.Openssl.Get.Shared.Ciphers.Overflow.Attempt.
    j. Please describe this type of cyberattack: Attack ID 29452-Apache.HTTPD.mod.proxy.ajp.DoS.

10. Please explain the role played by the FortiGate 80C firewall relating to a private server and network, including the 24x7 support package.
    a. If a private server is targeted by a cyberattack, malicious virus, or spam, how does the firewall identify the threat and notify the client?
    b. If a private server uses an alternative intrusion detection system in conjunction with a firewall, are there instances in which the firewall does not recognize an attack while the intrusion detection system does? Please explain.
    c. Did the FortiGate 80C firewall identify any cyberattack(s) on Secretary Clinton's server on February 8, 2014 and February 17, 2014?
        i. If so, what was the attack ID, the events count, the source of these attacks, and what actions were taken after identifying the cyberattack?
        ii. If not, please explain.

---

[4] Fortinet, Inc., FortiCare and Professional Services (last accessed Nov. 5, 2015) http://www.fortinet.com/support/forticare_support/index.html.

d. Did the FortiGate 80C firewall identify any cyberattack(s) on Secretary Clinton's server on March 4, 2014?
    i. If so, what was the attack ID, the events count, the source of these attacks, and what actions were taken after identifying the cyberattack?
    ii. If not, please explain.
e. Did the FortiGate 80C firewall identify any cyberattack(s) on Secretary Clinton's server on June 18, 2014?
    i. If so, what was the attack ID, the events count, the source of these attacks, and what actions were taken after identifying the cyberattack?
    ii. If not, please explain.

11. Is registration required in order for Fortinet's AntiVirus, web filtering, and email filtering services to be operative?
    a. Is it possible for a Fortinet 80C firewall device to be registered while at the same time to show Antivirus, web filtering, and email filtering services as expired? If so, please explain.
    b. Was there ever a gap between the renewal and the registration of either Fortinet 80C firewall connected to Secretary Clinton's private network? If so, please describe any possible security vulnerabilities during that time period.

12. Can you confirm whether the FortiGate 80C firewall installed on Secretary Clinton's private network contained the factory default certificate?

13. Please identify the employees at Fortinet who were responsible for providing services for Secretary Clinton's private server.
    a. Were background checks conducted on any of the employees working with Secretary Clinton's private server?
    b. Were any Fortinet employees cleared to access classified information? If so, what clearance levels did these employees possess?

Please provide this information and material as soon as possible, but no later than 5:00pm on November 19, 2015. Additionally, I ask that you please provide the Committee with a staff-level briefing to discuss Fortinet's role in providing security for Secretary Clinton's server and network.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of Government."[5] Additionally, S. Res. 73 (114th Congress) authorizes the Committee to examine "the efficiency and economy of operations of all branches and functions of the Government with particular reference to (i) the effectiveness of present national security methods, staffing and processes...."[6] For purposes of this request, please refer to the definitions and instructions in the enclosure.

---

[5] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[6] S. Res. 73 § 12, 114th Cong. (2015).

If you have any questions about this request, or concerns about the instructions or requirements in the enclosure, please contact Committee staff at (202) 224-4751. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

Enclosure

United States Senate
WASHINGTON, DC 20510

December 7, 2015

Mr. Justin Cooper
c/o Aaron M. Zebley, Esq.
WilmerHale
1875 Pennsylvania Avenue, NW
Washington, DC 20006

Dear Mr. Cooper:

The Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary are examining former Secretary of State Hillary Clinton's use of a private email account and server during her time leading the State Department. According to reports, you were responsible for setting up Secretary Clinton's server in 2008.[1] In January 2009, on behalf of the Clinton family, you reportedly bought the Internet domain name clintonemail.com.[2] That domain was registered under your name.[3] Based on these reports, it appears that you have unique, firsthand information relevant to the Committees' inquiry and we therefore request that you reconsider your decision to decline to cooperate in this important matter.

On September 8, 2015, Homeland Security Committee staff contacted you to seek your cooperation with the Committee's examination. Your attorney, Aaron Zebley, responded on your behalf on September 9, 2015. Over the ensuing weeks, Committee staff engaged Mr. Zebley in an extensive discussion about the Committee's request to speak with you. Mr. Zebley relayed your concerns about publicity surrounding your involvement with Secretary Clinton's email account and server. To assuage your concerns, Committee staff agreed to not disclose publicly that Mr. Zebley was engaging in discussions with the Committee or that you would appear before the Committee. The Homeland Security Committee has upheld its commitment to you over the course of two months since Mr. Zebley first conveyed your concerns about cooperating with this inquiry.

On October 6, 2015, following extensive discussions with Homeland Security Committee staff, Mr. Zebley notified the Committee that you had agreed to appear for a staff interview. The interview was scheduled for October 15, 2015.

---

[1] Carol D. Leonnig, Rosalind S. Helderman and Tom Hamburger, *FBI looking into the security of Hillary Clinton's private e-mail setup*, The Washington Post (August 4, 2015).
[2] Scott Shane & Michael S. Schmidt, *Hillary Clinton Emails Take Long Path to Controversy*, NEW YORK TIMES (Aug. 8, 2015).
[3] Chris Frates & Jose Pagliery, *Hillary Clinton's home server hard to trace*, CNN (Mar. 20, 2015).

Late on October 14, 2015, Mr. Zebley telephoned Homeland Security Committee staff to inform them that you had chosen to cancel the interview scheduled for the next day. Mr. Zebley could not articulate a precise reason for your change of heart, other than to reiterate the concerns he had relayed previously. During the conversation, Committee staff offered several additional proposals to further assuage your concerns about appearing before the Committee. Mr. Zebley agreed to discuss these proposals with you and committed to follow up with the Committee the next day. In the evening of the next day, October 15, Mr. Zebley informed Committee staff that he would telephone the following day. Mr. Zebley, however, never telephoned Committee staff and has not returned several phone messages left for him. His only communication since October 15—via email on October 19—was that he would "be in touch" if anything changed.

In addition, on October 16, 2015 and several times thereafter, the Judiciary Committee separately attempted to contact you and your attorney to discuss a possible interview regarding your involvement in setting up Secretary Clinton's email and server arrangement. After repeated phone calls and messages, your attorney has yet to respond.

The Committees continue to believe that you possess unique and relevant information pertinent to the Committees' inquiry of Secretary Clinton's use of a private email account and server while she served as Secretary of State. And that information falls squarely within the jurisdiction of the Committees. As such, in order to properly exercise our constitutional oversight functions, we again express our desire to meet with you. We would, of course, prefer that you meet with us in a voluntarily and informal manner, but we will consider other options if faced with a continuing lack of cooperation.

We are troubled by your attorney's complete refusal to engage the Committee in a discussion about how to further assuage your concerns. Our staff stands ready to continue their discussion with Mr. Zebley. Accordingly, we ask that you reconsider your decision to decline to appear for an informal interview with our respective Committee staff and that you direct Mr. Zebley to contact our staff to arrange for a meeting. Thank you for your assistance in this important matter.

Sincerely,

Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs

Charles E. Grassley
Chairman
Committee on the Judiciary

cc: The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

United States Senate

WASHINGTON, DC 20510

January 13, 2016

VIA ELECTRONIC TRANSMISSION

The Honorable John F. Kerry
Secretary of State
U.S. Department of State
2201 C Street, NW
Washington, DC 20520

Dear Secretary Kerry:

The Senate Homeland Security and Governmental Affairs Committee and the Senate Judiciary Committee are examining Secretary Clinton's use of a personal email account and server during her time leading the State Department. The Homeland Security and Governmental Affairs Committee has jurisdiction over national security procedures and federal records and the Judiciary Committee has legislative jurisdiction over the Freedom of Information Act and certain national security matters.

Over the last month, the Committees have interviewed current or former State Department employees about this matter. During the course of those interviews, we have learned of additional current or former State Department employees who may possess information relevant to the Committees' investigations. Accordingly, we request that the State Department make the following individuals available for interviews with Committee staff:

1. [redacted]
2.
3.
4.
5.
6.
7.
8.
9.
10.
11. Individual(s) serving as the Executive Secretariat during Secretary Clinton's tenure.

We ask that your staff contact our respective staff as soon as possible to begin facilitating the scheduling of these interviews. As in past practice, we request that the Department identify all relevant documents and communications for each individual listed above and produce those documents to the Committees prior to the dates of the interviews.

In addition, as requested by our staff, we ask that you produce:

1. All records relating to time and attendance for Mr. Bryan Pagliano, all approved timesheets, leave requests, and any requests for paid or unpaid excused absences or administrative leave.

2. The cybersecurity PowerPoint presentation and all associated documents referring or relating to the 2011 briefing by Diplomatic Security staff for Secretary Clinton's staff, including but not limited to agendas, attendee list, calendar invites, and meeting notes.

3. All documents referring or relating to the security violation investigation into Ms. Huma Abedin leaving classified documents in a hotel room during an official overseas trip, including but not limited to Form 117, and Form 118, and the final report of investigation.

4. All documents referring or relating to the cybersecurity private email auto-forward threat as described by Mr. Don Reid, including but not limited to email correspondence, a list of Department officials that used private email, interim reports, and a final report.

To the maximum extent possible, please provide unclassified responses to our questions; should a complete response to any question require that you send us classified information, you may send us that information under separate cover, via the Office of Senate Security. If you have questions, please contact David Brewer of the Homeland Security and Governmental Affairs Committee staff at (202) 224-4751 or Josh Flynn-Brown of the Judiciary Committee staff at (202) 224-5225.

Sincerely,

Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs

Charles E. Grassley
Chairman
Committee on the Judiciary

cc: The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

January 26, 2016

The Honorable John Kerry
Secretary of State
U.S. Department of State
2201 C Street, NW
Washington, DC 20520

Dear Secretary Kerry:

The Committee on Homeland Security and Governmental Affairs is examining former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. The Inspector General for the Intelligence Community (IC IG) identified additional classified emails sent or received by Secretary Clinton that contain highly sensitive intelligence classified at the "Special Access Program" (SAP) level.[1] The IC IG "received two sworn declarations from one [intelligence community] element" that "cover several dozen emails containing classified information."[2] The presence of this highly classified information on a non-official and unsecured platform could leave sensitive information vital to national security vulnerable to intrusion and removal.

I am highly concerned about the potential damage the mishandling of such highly sensitive material can have on our nation's security. As chairman of this Committee, it is my responsibility to assess "the efficiency and economy of operations of all branches and functions of the Government with particular reference to (i) the effectiveness of present national security methods, staffing, and processes . . . ."[3] Therefore, as chairman of this Committee and a senior member of the Senate Foreign Relations Committee, I request that the State Department make the documents containing SAP information identified by the IC IG available for my review. Given the sensitive nature of the information contained in these documents, you may make the documents available for my review via the Office of Senate Security. Please ask your staff to make arrangements to have these documents available for my review by Tuesday, February 2, 2016.

Thank you for your assistance in this very important matter.

Sincerely,

Ron Johnson
Chairman

[1] Letter to Sen. Richard Burr and Sen. Bob Corker, from I. Charles McCullough, III, Inspector General of the Intelligence Community (Jan. 14, 2016).
[2] *Id.*
[3] S. Res. 73 § 12, 114th Cong. (2015).

cc: The Honorable Thomas R. Carper
Ranking Member

United States Senate

WASHINGTON, DC 20510

February 22, 2016

VIA ELECTRONIC TRANSMISSION

The Honorable John Kerry
Secretary of State
U.S. Department of State
2201 C Street, NW
Washington, DC 20520

Dear Secretary Kerry:

The Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary are currently examining former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. To date, the State Department has publicly released information relevant to the Committees' inquiry pursuant to ongoing Freedom of Information Act (FOIA) litigation. The documents that have been publicly released through FOIA are, for the most part, heavily redacted. In response to many of these FOIA releases, we have requested unredacted versions often requiring a formal Committee letter. In order to streamline the document request and production process, we request unredacted copies of all documents released by the State Department—whether through FOIA, litigation, or any other means—referring or relating to Secretary Clinton's use of a private email account and server.

Based on conversations between Committee staff and the State Department's Bureau of Legislative Affairs, at times the Department does not believe that any of our previous letters to the Department requesting substantial information relating to this inquiry suffice to allow the Department to produce relevant FOIA documents without redactions. In addition, as part of our ongoing inquiry, the Committees have interviewed current and former State Department employees. The State Department possesses documents and communications sent or received by these employees relevant to the Committees' inquiry. However, the Committees often do not receive documents relevant to a witness interview until well after the interview has occurred—preventing the Committees from utilizing the documents during the interview.

The Department's posture has frustrated and delayed the production of complete, unredacted information to the Committees in a timely manner. Accordingly, in order to improve the efficiency of this process, we respectfully request that you provide the following information and materials:

1. All documents or communications, in unredacted form, that the State Department publicly releases in any form or manner referring or relating to:

a. Secretary Clinton's use of a private email account;
b. Secretary Clinton's use of a private server;
c. any communication technology used by Secretary Clinton, her staff, or her office; and
d. the use of email addresses hr15@att.blackberry.net, or hrl5@mycingular.blackberry.net and email addresses ending in @clintonemail.com or @hillaryclinton.com..

2. All documents or communications, in unredacted form, sent, received, or possessed by State Department employees interviewed or to be interviewed by the Committees referring or relating to:

a. Secretary Clinton's use of a private email account;
b. Secretary Clinton's use of a private server;
c. the security of the Secretary's office and personal electronic devices used for official business, including but not limited to:
    i. the State Department's information technology systems and other security systems;
    ii. use of State Department-issued devices such as laptops, BlackBerry devices, iPhones, iPads, and other communication devices; and
    iii. use of private devices such as personal laptops, BlackBerry devices, iPhones, iPads, servers, and other communication devices; and
d. preservation or searching of the records of the Secretary, her staff, or the Bureau of the Secretary for Federal Records Act, FOIA, Congressional oversight, Inspectors General, law enforcement, or other purposes.

Please provide this information and material as soon as possible, but no later than 5:00pm on March 22, 2016. For information and material that subsequently becomes available, we ask that you produce those documents on a rolling basis. Please send all classified information under a separate cover via the Office of Senate Security.

If you have any questions about this request, please contact Mike Lueptow or Scott Wittmann of the Homeland Security and Governmental Affairs Committee staff at (202) 224-4751 or Josh Flynn-Brown of the Judiciary Committee staff at (202) 224-5225. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs

Charles E. Grassley
Chairman
Committee on the Judiciary

cc: The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

United States Senate

WASHINGTON, DC 20510

March 3, 2016

VIA ELECTRONIC TRANSMISSION

The Honorable Loretta Lynch
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Attorney General Lynch:

We are writing regarding the immunity agreement between the Department of Justice and Mr. Bryan Pagliano, the IT Specialist who was responsible for managing former Secretary of State Hillary Clinton's non-government email server and related matters during her time leading the State Department.[1] In light of yesterday's *Washington Post* article reporting that the Department of Justice has granted immunity to Mr. Pagliano, we request a copy of that immunity agreement.[2]

As you know, in our September 14, 2015 request, the Committees specifically asked that you ensure that any agreement between the Department and Mr. Pagliano include a provision that requires Mr. Pagliano to cooperate fully with our Committees' investigation.[3] Subsequently, in a phone call with the Judiciary Committee on September 28, 2015, you stated that the Department had yet to make a determination on how it would approach Mr. Pagliano. Now that the decision has apparently been made, the Department should provide a copy of the agreement and answer the questions in our previous letter so that the Committees may assess how best to secure Mr. Pagliano's cooperation. The Committees believe that Mr. Pagliano possesses unique information about Secretary Clinton's private email account and server that is vital to the Committees' ongoing inquiries into this matter.

---

[1] *See* Letter from Ron Johnson, S. Comm. on Homeland Sec. & Governmental Affairs, & Charles E. Grassley, S. Comm. on the Judiciary, to The Honorable Loretta Lynch, U.S. Dept. of Justice (Sept. 14, 2015) [hereinafter "Sept. 14th letter"].

[2] *See e.g.*, Adam Goldman, *Justice Dept. grants immunity to staffer who set up Clinton email server*, THE WASHINGTON POST (March 2, 2016) https://www.washingtonpost.com/world/national-security/in-clinton-email-investigation-justice-department-grants-immunity-to-former-state-department-staffer/2016/03/02/e421e39e-e0a0-11e5-9c36-e1902f6b6571_story.html.

[3] Sept. 14th letter, *supra* note 1.

Accordingly, we request a copy of the immunity agreement between Mr. Pagliano and the Department by March 10, 2016. Thank you for your prompt cooperation with this request.

Sincerely,

Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs

Charles E. Grassley
Chairman
Committee on the Judiciary

cc: The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

United States Senate

WASHINGTON, DC 20510

March 3, 2016

VIA ELECTRONIC TRANSMISSION

Mr. Bryan M. Pagliano
c/o Mark MacDougall, Esq.
Constance O'Connor, Esq.
Connor Mullin, Esq.
Sean D'Arcy, Esq.
Akin Gump Strauss Hauer & Feld LLP
1333 New Hampshire Avenue, NW
Washington, DC 20036

Dear Mr. Pagliano:

We are writing to request that you reconsider your decision to not participate in an interview with the Committees in light of the recent news that you have been granted immunity by the Department of Justice.[1] We respect your constitutional rights and any legitimate personal assertion of your Fifth Amendment privilege against self-incrimination. However, the privilege is confined to instances in which the witness has reasonable cause to apprehend danger of prosecution based on his answers. *See Hoffman v. U.S.*, 341 U.S. 479, 486 (1951). Because the Department of Justice has granted you immunity from prosecution in this situation, there is no longer reasonable cause for you to believe that discussing these matters with the relevant oversight committees could result in your prosecution. Accordingly, we write to request that you make yourself available to provide information relevant to the Committees' ongoing examination of former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. In addition, we request that you provide a copy of the immunity agreement.

As mentioned in our prior correspondence, on August 19, 2015, staff of the Homeland Security and Governmental Affairs Committee requested an informal, voluntary interview with you to which you, through your attorney, declined and suggested you would likely avail yourself of your Fifth Amendment right against self-incrimination. Then, on August 28, 2015, staff of the Judiciary Committee reached out to you seeking an interview regarding your role in setting up and maintaining Secretary Clinton's private email and server. In response, your attorneys suggested that you would rely on your Fifth Amendment right and decline to answer any questions the Committee posed. In an attempt to find a path forward, we wrote to you and your attorneys requesting your attorneys meet with Committee staff to explore alternative options,

---

[1] *See e.g.*, Adam Goldman, *Justice Dept. grants immunity to staffer who set up Clinton email server*, THE WASHINGTON POST (March 2, 2016) https://www.washingtonpost.com/world/national-security/in-clinton-email-investigation-justice-department-grants-immunity-to-former-state-department-staffer/2016/03/02/e421e39e-e0a0-11e5-9c36-e1902f6b6571_story.html.

such as a proffer session, to obtain the unique information you possess.[2] Rather than meet with Committee staff, your attorneys declined to participate in any further discussions.[3] On September 14, 2015, we wrote to you again to reconsider your decision to not voluntarily engage with the Committees.[4] On September 15, 2015, your attorneys again declined to cooperate with Committee staff to discuss possible alternatives to obtain your testimony.[5]

As the Committees continue investigating Secretary Clinton's use of a private email account and server, and in light of your recent grant of immunity by the Department of Justice, the Fifth Amendment privilege is no longer applicable, and we are thus reintroducing our request to speak with you voluntarily regarding your involvement with Secretary Clinton's private email account and server. We are also reintroducing our October 8, 2015 request that you produce all documents and communications sent or received from your @pagliano.com email address referring or relating to Secretary Clinton's use of a private email account or server.[6] The Committees believe that you possess unique information about this matter that is otherwise unavailable and would appreciate your full cooperation with the Committees' requests, including providing a copy of the immunity agreement. As such, we request that you or your attorney contact Committee staff by March 10, 2016 to arrange the interview and production of responsive documents.

Thank you for your attention to this important matter.

Sincerely,

Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs

Charles E. Grassley
Chairman
Committee on the Judiciary

cc: The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

---

[2] Letter from Ron Johnson, S. Comm. on Homeland Sec. & Governmental Affairs, & Charles E. Grassley, S. Comm. on the Judiciary, to Mark J. MacDougall et al., Akin Gump Strauss Hauer & Feld LLP (Sept. 4, 2015).
[3] Letter from Mark J. MacDougall et al., Akin Gump Strauss Hauer & Feld LLP, to Ron Johnson, S. Comm. on Homeland Sec. & Governmental Affairs, & Charles E. Grassley, S. Comm. on the Judiciary (Sept. 9, 2015).
[4] Letter from Ron Johnson, S. Comm. on Homeland Sec. & Governmental Affairs, & Charles E. Grassley, S. Comm. on the Judiciary, to Mark J. MacDougall et al., Akin Gump Strauss Hauer & Feld LLP (Sept. 14, 2015).
[5] Letter from Mark J. MacDougall et al., Akin Gump Strauss Hauer & Feld LLP, to Ron Johnson, S. Comm. on Homeland Sec. & Governmental Affairs, & Charles E. Grassley, S. Comm. on the Judiciary (Sept. 15, 2015).
[6] *See* Letter from Ron Johnson, S. Comm. on Homeland Sec. & Governmental Affairs, & Charles E. Grassley, S. Comm. on the Judiciary, to Mark J. MacDougall et al., Akin Gump Strauss Hauer & Feld LLP (Oct. 8, 2015).

United States Senate

WASHINGTON, DC 20510

March 4, 2016

VIA ELECTRONIC TRANSMISSION

Mr. John Bentel
c/o Randall J. Turk
Partner
Baker Botts, LLP
1299 Pennsylvania Ave NW
Washington, DC 20004

Dear Mr. Bentel,

The Committee on the Judiciary and the Committee on Homeland Security and Governmental Affairs are examining former Secretary of State Hillary Clinton's use of a private email server and personal email account during her time leading the Department of State. During your tenure at the Department, you served as the Director of the Office of the Executive Secretariat – Information Resource Management (S/ES-IRM). As such, you were a responsible party for the Secretary's information management and information technology needs. In addition, according to current and former Department personnel who have been interviewed by the Committees, you may have specific knowledge relating to Secretary Clinton's private server and email arrangement, as well as knowledge of the Secretary's IT issues as they relate to her personal BlackBerry device that she used for official State Department business.

On December 4, 2015, Judiciary Committee staff contacted your attorney, Mr. Randall Turk, to seek your cooperation with the Committees' examination. In the course of several email and phone call exchanges, Judiciary Committee staff made clear to your attorney that, as Director of S/ES-IRM, you may possess unique and relevant information pertinent to the Committees' inquiry. In reply, Mr. Turk stated that you voluntarily sat for an interview with the U.S. House Select Committee on Benghazi (Benghazi Committee) and that you had "no memory or knowledge of the matters [you were] questioned about [...]" and that there was "little point" in repeating a similar interview. It is worth noting that the Committees' line of questioning would most certainly be different from the Benghazi Committee, since the respective Committees are examining different issues. These substantive differences were made clear during a phone call before the New Year between Judiciary Committee staff and Mr. Turk.

Further, the Judiciary Committee noted that since you availed yourself of an interview with the Benghazi Committee, it would be fair and reasonable to do the same with our Committees. And finally, with an understanding that you no longer live in the Washington, D.C. metro area, as an accommodation the Judiciary Committee offered to conduct an interview of you by phone. On January 20, 2016, Judiciary Committee staff emailed Mr. Turk to again apprise him of the Committee's desire to speak with you. Mr. Turk has not responded.

It appears that you were an integral figure in the operation of the Executive Secretariat and that you would have particular and unique knowledge relevant to the Committees' inquiry. Indeed, Department personnel have noted that your subordinates in the Executive Secretariat's office, who reported directly to you, had knowledge of Secretary Clinton's private email server, which leads one to conclude that you were likely made aware of the server. One aspect of the Committees' investigation is to determine what actions, if any, were taken to purposefully circumvent the Freedom of Information Act and federal records preservation requirements, issues within the jurisdiction of the respective Committees. Your role in the Executive Secretariat may shed light on how others in the Executive Secretariat approached and dealt with these issues.

As such, the Committees believe that you possess unique and relevant information pertinent to the Committees' inquiry. In order to properly exercise our constitutional oversight functions, we need to speak with you. We would, of course, prefer that you meet with us in a voluntary and informal manner, but we will consider other options if faced with a continuing lack of cooperation.

We are troubled by your refusal to engage with the Committees even after repeated overtures of accommodation. Please reconsider your decision to decline a voluntary, informal phone interview with our respective Committee staff and direct Mr. Turk to contact our staff to arrange a call. You may contact Josh Flynn-Brown of the Judiciary Committee staff at (202) 224-5225 or Mike Lueptow of the Homeland Security and Governmental Affairs Committee staff at (202) 224-4751 staff to do so. Thank you for your assistance in this important matter.

Sincerely,

Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs

Charles E. Grassley
Chairman
Committee on the Judiciary

cc: The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

United States Senate

WASHINGTON, DC 20510

April 27, 2016

VIA ELECTRONIC TRANSMISSION

Mr. Marcel Lehel Lazar
c/o Shannon Quill, Esq.
United States Public Defender
1650 King Street, Suite 500
Alexandria, VA 22314

Dear Mr. Lazar:

The United States Senate Committee on the Judiciary and Committee on Homeland Security and Governmental Affairs are currently investigating a number of issues surrounding Secretary Clinton's non-government server arrangement and personal email use for official government business and related matters, including whether the arrangement interfered with Freedom of Information Act and Federal Records Act compliance and the potential mishandling of classified information by Secretary Clinton and her senior staff. Over 2,000 emails containing classified information were transmitted through and stored on Secretary Clinton's non-government server.[1] Some of those emails include highly classified information at the TS/SCI level as well as information from Special Access Programs.[2]

Multiple media reports indicate that that you allegedly hacked into the email account of Sidney Blumenthal, one of Secretary Clinton's confidants during her time at the Department of State, and acquired emails sent between them.[3] It is also widely reported that your public release of hacked emails from Mr. Blumenthal's account in March 2013 was the first public indication that Secretary Clinton maintained a personal email address during her time at the Department and used it for official business.[4] Further, in a news interview you purportedly claimed that you "had memos Hillary Clinton got as a State Secretary, with CIA briefings [that] were being read by her [and] two other people from the US Government."[5] It is not clear to what

---

[1] *See e.g.,* Anita Kumar, *At Least 2,079 Clinton Emails Contain Classified Material*, MCCLATCHYDC (Feb. 29, 2016). Available at, http://www.mcclatchydc.com/news/politics-government/election/article63218372.html

[2] *See* Justin Fishel, *Hillary Clinton Accused Again of Handling Top Secret Info Through Private Email*, ABCNEWS (Jan. 20, 2016). Available at, http://abcnews.go.com/International/hillary-clinton-accused-handling-top-secret-info-private/story?id=36385744

[3] Catherine Herridge, Pamela K. Browne, *Source: No "Coincidence" Romanian Hacker Guccifer Extradited Amid Clinton Probe,* FOX NEWS (April 8, 2016). Available at, http://nation.foxnews.com/2016/04/10/source-no-coincidence-romanian-hacker-guccifer-extradited-amid-clinton-email-probe

[4] *Id.; See also,* Jeff Gerth and Sam Biddle, *Leaked Private Emails Reveal Ex-Clinton Aide's Secret Spy Network,* GAWKER (March 27, 2015). Available at, http://gawker.com/leaked-private-emails-reveal-ex-clinton-aides-secret-sp-1694112647

[5] *Supra* at note 3, citing Matei Rosca, *Exclusive: Jailed Hacker Guccifer Boasts, "I Used to Read [Clinton's] Memos...and Then Do the Gardening"* PANDO, Mar. 20, 2015. Available at,

extent, if any, you were able to gain access to Secretary Clinton's non-government server to acquire this information.

Your potential access to Secretary Clinton's server is of interest to the Committees. We understand that you have recently been extradited to stand trial in Alexandria, Virginia. It has been reported that while you were imprisoned in Romania, you met with the FBI, members of the Secret Service, and members of Cyber Command to discuss how you accessed and read memos marked "official use only."[6] Given the potential knowledge that you may have regarding Secretary Clinton's non-government server, an interview with the Committees' investigative staff is likely to assist in its inquiry. Please contact Josh Flynn-Brown of the Judiciary Committee staff at (202) 224-5225 or Michael Lueptow and Scott Wittmann of the Homeland Security and Governmental Affairs Committee staff at (202) 224-4751 to make the necessary scheduling arrangements.

Sincerely,

Ron Johnson
Chairman
Committee on Homeland Security and
Governmental Affairs

Charles E. Grassley
Chairman
Committee on the Judiciary

cc: The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

[6] *Supra* n. 3.

United States Senate

WASHINGTON, DC 20510

May 12, 2016

VIA ELECTRONIC TRANSMISSION

Mr. Justin Cooper
c/o Aaron M. Zebley, Esq.
WilmerHale
1875 Pennsylvania Avenue NW
Washington, DC 20006

Dear Mr. Cooper:

The Committee on the Judiciary and the Committee on Homeland Security and Governmental Affairs are examining former Secretary of State Hillary Clinton's use of a private email account and server during her time leading the State Department. According to reports, you were responsible for setting up Secretary Clinton's server in 2008.[1] In January 2009, on behalf of the Clinton family, you reportedly bought the Internet domain name clintonemail.com.[2] That domain was registered under your name.[3] Based on these reports, it appears that you have unique, firsthand information relevant to the Committees' inquiry.

Accordingly, the Committees wrote to you on December 7, 2015, requesting to speak with you regarding your purported knowledge of Secretary Clinton's non-government server arrangement. In that letter, the Committees noted the numerous times since September 2015 that we have reached out to you in an attempt to schedule an interview. Indeed, in October 2015 you agreed to sit for a staff interview with the Homeland Security and Governmental Affairs Committee. However, the day before the interview was to take place, your attorney notified the Committee that you had chosen to cancel it.

In response to the Committees' December 7, 2015, letter to you, your attorney responded that he will provide an update to the Committees if there is "additional information" related to your potential participation in a Committee interview. To date, the Committees have not received any additional information relating to your participation.

---

[1] Carol D. Leonnig, Rosalind S. Helderman and Tom Hamburger, *FBI looking into the security of Hillary Clinton's private e-mail setup*, The Washington Post (August 4, 2015).
[2] Scott Shane & Michael S. Schmidt, *Hillary Clinton Emails Take Long Path to Controversy*, NEW YORK TIMES (Aug. 8, 2015).
[3] Chris Frates & Jose Pagliery, *Hillary Clinton's home server hard to trace*, CNN (Mar. 20, 2015).

The Committees continue to believe that you possess unique and relevant information pertinent to the Committees' inquiry of Secretary Clinton's use of a private email account and server while she served as Secretary of State. This information falls squarely within the jurisdiction of the Committees. As such, in order to properly exercise our constitutional oversight functions, we again express our desire to meet with you. As noted in our December 7 letter, we would, of course, prefer that you meet with us in a voluntarily and informal manner, but we will consider other options if faced with a continuing lack of cooperation.

We ask that you reconsider your decision to decline to appear.

Sincerely,

Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs

Charles E. Grassley
Chairman
Committee on the Judiciary

cc: The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

United States Senate

WASHINGTON, DC 20510

June 14, 2016

VIA ELECTRONIC TRANSMISSION

Mr. Marcel Lehel Lazar
c/o Shannon Quill, Esq.
United States Public Defender
1650 King Street, Suite 500
Alexandria, VA 22314

Dear Mr. Lazar:

According to court records, your criminal case recently came to a close. You agreed to a plea deal and an agreement to cooperate fully with the government, including providing "all information known to [you] regarding any criminal activity as requested by the government."[1] As you are aware, we wrote to you on April 27, 2016, requesting that you meet with our staff. The United States Senate Committee on the Judiciary and Committee on Homeland Security and Governmental Affairs are currently investigating a number of issues surrounding Secretary Clinton's non-government server arrangement and personal email use for official government business, including whether the arrangement interfered with Freedom of Information Act and Federal Records Act compliance. In addition, the Committees are also investigating the potential national security implications of Secretary Clinton's decision to use a non-government server and personal email account to conduct official State Department business.

Press reports indicate that that you allegedly hacked into the email accounts of Secretary Powell and Sidney Blumenthal, one of Secretary Clinton's confidants during her time at the Department of State.[2] It is also widely reported that your public release of hacked emails from Mr. Blumenthal's account in March 2013 was the first indication that Secretary Clinton maintained a personal email address during her time at the Department and used it for official business.[3] Further, in a news interview you purportedly claimed that you "had memos Hillary Clinton got as a State Secretary, with CIA briefings [that] were being read by her [and] two other people for the US Government."[4] In two interviews last month, you claimed that you hacked

---

[1] Plea Agreement, *U.S. v. Lazar*, 1:14-cr-213 (EDVA), ECF No. 28.
[2] Catherine Herridge, Pamela K. Browne, *Source: No "Coincidence" Romanian Hacker Guccifer Extradited Amid Clinton Probe,* FOX NEWS (April 8, 2016). Available at http://www.foxnews.com/politics/2016/04/08/source-no-coincidence-romanian-hacker-guccifer-extradited-amid-clinton-probe.html
[3] *Id.; See also,* Jeff Gerth and Sam Biddle, *Leaked Private Emails Reveal Ex-Clinton Aide's Secret Spy Network,* GAWKER (March 27, 2015). Available at, http://gawker.com/leaked-private-emails-reveal-ex-clinton-aides-secret-sp-1694112647
[4] *Supra* at note 2, citing Matei Rosca, *Exclusive: Jailed Hacker Guccifer Boasts, "I Used to Read [Clinton's] Memos...and Then Do the Gardening"* PANDO, Mar. 20, 2015. Available at, https://pando.com/2015/03/20/exclusive-interview-jailed-hacker-guccifer-boasts-i-used-to-read-hillarys-memos-for-six-seven-hours-and-then-do-the-gardening/

into Secretary Clinton's non-government server, allegedly saying the server "was like an open orchid on the Internet. There were hundreds of folders."[5]

Given the ongoing investigation into Secretary Clinton's non-government server arrangement and related matters, your alleged access to Secretary Clinton's server is of interest to the Committees. In light of your recent plea deal, you are no longer in legal jeopardy, and we would like to set up a meeting between you and our investigative staff. Please contact Josh Flynn-Brown of the Judiciary Committee staff at (202) 224-5225 and Michael Lueptow of the Homeland Security and Governmental Affairs Committee at (202) 224-4751 to make the necessary scheduling arrangements. We very much appreciate your consideration.

Sincerely,

Charles E. Grassley
Chairman
Committee on the Judiciary

Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs

cc:

The Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security
and Governmental Affairs

[5] Cynthia McFadden, Tim Uehlinger & Tracy Connor, *Hacker 'Guccifer': I got inside Hillary Clinton's server*, NBC NEWS, May 5, 2016. *See also* Catherin Herridge & Pamela K. Browne, *Romanian hacker Guccifer: I breached Clinton server, 'it was easy,'* FOX NEWS, May 4, 2016.

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

July 5, 2016

The Honorable James B. Comey
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, DC 20535

Dear Director Comey:

The Committee on Homeland Security and Governmental Affairs is continuing to examine former Secretary of State Hillary Clinton's use of a private email account and server during her time at the U.S. State Department.

On July 5, 2016, you announced the findings and recommendation of the Federal Bureau of Investigation's (FBI) examination of Secretary Clinton's use of a personal email system. In your statement, you reported that a total of 110 emails in 52 email chains were classified at the time they were sent or received, including emails sent or received by Secretary Clinton that were classified at the Top Secret/Special Access Program level at the time.[1] You acknowledged that "there is evidence that [Secretary Clinton or her colleagues] were extremely careless in their handling of very sensitive, highly classified information."[2] However, the FBI did not recommend charges against Secretary Clinton.

In light of your recent statement regarding the FBI's investigation, I write to better understand the resources that the FBI employed during this investigation. Accordingly, I request that you please provide the following information and materials:

1. The total number of FBI employees assigned to the investigation of former Secretary Clinton's use of a private email account and server.

2. A list of all FBI components and resources that have worked or been consulted on the FBI's investigation.

3. An estimate of the total cost associated with the FBI's investigation of Secretary Clinton's use of a private email account and server. To your knowledge, what other federal departments or agencies incurred costs associated with the FBI's investigation?

---

[1] Fed. Bureau of Investigation, Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System (July 5, 2016).
[2] *Id.*

4. According to your statement, you determined that Secretary Clinton's "handling of very sensitive, highly classified information" was "extremely careless."[3] However, you found that the actions of Secretary Clinton did not lead to a recommendation to pursue criminal charges, including charges under the "gross negligence" standard.[4]

    a. What is the difference, in the FBI's view, between extreme carelessness and gross negligence?

    b. If the evidence that the FBI collected about Secretary Clinton's use of a private email account and server did not constitute gross negligence, what set of facts would cause the FBI to recommend criminal charges under the gross negligence standard?

Please provide this information as soon as possible, but no later than 5:00 p.m. on July 19, 2016. If you have any questions about this request, please ask your staff to contact Mike Lueptow or Scott Wittmann at (202) 224-4751. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

[3] *Id.*
[4] 18 U.S.C. § 793(f).

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

July 11, 2016

The Honorable Loretta Lynch
Attorney General
U.S. Department of Justice
Washington, DC 20530

Dear Attorney General Lynch:

The Committee on Homeland Security and Governmental Affairs continues to examine former Secretary of State Hillary Clinton's use of a private e-mail account and server during her time at the U.S. State Department. As a part of this examination, I request information about the resources that government agencies, including the Department of Justice, dedicated to cooperating with the Federal Bureau of Investigation's (FBI) examination into Secretary Clinton's use of a personal e-mail system.

On July 5, 2016, FBI Director James Comey announced the findings and recommendation of the FBI's investigation into Secretary Clinton. Director Comey described the FBI's investigation, including assistance that the FBI received from other federal agencies.

Director Comey stated that FBI investigators "read all of the approximately 30,000 e-mails provided by Secretary Clinton to the State Department in December 2014."[1] Director Comey explained that:

> Where an e-mail was assessed as possibly containing classified information, the FBI referred the e-mail to any U.S. government agency that was a likely "owner" of information in the e-mail, so that agency could make a determination as to whether the e-mail contained classified information at the time it was sent or received, or whether there was reason to classify the e-mail now, even if its content was not classified at the time it was sent . . . .[2]

Additionally, Director Comey stated that the FBI "discovered several thousand work-related e-mails that were not in the group of 30,000 that were returned by Secretary Clinton to State in 2014," in part by "reviewing the archived government e-mail accounts of people who had been government employees at the same time as Secretary Clinton, including high-ranking officials at other agencies, people with whom a Secretary of State might naturally correspond."[3]

---

[1] Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System, Washington, D.C. (July 5, 2016).
[2] *Id.*
[3] *Id.*

Finally, Director Comey stated that the FBI "interviewed many people, from those involved in setting up and maintaining the various iterations of Secretary Clinton's personal server, to staff members with whom she corresponded on e-mail, to those involved in the e-mail production to State, and finally, Secretary Clinton herself."[4]

In light of Director Comey's statements regarding the assistance that the FBI received from other agencies, I write to better understand the resources that the Department of Justice—other than the FBI—employed to cooperate with the FBI and other federal agency investigations. Accordingly, I request that you please provide the following information and materials:

1. The total number of Department of Justice employees who performed work related to federal agency investigations of Secretary Clinton's use of a private e-mail account and server.

2. A list of all Department of Justice components and resources that have worked or been consulted on federal agency investigations of Secretary Clinton's use of a private e-mail account and server.

3. An estimate of the total cost associated with the Department of Justice's cooperation with federal agency investigations of Secretary Clinton's use of a private e-mail account and server.

4. The total number of e-mails that the FBI referred to the Department of Justice for a determination of whether the e-mail contained classified information, either at the time it was transmitted or presently.

Please provide this information as soon as possible, but no later than 5:00 p.m. on July 25, 2016. If you have any questions about this request, please ask your staff to contact Mike Lueptow or Scott Wittmann at (202) 224-4751. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

[4] *Id.*

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

July 11, 2016

The Honorable I. Charles McCullough, III
Inspector General of the Intelligence Community
Office of the Director of National Intelligence
Washington, DC 20511

Dear Inspector General McCullough:

The Committee on Homeland Security and Governmental Affairs continues to examine former Secretary of State Hillary Clinton's use of a private e-mail account and server during her time at the U.S. State Department. As a part of this examination, I request information about the resources that government agencies, including the Office of the Inspector General of the Intelligence Community (IC IG), dedicated to cooperating with the Federal Bureau of Investigation's (FBI) examination into Secretary Clinton's use of a personal e-mail system.

On July 5, 2016, FBI Director James Comey announced the findings and recommendation of the FBI's investigation into Secretary Clinton. Director Comey described the FBI's investigation, including assistance that the FBI received from other federal agencies.

Director Comey stated that FBI investigators "read all of the approximately 30,000 e-mails provided by Secretary Clinton to the State Department in December 2014."[1] Director Comey explained that:

> Where an e-mail was assessed as possibly containing classified information, the FBI referred the e-mail to any U.S. government agency that was a likely "owner" of information in the e-mail, so that agency could make a determination as to whether the e-mail contained classified information at the time it was sent or received, or whether there was reason to classify the e-mail now, even if its content was not classified at the time it was sent . . . .[2]

Additionally, Director Comey stated that the FBI "discovered several thousand work-related e-mails that were not in the group of 30,000 that were returned by Secretary Clinton to State in 2014," in part by "reviewing the archived government e-mail accounts of people who had been government employees at the same time as Secretary Clinton, including high-ranking officials at other agencies, people with whom a Secretary of State might naturally correspond."[3]

---

[1] Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System (July 5, 2016), *available at* https://www.fbi.gov/news/pressrel/press-releases/statement-by-fbi-director-james-b.-comey-on-the-investigation-of-secretary-hillary-clintons-use-of-a-personal-e-mail-system.
[2] *Id.*
[3] *Id.*

Finally, Director Comey stated that the FBI "interviewed many people, from those involved in setting up and maintaining the various iterations of Secretary Clinton's personal server, to staff members with whom she corresponded on e-mail, to those involved in the e-mail production to State, and finally, Secretary Clinton herself."[4]

In light of Director Comey's statements regarding the assistance that the FBI received from other agencies, I write to better understand the resources that the IC IG employed to cooperate with the FBI and other federal agency investigations. Accordingly, I request that you please provide the following information and materials:

1. The total number of employees within the IC IG who performed work related to federal agency investigations of Secretary Clinton's use of a private e-mail account and server.

2. A list of all IC IG components and resources that have worked or been consulted on federal agency investigations of Secretary Clinton's use of a private e-mail account and server.

3. An estimate of the total cost associated with the IC IG's cooperation with federal agency investigations of Secretary Clinton's use of a private e-mail account and server.

Please provide this information as soon as possible, but no later than 5:00 p.m. on July 25, 2016. To the maximum extent possible, please provide unclassified responses to my questions; should a complete response to any question require that you send me classified information, you may send me that information under separate cover, via the Office of Senate Security. If you have any questions about this request, please ask your staff to contact Mike Lueptow or Scott Wittmann at (202) 224-4751. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

[4] *Id.*

United States Senate

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

July 11, 2016

The Honorable James R. Clapper
Director of National Intelligence
Office of the Director of National Intelligence
Washington, DC 20511

Dear Director Clapper:

The Committee on Homeland Security and Governmental Affairs continues to examine former Secretary of State Hillary Clinton's use of a private e-mail account and server during her time at the U.S. State Department. As a part of this examination, I request information about the resources that government agencies, including members of the intelligence community, dedicated to cooperating with the Federal Bureau of Investigation's (FBI) examination into Secretary Clinton's use of a personal e-mail system.

On July 5, 2016, FBI Director James Comey announced the findings and recommendation of the FBI's investigation into Secretary Clinton. Director Comey described the FBI's investigation, including assistance that the FBI received from other federal agencies.

Director Comey stated that FBI investigators "read all of the approximately 30,000 e-mails provided by Secretary Clinton to the State Department in December 2014."[1] Director Comey explained that:

> Where an e-mail was assessed as possibly containing classified information, the FBI referred the e-mail to any U.S. government agency that was a likely "owner" of information in the e-mail, so that agency could make a determination as to whether the e-mail contained classified information at the time it was sent or received, or whether there was reason to classify the e-mail now, even if its content was not classified at the time it was sent . . . .[2]

Additionally, Director Comey stated that the FBI "discovered several thousand work-related e-mails that were not in the group of 30,000 that were returned by Secretary Clinton to State in 2014," in part by "reviewing the archived government e-mail accounts of people who had been government employees at the same time as Secretary Clinton, including high-ranking officials at other agencies, people with whom a Secretary of State might naturally correspond."[3]

---

[1] Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System, Washington, D.C. (July 5, 2016).
[2] *Id.*
[3] *Id.*

Finally, Director Comey stated that the FBI "interviewed many people, from those involved in setting up and maintaining the various iterations of Secretary Clinton's personal server, to staff members with whom she corresponded on e-mail, to those involved in the e-mail production to State, and finally, Secretary Clinton herself."[4]

In light of Director Comey's statements regarding the assistance that the FBI received from other agencies, I write to better understand the resources that the intelligence community employed to cooperate with the FBI and other federal agency investigations. Accordingly, I request that you please provide the following information and materials:

1. The total number of employees within components of the intelligence community who performed work related to federal agency investigations of Secretary Clinton's use of a private e-mail account and server.

2. A list of all intelligence community components and resources that have worked or been consulted on federal agency investigations of Secretary Clinton's use of a private e-mail account and server.

3. An estimate of the total cost associated with the intelligence community's cooperation with federal agency investigations of Secretary Clinton's use of a private e-mail account and server.

4. The total number of e-mails that the FBI referred to the Office of the Director of National Intelligence or components of the intelligence community for a determination of whether the e-mail contained classified information, either at the time it was transmitted or presently.

5. The total number of e-mails that the Office of the Director of National Intelligence or components of the intelligence community produced to the FBI that were discovered by reviewing the archived government e-mail accounts of current or former employees within the intelligence community.

Please provide this information as soon as possible, but no later than 5:00 p.m. on July 25, 2016. To the maximum extent possible, please provide unclassified responses to my questions; should a complete response to any question require that you send me classified information, you may send me that information under separate cover, via the Office of Senate Security.

[4] *Id.*

If you have any questions about this request, please ask your staff to contact Mike Lueptow or Scott Wittmann at (202) 224-4751. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

July 11, 2016

The Honorable John Kerry
Secretary of State
U.S. Department of State
2201 C Street, NW
Washington, DC 20520

Dear Secretary Kerry:

The Committee on Homeland Security and Governmental Affairs continues to examine former Secretary of State Hillary Clinton's use of a private e-mail account and server during her time at the U.S. State Department. As a part of this examination, I request information about the resources that government agencies, including the State Department, dedicated to cooperating with the Federal Bureau of Investigation's (FBI) examination into Secretary Clinton's use of a personal e-mail system.

On July 5, 2016, FBI Director James Comey announced the findings and recommendation of the FBI's investigation into Secretary Clinton. Director Comey described the FBI's investigation, including assistance that the FBI received from other federal agencies.

Director Comey stated that FBI investigators "read all of the approximately 30,000 e-mails provided by Secretary Clinton to the State Department in December 2014."[1] Director Comey explained that:

> Where an e-mail was assessed as possibly containing classified information, the FBI referred the e-mail to any U.S. government agency that was a likely "owner" of information in the e-mail, so that agency could make a determination as to whether the e-mail contained classified information at the time it was sent or received, or whether there was reason to classify the e-mail now, even if its content was not classified at the time it was sent . . . .[2]

Additionally, Director Comey stated that the FBI "discovered several thousand work-related e-mails that were not in the group of 30,000 that were returned by Secretary Clinton to State in 2014," in part by "reviewing the archived government e-mail accounts of people who had been government employees at the same time as Secretary Clinton, including high-ranking officials at other agencies, people with whom a Secretary of State might naturally correspond."[3]

---

[1] Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System, Washington, D.C. (July 5, 2016).
[2] *Id.*
[3] *Id.*

Finally, Director Comey stated that the FBI "interviewed many people, from those involved in setting up and maintaining the various iterations of Secretary Clinton's personal server, to staff members with whom she corresponded on e-mail, to those involved in the e-mail production to State, and finally, Secretary Clinton herself."[4]

In light of Director Comey's statements regarding the assistance that the FBI received from other agencies, I write to better understand the resources that the State Department employed to cooperate with the FBI and other federal agency investigations. Accordingly, I request that you please provide the following information and materials:

1. The total number of State Department employees who performed work related to federal agency investigations of Secretary Clinton's use of a private e-mail account and server.

2. A list of all State Department components and resources that have worked or been consulted on federal agency investigations of Secretary Clinton's use of a private e-mail account and server.

3. An estimate of the total cost associated with the State Department's cooperation with federal agency investigations of Secretary Clinton's use of a private e-mail account and server.

4. The total number of e-mails that the FBI referred to the State Department for a determination of whether the e-mail contained classified information, either at the time it was transmitted or presently.

5. The total number of e-mails that the State Department produced to the FBI that were discovered by reviewing the archived government e-mail accounts of current or former State Department employees.

Please provide this information as soon as possible, but no later than 5:00 p.m. on July 25, 2016. If you have any questions about this request, please ask your staff to contact Mike Lueptow or Scott Wittmann at (202) 224-4751. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman

[4] *Id.*

cc: The Honorable Thomas R. Carper
Ranking Member

United States Senate

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

July 11, 2016

The Honorable Steve Linick
Inspector General
U.S. Department of State
2201 C Street, NW
Washington, DC 20520

Dear Inspector General Linick:

The Committee on Homeland Security and Governmental Affairs continues to examine former Secretary of State Hillary Clinton's use of a private e-mail account and server during her time at the U.S. State Department. As a part of this examination, I request information about the resources that government agencies, including the Department of State Office of Inspector General (State OIG), dedicated to cooperating with the Federal Bureau of Investigation's (FBI) examination into Secretary Clinton's use of a personal e-mail system.

On July 5, 2016, FBI Director James Comey announced the findings and recommendation of the FBI's investigation into Secretary Clinton. Director Comey described the FBI's investigation, including assistance that the FBI received from other federal agencies.

Director Comey stated that FBI investigators "read all of the approximately 30,000 e-mails provided by Secretary Clinton to the State Department in December 2014."[1] Director Comey explained that:

> Where an e-mail was assessed as possibly containing classified information, the FBI referred the e-mail to any U.S. government agency that was a likely "owner" of information in the e-mail, so that agency could make a determination as to whether the e-mail contained classified information at the time it was sent or received, or whether there was reason to classify the e-mail now, even if its content was not classified at the time it was sent . . . .[2]

Additionally, Director Comey stated that the FBI "discovered several thousand work-related e-mails that were not in the group of 30,000 that were returned by Secretary Clinton to State in 2014," in part by "reviewing the archived government e-mail accounts of people who had been government employees at the same time as Secretary Clinton, including high-ranking officials at other agencies, people with whom a Secretary of State might naturally correspond."[3]

---

[1] Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System, Washington, D.C. (July 5, 2016).
[2] *Id.*
[3] *Id.*

Finally, Director Comey stated that the FBI "interviewed many people, from those involved in setting up and maintaining the various iterations of Secretary Clinton's personal server, to staff members with whom she corresponded on e-mail, to those involved in the e-mail production to State, and finally, Secretary Clinton herself."[4]

In light of Director Comey's statements regarding the assistance that the FBI received from other agencies, I write to better understand the resources that the State OIG employed to cooperate with the FBI and other federal agency investigations. Accordingly, I request that you please provide the following information and materials:

1. The total number of State OIG employees who performed work related to federal agency investigations of Secretary Clinton's use of a private e-mail account and server.

2. A list of all State OIG components and resources that have worked or been consulted on federal agency investigations of Secretary Clinton's use of a private e-mail account and server.

3. An estimate of the total cost associated with the State OIG's cooperation with federal agency investigations of Secretary Clinton's use of a private e-mail account and server.

Please provide this information as soon as possible, but no later than 5:00 p.m. on July 25, 2016. If you have any questions about this request, please ask your staff to contact Mike Lueptow or Scott Wittmann at (202) 224-4751. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

[4] *Id.*

Congress of the United States
Washington, DC 20515

July 12, 2016

Mr. Austin McChord
Chief Executive Officer
Datto, Inc.
101 Merritt 7, 7th Floor
Norwalk, CT 06851

Dear Mr. McChord:

The House Committee on Science, Space, and Technology and the Senate Committee on Homeland Security and Governmental Affairs are examining former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. The Committees understand that a product offered by Datto, Inc.—the Datto SIRIS S2000—was purchased in 2013 for Secretary Clinton to provide on-site, immediate recovery of backup data in the event that the primary server failed. We write to reiterate our previous requests for information regarding Datto's role relating to the security of Secretary Clinton's private server and email account.

On July 5, 2016, Federal Bureau of Investigation (FBI) Director James Comey announced the conclusion of the FBI's investigation into Secretary Clinton. While the FBI did not recommend charges against Secretary Clinton, it did identify numerous security concerns regarding Secretary Clinton's use of a private server and email account. Specifically, Director Comey said that "it is possible that hostile actors gained access to Secretary Clinton's personal email account."[1] This finding was based on the fact that "hostile actors gained access to the private commercial email accounts of people with whom Secretary Clinton was in regular contact from her personal account."[2] In addition, Director Comey raised the concern about the possibility that Secretary Clinton's server was hacked because of the fact that her personal email domain was known by a large number of people and "she also used her personal email extensively while outside the United States, including sending and receiving work-related emails in the territory of sophisticated adversaries."[3]

On October 5, 2015, Senator Ron Johnson, chairman of the Senate Homeland Security and Governmental Affairs Committee, wrote to you seeking information about the Datto device used in conjunction with Secretary Clinton's private server. In addition, on January 14, 2016, Congressman Lamar Smith, chairman of the House Committee on Science, Space, and Technology, wrote to you seeking similar information. Datto declined to provide complete responses to the Committees' inquiries, citing that it did not have its client's consent to produce documents or information. Therefore, we are writing to jointly reiterate the previous requests for

---

[1] Fed. Bureau of Investigation, Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal Email System (July 5, 2016).
[2] *Id.*
[3] *Id.*

information and materials that Datto has yet to provide. The information that Committees seek from Datto will offer better insight into the security and data backup capabilities of Secretary Clinton's private server and what potential vulnerabilities to federal records and sensitive information need to be mitigated.

The Committee on Science, Space, and Technology has jurisdiction over the National Institute of Standards and Technology (NIST) which develops cybersecurity standards and guidelines as set forth in House Rule X. The NIST publishes the *Framework for Improving Critical Infrastructure Cybersecurity* (the Framework).[4] The Framework sets industry standards and best practices to help organizations manage cybersecurity risks.[5] The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of Government."[6] Additionally, S. Res. 73 (114th Congress) authorizes the Committee to examine "the efficiency and economy of operations of all branches and functions of the Government with particular reference to (i) the effectiveness of present national security methods, staffing and processes…."[7] Because former Secretary Clinton chose to forego using State's official government system, which is governed by strict federal cybersecurity guidelines, the Committees have questions about whether the level of security of Secretary Clinton's private server, email account, and backup devices is comparable to the cybersecurity standards prescribed by the NIST Framework and reiterate our prior requests for information from Datto.

Please provide this information and material as soon as possible, but no later than 5:00 p.m. on July 26, 2016. If Datto does not provide all of the requested materials, the Committees will consider use of the compulsory process.

If you have any questions about this request, please contact Science Committee staff at 202-225-6371 or Homeland Security Committee staff at 202-224-4751. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman
Committee on Science, Space,
and Technology
U.S. House of Representatives

Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs
U.S. Senate

---

[4] Nat'l Institute of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (last visited Jan. 12, 2016).
[5] *Id.*
[6] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[7] S. Res. 73 § 12, 114th Cong. (2015).

cc: The Honorable Eddie Bernice Johnson
Ranking Minority Member
Committee on Science, Space, and Technology

The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

Congress of the United States
Washington, DC 20515

July 12, 2016

Mr. Treve Suazo
Chief Executive Officer
Platte River Networks
5700 Washington Street
Denver, CO 80216

Dear Mr. Suazo:

The House Committee on Science, Space, and Technology and the Senate Committee on Homeland Security and Governmental Affairs are examining former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. According to information obtained by the Committees, Secretary Clinton hired Platte River Networks to provide information technology services for Secretary Clinton's private server and email account.

On July 5, 2016, Federal Bureau of Investigation (FBI) Director James Comey announced the conclusion of the FBI's investigation into Secretary Clinton. While the FBI did not recommend charges against Secretary Clinton, it did identify numerous security concerns regarding Secretary Clinton's use of a private server and email account. Specifically, Director Comey said that "it is possible that hostile actors gained access to Secretary Clinton's personal email account."[1] This finding was based on the fact that "hostile actors gained access to the private commercial email accounts of people with whom Secretary Clinton was in regular contact from her personal account."[2] In addition, Director Comey raised the concern about the possibility that Secretary Clinton's server was hacked because of the fact that her personal email domain was known by a large number of people and "she also used her personal email extensively while outside the United States, including sending and receiving work-related emails in the territory of sophisticated adversaries."[3]

On August 8, 2015, Senator Ron Johnson, chairman of the Senate Homeland Security and Governmental Affairs Committee, wrote to you seeking information about services provided by Platte River Networks, including maintaining Secretary Clinton's private server. After an initial production by Platte River Networks, Chairman Johnson's staff requested the opportunity to interview Platte River Networks employees familiar with Secretary Clinton's servers' configuration. In addition, on January 14, 2016, Congressman Lamar Smith, chairman of the House Committee on Science, Space, and Technology, wrote to you seeking similar information.

---

[1] Fed. Bureau of Investigation, Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal Email System (July 5, 2016).
[2] *Id.*
[3] *Id.*

Platte River Networks declined to provide complete responses to Chairman Smith's inquiry and declined to provide relevant employees to be interviewed by Chairman Johnson's staff. Therefore, we are writing to jointly reiterate the previous requests for information and staff-level interviews from Platte River Networks. The information that the Committees seek from Platte River Networks will offer better insight into the security capabilities of Secretary Clinton's private server and what potential vulnerabilities to federal records and sensitive information need to be mitigated.

To assist with the Committees' inquiries, we request interviews with the following individuals:

1. [redacted]
2.
3.
4.
5.
6.
7.

The Committee on Science, Space, and Technology has jurisdiction over the National Institute of Standards and Technology (NIST) which develops cybersecurity standards and guidelines as set forth in House Rule X. The NIST publishes the *Framework for Improving Critical Infrastructure Cybersecurity* (the Framework).[4] The Framework sets industry standards and best practices to help organizations manage cybersecurity risks.[5] The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of Government."[6] Additionally, S. Res. 73 (114th Congress) authorizes the Committee to examine "the efficiency and economy of operations of all branches and functions of the Government with particular reference to (i) the effectiveness of present national security methods, staffing and processes...."[7] Because former Secretary Clinton chose to forego using State's official government system, which is governed by strict federal cybersecurity guidelines, the Committees have questions about whether the level of security of Secretary Clinton's private server and email account is comparable to the cybersecurity standards prescribed by the NIST Framework and reiterate our prior requests for information from Platte River Networks.

Please provide this information and material as soon as possible, but no later than 5:00 p.m. on July 26, 2016. In addition, please coordinate with Committees staff in order to arrange for the staff-level interviews. If Platte River Networks does not provide all of the requested materials, the Committees will consider use of the compulsory process.

---

[4] Nat'l Institute of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (last visited Jan. 12, 2016).
[5] *Id.*
[6] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[7] S. Res. 73 § 12, 114th Cong. (2015).

If you have any questions about this request, please contact Science Committee staff at 202-225-6371 or Homeland Security Committee staff at 202-224-4751. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman
Committee on Science, Space,
and Technology
U.S. House of Representatives

Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs
U.S. Senate

cc: The Honorable Eddie Bernice Johnson
Ranking Minority Member
Committee on Science, Space, and Technology

The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

Congress of the United States
Washington, DC 20515

July 12, 2016

Mr. Victor Nappe
Chief Executive Officer
SECNAP Network Security Corp.
Technology Research Park
3651 FAU Boulevard, Suite 400
Boca Raton, FL 33431

Dear Mr. Nappe:

The House Committee on Science, Space, and Technology and the Senate Committee on Homeland Security and Governmental Affairs are examining former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. The Committees understand that a product offered by SECNAP Network Security Corp. (SECNAP)—CloudJacket SMB—was purchased to perform threat monitoring of the network connected to Secretary Clinton's private server in June 2013. We write to reiterate our previous requests for information regarding SECNAP's role relating to the security of Secretary Clinton's private server and email account.

On July 5, 2016, Federal Bureau of Investigation (FBI) Director James Comey announced the conclusion of the FBI's investigation into Secretary Clinton. While the FBI did not recommend charges against Secretary Clinton, it did identify numerous security concerns regarding Secretary Clinton's use of a private server and email account. Specifically, Director Comey said that "it is possible that hostile actors gained access to Secretary Clinton's personal email account."[1] This finding was based on the fact that "hostile actors gained access to the private commercial e-mail accounts of people with whom Secretary Clinton was in regular contact from her personal account."[2] In addition, Director Comey raised the concern about the possibility that Secretary Clinton's server was hacked because of the fact that her personal e-mail domain was known by a large number of people and "she also used her personal email extensively while outside the United States, including sending and receiving work-related emails in the territory of sophisticated adversaries."[3]

On October 5, 2015, Senator Ron Johnson, chairman of the Senate Homeland Security and Governmental Affairs Committee, wrote to you seeking information about the SECNAP device used in conjunction with Secretary Clinton's private server. In addition, on January 14, 2016, Congressman Lamar Smith, chairman of the House Committee on Science, Space, and Technology, wrote to you seeking similar information. SECNAP declined to provide complete responses to the Committees' inquiries, citing that it did not have its client's consent to produce documents or information. Therefore, we are writing to jointly reiterate the previous requests for

---

[1] Fed. Bureau of Investigation, Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System (July 5, 2016).
[2] *Id.*
[3] *Id.*

information and materials that SECNAP has yet to provide. The information that Committees seek from SECNAP will offer better insight into the security capabilities of Secretary Clinton's private server and what potential vulnerabilities to federal records and sensitive information need to be mitigated.

The Committee on Science, Space, and Technology has jurisdiction over the National Institute of Standards and Technology (NIST) which develops cybersecurity standards and guidelines as set forth in House Rule X. The NIST publishes the *Framework for Improving Critical Infrastructure Cybersecurity* (the Framework).[4] The Framework sets industry standards and best practices to help organizations manage cybersecurity risks.[5] The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of Government."[6] Additionally, S. Res. 73 (114th Congress) authorizes the Committee to examine "the efficiency and economy of operations of all branches and functions of the Government with particular reference to (i) the effectiveness of present national security methods, staffing and processes…."[7] Because former Secretary Clinton chose to forego using State's official government system, which is governed by strict federal cybersecurity guidelines, the Committees have questions about whether the level of security of Secretary Clinton's private server and email account is comparable to the cybersecurity standards prescribed by the NIST Framework and reiterate our prior requests for information from SECNAP.

Please provide this information and material as soon as possible, but no later than 5:00pm on July 26, 2016. If SECNAP does not provide all of the requested materials, the Committees will consider use of the compulsory process.

If you have any questions about this request, please contact Science Committee staff at 202-225-6371 or Homeland Security Committee staff at 202-224-4751. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman
Committee on Science, Space,
and Technology
U.S. House of Representatives

Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs
U.S. Senate

---

[4] Nat'l Institute of Standards & Tech., *Framework for Improving Critical Infrastructure Cybersecurity* (Feb. 12, 2014), *available at* http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf (last visited Jan. 12, 2016).
[5] *Id.*
[6] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[7] S. Res. 73 § 12, 114th Cong. (2015).

cc: The Honorable Eddie Bernice Johnson
Ranking Minority Member
Committee on Science, Space, and Technology

The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

Congress of the United States
Washington, DC 20515

August 22, 2016

Mr. Austin McChord
Chief Executive Officer
Datto, Inc.
101 Merritt 7, 7th Floor
Norwalk, CT 06851

Dear Mr. McChord:

The House Committee on Science, Space, and Technology and the Senate Committee on Homeland Security and Governmental Affairs are examining former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. The Committees understand that a product offered by Datto, Inc.—the Datto SIRIS S2000—was purchased in 2013 for Secretary Clinton to provide on-site, immediate recovery of backup data in the event that the primary server failed. According to Datto's previous written responses to the Committees, Datto could not produce documents pursuant to the Committees' requests[1] because it did not have consent from its client. Datto is uniquely situated to provide firsthand information about its product and how it was used in conjunction with Secretary Clinton's private server and email account. Therefore, in order to assist Datto in producing the requested information, Chairman Smith has enclosed a subpoena for that material.

For several months, we have sought Datto's voluntary cooperation with congressional efforts to understand the policy consequences of Secretary Clinton's use of a private server and email account. This effort, undertaken concurrently with a federal criminal investigation, has a different focus than the criminal inquiry and derives from different authority. "The scope of [Congress's] power of inquiry . . . is as penetrating and far-reaching as the potential power to enact and appropriate under the Constitution."[2] The congressional investigatory power "encompasses inquiries concerning the administration of existing laws as well as proposed or possibly needed statutes."[3] The Committees have particular jurisdiction in this inquiry pursuant to House Rule X and Senate Rule XXV, respectively.

---

[1] On October 5, 2015, Senator Ron Johnson, chairman of the Senate Homeland Security and Governmental Affairs Committee, wrote to you seeking information about the Datto device used in conjunction with Secretary Clinton's private server. Separately, on January 14, 2016, Congressman Lamar Smith, chairman of the House Committee on Science, Space, and Technology, wrote to you seeking similar information. Datto declined to provide complete responses to the Committees' inquiries, citing that it did not have its client's consent to produce documents or information. On July 12, 2016, Chairman Smith and Johnson jointly reiterated their previous requests for information and materials, but Datto again declined through counsel, citing it did not have its client's consent.

[2] *Eastland v. U.S. Servicemen's Fund*, 421 U.S. 491, 504, n. 15 (1975) (quoting Barenblatt v. United States, 360 U.S. 109, 111 (1959)).

[3] *Watkins v. United States*, 354 U.S. 178, 187 (1957).

On July 5, 2016, Federal Bureau of Investigation (FBI) Director James Comey announced the conclusion of the FBI's investigation into Secretary Clinton. Although the FBI did not recommend criminal charges against Secretary Clinton, Director Comey explained that Secretary Clinton's actions handling classified information were "extremely careless."[4] In addition, as we noted in our previous letter to you, the FBI identified numerous security concerns regarding Secretary Clinton's use of a private server and email account that could merit changes to federal law. While the FBI's criminal investigation is instructive for the Committees' examination, it does not substitute for the Committees' fact-finding. Among other topics, the Committees have questions about the structure and security of Secretary Clinton's email system, whether it was comparable to the cybersecurity standards prescribed by the NIST Framework, and the preservation of records on the system.

The information sought by the Committees is crucial in furthering the Committee's understanding of Secretary Clinton's private server and informing policy changes to prevent similar email arrangements in the future. Please provide the documents responsive to the enclosed subpoena by September 9, 2016. Please contact Drew Colliatie of Chairman Smith's staff with any questions about the subpoena. Thank you for your attention to this important matter.

Sincerely,

Lamar Smith
Chairman
Committee on Science, Space,
and Technology
U.S. House of Representatives

Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs
U.S. Senate

cc: The Honorable Eddie Bernice Johnson
Ranking Minority Member
Committee on Science, Space, and Technology

The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

Enclosures

---

[4] Fed. Bureau of Investigation, Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal EMail System (July 5, 2016).

Congress of the United States
Washington, DC 20515

August 22, 2016

Mr. Treve Suazo
Chief Executive Officer
Platte River Networks
5700 Washington Street
Denver, CO 80216

Dear Mr. Suazo:

The House Committee on Science, Space, and Technology and the Senate Committee on Homeland Security and Governmental Affairs are examining former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. According to information obtained by the Committees, Secretary Clinton hired Platte River Networks to provide information technology services for Secretary Clinton's private server and email account. Platte River Networks (PRN) declined to comply in full with the Committees' requests for documents and interviews.[1] Therefore, in order to enable the Committees to fully examine the circumstances surrounding Secretary Clinton's private server and email account, Chairman Smith has issued the enclosed subpoena for documents.

For several months, we have sought PRN's voluntary cooperation with congressional efforts to understand the policy consequences of Secretary Clinton's use of a private server and email account. This effort, undertaken concurrently with a federal criminal investigation, has a different focus than the criminal inquiry and derives from different authority. "The scope of [Congress's] power of inquiry . . . is as penetrating and far-reaching as the potential power to enact and appropriate under the Constitution."[2] The congressional investigatory power "encompasses inquiries concerning the administration of existing laws as well as proposed or possibly needed statutes."[3] The Committees have particular jurisdiction in this inquiry pursuant to House Rule X and Senate Rule XXV, respectively.

---

[1] On August 11, 2015, Senator Ron Johnson, chairman of the Senate Homeland Security and Governmental Affairs Committee, wrote to you seeking information and a staff briefing about services provided by PRN relating to Secretary Clinton's private server. After an initial production of documents, Chairman Johnson's staff requested the opportunity to speak directly with PRN employees familiar with Secretary Clinton's servers' configuration. PRN, through its counsel, refused. Separately, on January 14, 2016, Congressman Lamar Smith, chairman of the House Committee on Science, Space, and Technology, wrote to you seeking similar information. PRN declined to provide complete responses to the Chairman Smith's inquiry and declined to provide relevant employees to be interviewed by Chairman Johnson's staff. On July 12, 2016, Chairman Smith and Chairman Johnson jointly reiterated their previous requests for information and materials, but PRN again declined through counsel to product the requested information.

[2] *Eastland v. U.S. Servicemen's Fund*, 421 U.S. 491, 504, n. 15 (1975) (quoting Barenblatt v. United States, 360 U.S. 109, 111 (1959)).

[3] *Watkins v. United States*, 354 U.S. 178, 187 (1957).

Following the Committees' July 12, 2016, letter, your attorney has refused to cooperate with the Committees' ongoing investigation. Science Committee staff attempted to reach out to your attorney on multiple occasions through phone calls, voicemails, and e-mails to learn about the status of providing information responsive to the Committees' requests. Yet, instead of providing a timely and substantive response to the Committees' requests, your attorney sent an e-mail nearly one month following the Committees' letter, criticizing Science Committee staff's efforts to reach him via phone and demanding only to communicate in writing, which he apparently does not believe includes e-mail. When asked again by Science Committee staff to have a phone conversation regarding the ongoing inquiry, your attorney refused to provide a response, citing that he was traveling in Europe. Finally, over a month after the Committees' July 12, letter, your attorney unequivocally refused to accept electronic service on your behalf, stating in a subject line of an e-mail, "Platte River Networks REJECTS electronic service," providing no explanation or text in the body of the e-mail.[4]

PRN is uniquely situated to provide firsthand information about Secretary Clinton's private server and email account. The timeline of PRN's involvement with Secretary Clinton's email systems suggests that PRN has unique knowledge about the state of Secretary Clinton's system at the time she left the State Department. In addition, at least two PRN employees had repeated and detailed communications with representatives of Secretary Clinton about the email system for a period of several years.[5]

On July 5, 2016, Federal Bureau of Investigation (FBI) Director James Comey announced the conclusion of the FBI's investigation into Secretary Clinton. Although the FBI did not recommend criminal charges against Secretary Clinton, Director Comey explained that Secretary Clinton's actions handling classified information were "extremely careless."[6] In addition, as we noted in our previous letter to you, the FBI identified numerous security concerns regarding Secretary Clinton's use of a private server and email account that could merit changes to federal law. While the FBI's criminal investigation is instructive for the Committees' examination, it does not substitute for the Committees' fact-finding. Among other topics, the Committees have questions about the structure and security of the email system, whether it was comparable to the cybersecurity standards prescribed by the NIST Framework, and the preservation of records on the system.

The information sought by the Committees is crucial in furthering the Committees' understanding of Secretary Clinton's private server and informing policy changes to prevent similar email arrangements in the future. Please provide the documents responsive to the enclosed subpoena by September 9, 2016. Please contact Drew Colliatie of Chairman Smith's

---

[4] E-mail from Kenneth Eichner, Attorney, Eichner Law, to Committee Staff (Aug. 19, 2016, 10:33 p.m.).
[5] *See* Letter from Sen. Ron Johnson, Chairman, U.S. Senate Homeland Security & Governmental Affairs Committee, to Austin McChord, CEO, Datto, Inc. (Oct. 5, 2015); Letter from Sen. Ron Johnson, Chairman, U.S. Senate Homeland Security & Governmental Affairs Committee, to Victor Nappe, CEO, SECNAP Network Security Corp. (Oct. 5, 2015).
[6] Fed. Bureau of Investigation, Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal Email System (July 5, 2016).

staff with any questions about the subpoena. Thank you for your attention to this important matter.

Sincerely,

Lamar Smith
Chairman
Committee on Science, Space,
and Technology
U.S. House of Representatives

Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs
U.S. Senate

cc: The Honorable Eddie Bernice Johnson
Ranking Minority Member
Committee on Science, Space, and Technology

The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

Enclosures

Congress of the United States
Washington, DC 20515

August 22, 2016

Mr. Victor Nappe
Chief Executive Officer
SECNAP Network Security Corp.
Technology Research Park
3651 FAU Boulevard, Suite 400
Boca Raton, FL 33431

Dear Mr. Nappe:

The House Committee on Science, Space, and Technology and the Senate Committee on Homeland Security and Governmental Affairs are examining former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. The Committees understand that a product offered by SECNAP Network Security Corp. (SECNAP)—CloudJacket SMB—was purchased to perform threat monitoring of the network connected to Secretary Clinton's private server in June 2013. According to SECNAP's previous written responses to the Committees, SECNAP could not produce documents pursuant to the Committees' requests[1] because it did not have consent from its clients. SECNAP is uniquely situated to provide firsthand information about its product and how it was used in conjunction with Secretary Clinton's private server and email account. Therefore, in order to assist SECNAP in producing the requested information, Chairman Smith has enclosed a subpoena for that material.

For several months, we have sought SECNAP's voluntary cooperation with congressional efforts to understand the policy consequences of Secretary Clinton's use of a private server and email account. This effort, undertaken concurrently with a federal criminal investigation, has a different focus than the criminal inquiry and derives from different authority. "The scope of [Congress's] power of inquiry . . . is as penetrating and far-reaching as the potential power to enact and appropriate under the Constitution."[2] The congressional investigatory power "encompasses inquiries concerning the administration of existing laws as well as proposed or possibly needed statutes."[3] The Committees have particular jurisdiction in this inquiry pursuant to House Rule X and Senate Rule XXV, respectively.

---

[1] On October 5, 2015, Senator Ron Johnson, chairman of the Homeland Security and Governmental Affairs Committee, wrote to you seeking information about the SECNAP device used in conjunction with Secretary Clinton's private server. Separately, on January 14, 2016, Congressman Lamar Smith, chairman of the Committee on Science, Space, and Technology, wrote to you seeking similar information. SECNAP declined to provide complete responses to the Committees' inquiries, citing that it did not have its clients' consent to produce documents or information. On July 12, 2016, Chairman Smith and Johnson jointly reiterated their previous requests for information and materials, but SECNAP again declined through counsel, citing it did not have its clients' consent.

[2] *Eastland v. U.S. Servicemen's Fund*, 421 U.S. 491, 504, n. 15 (1975) (quoting Barenblatt v. United States, 360 U.S. 109, 111 (1959)).

[3] *Watkins v. United States*, 354 U.S. 178, 187 (1957).

On July 5, 2016, Federal Bureau of Investigation (FBI) Director James Comey announced the conclusion of the FBI's investigation into Secretary Clinton. Although the FBI did not recommend criminal charges against Secretary Clinton, Director Comey explained that Secretary Clinton's actions handling classified information were "extremely careless."[4] In addition, as we noted in our previous letter to you, the FBI identified numerous security concerns regarding Secretary Clinton's use of a private server and email account that could merit changes to federal law. While the FBI's criminal investigation is instructive for the Committees' examination, it does not substitute for the Committees' fact-finding. Among other topics, the Committees have questions about the structure and security of Secretary Clinton's email system, whether it was comparable to the cybersecurity standards prescribed by the NIST Framework, and the preservation of records on the system.

The information sought by the Committees is crucial in furthering the Committee's understanding of Secretary Clinton's private server and informing policy changes to prevent similar email arrangements in the future. Please provide the documents responsive to the enclosed subpoena by September 9, 2016. Please contact Drew Colliatie of Chairman Smith's staff with any questions about the subpoena. Thank you for your attention to this important matter.

Sincerely,

Lamar Smith
Chairman
Committee on Science, Space,
and Technology
U.S. House of Representatives

Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs
U.S. Senate

cc: The Honorable Eddie Bernice Johnson
Ranking Minority Member
Committee on Science, Space, and Technology

The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and Governmental Affairs

Enclosures

---

[4] Fed. Bureau of Investigation, Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal EMail System (July 5, 2016).

Congress of the United States
Washington, DC 20515

September 9, 2016

The Honorable Loretta E. Lynch
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Dear Attorney General Lynch,

The House Committee on Science, Space, and Technology and the Senate Committee on Homeland Security and Governmental Affairs are examining former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. Materials released by the Federal Bureau of Investigation (FBI) on September 2, 2016,[1] raise significant questions about the security of Secretary Clinton's server, including how her aides tasked with managing her server ensured that our nation's most sensitive national security information stored on her server was not compromised. In light of the FBI's selective release of certain information, the Committees are requesting additional materials necessary to further their oversight.

Following calls from across the political spectrum and Freedom of Information Act requests for the FBI to release all information obtained during the course of its investigation into the security of Secretary Clinton's private server,[2] the FBI self-selected certain information for public release on September 2, 2016.[3] Included in these materials were a summary of Secretary Clinton's July 2, 2016, interview with the FBI and a summary of the investigation.[4] Although the FBI opted not to make *all* information obtained during the course of its investigation public, the FBI's selective release raises significant additional questions about how Secretary Clinton's aides tasked with managing the private email arrangement handled highly sensitive information stored on her server.

Interviews summarized by the FBI indicate that a Platte River Networks employee, at the behest of Mrs. Clinton's top adviser, Cheryl Mills, apparently carried out mass deletions of information contained on Mrs. Clinton's email server, using software called BleachBit, *after* the *New York Times* uncovered the existence of her private server and email arrangement in March

---

[1] Federal Bureau of Investigation, Press Release, *FBI Releases Documents in Hillary Clinton E-Mail Investigation* (Sept. 2, 2016), *available at* https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-documents-in-hillary-clinton-e-mail-investigation (last visited Sept. 9, 2016) [hereinafter FBI Press Release, Sept. 2, 2016].
[2] *See, e.g.*, Harper Neidig, *Clinton Camp Wants FBI Interview Files Released to the Public*, THE HILL, Aug. 16, 2016, *available at* http://thehill.com/blogs/ballot-box/presidential-races/291646-clinton-campaign-calls-for-fbi-interview-notes-to-be (last visited Sept. 9, 2016); Reena Flores, *FBI Releases Documents from Hillary Clinton Email Investigation*, CBS NEWS, Sept. 2, 2016, *available at* http://www.cbsnews.com/news/fbi-releases-documents-from-hillary-clinton-email-investigation/ (last visited Sept. 9, 2016).
[3] FBI Press Release, Sept. 2, 2016, *supra* note 1.
[4] *Id.*

2015.[5] The same Platte River Networks employee charged with deleting emails forgot to do so as instructed. During an interview with the FBI, the Platte River Networks employee apparently declared he had an "oh s***" moment when he remembered that he had been directed to delete the files back in December 2014, but had failed to do so.[6] Even more troublesome, the employee apparently deleted emails from her server after Benghazi Select Committee Chairman Trey Gowdy issued a preservation order to retain and produce documents.[7] Further, crucial details regarding phone calls between Clinton aides and Platte River Networks employees in the time frame surrounding the mass deletion were withheld from the FBI.[8]

The FBI's release of information regarding its investigation highlights many inherent limitations of its review due to the destruction of evidence and inability to recover devices used by Secretary Clinton.[9] According to the report, Secretary Clinton used 13 email capable devices and one laptop during her tenure as Secretary of State. Secretary Clinton's attorneys, however, were unable to locate *any* of the devices.[10] Clinton aides reportedly destroyed at least two old Blackberries by smashing them with a hammer or breaking them in half.[11]

The FBI stated in its report that "investigative limitations, including the FBI's inability to obtain all mobile devices and various computer components associated with Clinton's personal email systems, **prevented the FBI from conclusively determining whether the classified information transmitted and stored on Clinton's personal server systems was compromised via cyber intrusion or other means**."[12] This admission not only raises questions about the breadth of the review the FBI was able to undertake, but also whether Clinton aides attempted to destroy evidence to avoid answering questions about her private email and server arrangement in the event her unique arrangement was exposed.

Because information obtained during the FBI's investigation is important to furthering the Committees' inquiry, we request that you provide unclassified and unredacted copies of interview notes and any accompanying materials for any interviews of Bryan Pagliano, Justin Cooper, and all employees of Platte River Networks. These individuals tasked by Secretary Clinton and her senior advisors to manage her server did not have security clearances and, in some cases, did not have a particular expertise in cybersecurity. It is important for the American public to have a thorough understanding of how Secretary Clinton's aides handled sensitive national security information.

---

[5] FBI Records, The Vault, at 17–19 (Pt. 01 of 02); Michael Schmidt, *Clinton Used Personal Email Account at State Dept., Possibly Breaking Rules*, NY TIMES, Mar. 2, 2016, *available at* http://www.nytimes.com/2015/03/03/us/politics/hillary-clintons-use-of-private-email-at-state-department-raises-flags.html?_r=0 (last visited Sept. 9, 2016).

[6] FBI Records, The Vault, at 19 (Pt. 01 of 02).

[7] Subpoena issued to The Honorable Hillary R. Clinton, U.S. House of Rep., Select Comm. on the Events Surrounding the 2012 Terrorist Attack in Benghazi, Mar. 4, 2015, *available at* http://benghazi.house.gov/sites/republicans.benghazi.house.gov/files/Kendall.Clinton%20Subpoena%20-%202015.03.04.pdf (last visited Sept. 9, 2016).

[8] FBI Records, The Vault, at 19 (Pt. 01 of 02).

[9] *Id.* at 8–9.

[10] *Id.* at 8.

[11] *Id.* at 9.

[12] *Id.* at 2. Emphasis added.

The FBI has expressed its "commitment to transparency with respect to the FBI's investigation of former Secretary of State Clinton's use of a personal email server."[13] The Committees request that you, along with Director Comey, follow through on this commitment by providing the requested information sought by the Committees, which is crucial to furthering the Committees' understanding of Secretary Clinton's private server and informing policy changes to prevent similar email arrangements in the future. "The scope of [Congress's] power of inquiry . . . is as penetrating and far-reaching as the potential power to enact and appropriate under the Constitution."[14] The congressional investigatory power "encompasses inquiries concerning the administration of existing laws as well as proposed or possibly needed statutes."[15] The Committees have particular jurisdiction in this inquiry pursuant to House Rule X and Senate Rule XXV, respectively.

Please provide the documents responsive to the request by September 16, 2016. Enclosed are instructions for producing documents to the Committees. Please contact Drew Colliatie or Caroline Ingram of Chairman Smith's staff or Michael Lueptow or Scott Wittmann with Senator Johnson's staff with any questions. Thank you for your attention to this important matter.

Sincerely,

Lamar Smith
Chairman
Committee on Science, Space,
and Technology
U.S. House of Representatives

Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs
U.S. Senate

cc: The Honorable James B. Comey, Jr., Director
Federal Bureau of Investigation

The Honorable Eddie Bernice Johnson, Ranking Minority Member
Committee on Science, Space, and Technology

The Honorable Thomas R. Carper, Ranking Member
Committee on Homeland Security and Governmental Affairs

Enclosure

---

[13] Matt Zapotsky, *Documents from the Hillary Clinton Email Investigation Might be Made Public*, WASH. POST, Aug. 17, 2016, *available at* https://www.washingtonpost.com/news/powerpost/wp/2016/08/17/documents-from-the-hillary-clinton-email-investigation-might-be-made-public/ (last visited Sept. 9, 2016).
[14] *Eastland v. U.S. Servicemen's Fund*, 421 U.S. 491, 504, n. 15 (1975) (quoting *Barenblatt v. United States*, 360 U.S. 109, 111 (1959)).
[15] *Watkins v. United States*, 354 U.S. 178, 187 (1957).

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

October 28, 2016

The Honorable James B. Comey
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, DC 20535

Dear Director Comey:

On October 28, 2016, I received your letter supplementing your testimony to the Committee about the FBI's investigation of former Secretary Clinton's use of a private email server. In your letter, you stated that "the FBI has learned of the existence of emails that appear to be pertinent to the investigation."[1] Now that the FBI has become aware of these new emails, you noted that the FBI will take "appropriate investigative steps designed to allow investigators to review these emails to determine whether they contain classified information, as well as to assess their importance to [the FBI's] investigation."[2]

You had previously stated in your testimony to Congress that "I wanted to be as transparent as possible."[3] In line with your commitment to be transparent with Congress and the public, I respectfully request that the FBI provide as much information as possible about these new developments without harming the integrity of its ongoing investigation. In particular, there are important questions about the nature and source of these new emails, when and how the FBI learned of them, what investigative steps the FBI is taking to obtain these emails, and the role of the Justice Department in the process. Most importantly, if the FBI determines that any additional classified information has been put at risk of exposure to our enemies, it is vital that the intelligence community take all appropriate steps to mitigate the potential damage to our national security.

---

[1] Letter from The Honorable James Comey, Director, Fed. Bureau of Investigation, to Sen. Ron Johnson, S. Comm. on Homeland Security & Gov't Affairs, et al. (Oct. 28, 2016).
[2] *Id.*
[3] *Oversight of the State Department Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (2016) (testimony of The Honorable James Comey, Director, Fed. Bureau of Investigation).

My staff has informally requested more information from the FBI, which declined the request. Accordingly, in the interest of transparency, I ask that you make your staff available to brief my staff on these and other related questions as soon as possible, but no later than November 4, 2016. Thank you for your prompt attention to this important matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

November 7, 2016

The Honorable James B. Comey
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue, NW
Washington, DC 20535

Dear Director Comey:

The Committee on Homeland Security and Governmental Affairs continues to examine former Secretary of State Hillary Clinton's use of a private email system for official business. On July 5, 2016, you informed the American public that Secretary Clinton's use of a private email system was "extremely careless" and that you could not rule out the possibility that foreign adversaries gained access to her email system.[1] The Federal Bureau of Investigation's (FBI) examination found 81 email chains with 193 individual emails on Secretary Clinton's email system that contained information classified at the time the emails were sent or received.[2] The FBI also found that Secretary Clinton emailed directly with President Obama while outside the United States.[3] You recommended against prosecution, however—a recommendation which the Attorney General accepted.

On October 28, 2016, you notified the Committee that "the FBI has learned of the existence of emails that appear to be pertinent to the investigation."[4] You wrote that the FBI would take steps to obtain and review the new emails.[5] On November 6, 2016, you again wrote to the Committee, writing "[b]ased on our review, we have not changed our conclusions that we expressed in July with respect to Secretary Clinton."[6]

Your two most recent letters to the Committee leave several unanswered questions about this new material and the FBI's review of it. Accordingly, in the interest of transparency, I ask that you please provide the following information and material as soon as possible:

---

[1] Fed. Bureau of Investigation, Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System (July 5, 2016).
[2] Fed. Bureau of Investigation, Clinton E-mail Investigation: Mishandling of Classified – Unknown Subject or Country (SIM) 20 (July 2016).
[3] *Id.* at 15; *see also* Fed. Bureau of Investigation, Summary of Interview of Huma Abedin 10 (Apr. 5, 2016).
[4] Letter from The Honorable James Comey, Director, Fed. Bureau of Investigation, to Sen. Ron Johnson, S. Comm. on Homeland Security & Gov't Affairs, et al. (Oct. 28, 2016).
[5] *Id.*
[6] Letter from The Honorable James Comey, Director, Fed. Bureau of Investigation, to Sen. Ron Johnson, S. Comm. on Homeland Security & Gov't Affairs, et al. (Nov. 6, 2016).

1. Within the material reviewed by the FBI since October 28, how many new emails did the FBI identify that were not duplicates of emails already reviewed? Has the FBI provided these new emails to the State Department?

2. Within the material reviewed by the FBI since October 28, how many emails contained information classified at the time the emails were sent or received? Please provide this information broken down by classification level.

3. Within the material reviewed by the FBI since October 28, did the FBI identify any new individuals who either sent or received classified information on an unclassified email system? Please provide the names of these individuals.

4. Your November 6 letter limits your conclusions "with respect to Secretary Clinton."[7] Is the FBI continuing to examine matters relating to other current or former State Department employees relating to the mishandling of classified information or the destruction of federal records? Please explain.

5. Did the FBI obtain the emails reviewed since October 28 via a search warrant or subpoena? Please explain.

6. Did the FBI consult or notify the Justice Department about its conclusion prior to your November 6 letter to Congress? If so, which Justice Department official(s) were notified?

7. News reports suggest that the FBI discovered the new emails relating to Secretary Clinton's private email system during a separate investigation into former Congressman Anthony Weiner.[8] Are these reports accurate?

8. According to a *Washington Post* report, "senior FBI officials" knew about the new emails related to Secretary Clinton's email system "at least two weeks before Director James B. Comey notified Congress."[9] Please provide a detailed timeline of the FBI's discovery of the new emails and the notification of FBI and Justice Department leadership.

9. Another recent news report suggests that "senior Justice Department officials" warned you against sending your October 28 letter to Congress.[10] If this report is accurate, please identify the officials who attempted to persuade you not to communicate with Congress.

10. A recent news report suggests that Secretary Clinton allowed a member of her household staff who did not have a security clearance to handle classified information, and even

---

[7] *Id.*
[8] *See, e.g.*, *FBI reported found new Huma Abedin emails on Anthony Weiner laptop*, The Week, Nov. 4, 2016.
[9] Sari Horowitz & Ellen Nakashima, *Senior FBI officials were told of new emails in early October but wanted more information before renewing Clinton probe*, Wash. Post, Nov. 2, 2016.
[10] Devlin Barrett, *Justice Department officials warned FBI's Comey about sending letter on Clinton emails*, Wall St. J., Oct. 29, 2016.

allowed her to have access to the sensitive compartmented information facility in Secretary Clinton's home.[11] Did the FBI examine these facts? If so, did the FBI determine whether this individual in fact had access to classified information? Did the FBI take into account these facts when evaluating whether former Secretary Clinton was grossly negligent in the handling of classified information?

I ask that you please provide this information as soon as possible. Thank you for your prompt attention to this important matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

[11] Paul Sperry, *Clinton directed her maid to print out classified materials*, N.Y. Post, Nov. 6, 2016.

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

September 8, 2017

Mr. Adam Miles
Acting Special Counsel
U.S. Office of Special Counsel
1730 M Street, NW
Washington, DC 20036

Dear Mr. Miles:

I write to seek information about the Office of Special Counsel's (OSC) investigation concerning former FBI Director James Comey.[1] I respectfully request your cooperation with this inquiry.

In November 2016, OSC opened an investigation to determine whether Mr. Comey violated the Hatch Act in the course of the FBI's investigation into former Secretary of State Hillary Clinton's private email system.[2] As part of its investigation, the OSC requested information from Mr. Comey in November 2016, but it is unclear whether Mr. Comey provided any information to OSC.[3] During the investigation, OSC apparently reviewed documents from the FBI and interviewed two FBI officials, Trisha Anderson and former FBI chief of staff Jim Rybicki, in May 2017.[4] OSC's investigation ran about seven months, until OSC closed its investigation following Mr. Comey's departure from the FBI.[5]

During its investigation of Mr. Comey, OSC executed at least three non-disclosure agreements (NDA) relating to FBI information obtained during the course of OSC's investigation.[6] The NDAs—signed only by an employee of OSC—covered information about the identities of FBI employees interviewed, information deemed to be "deliberative," and information deemed to be "protected by attorney client privilege."[7] By the terms of the NDAs, OSC restricted itself from releasing information without "prior written authorization from the Department of Justice."[8]

---

[1] U.S. Office of Special Counsel Complaint No. HA-17-0515.
[2] Comm. staff email with the Office of Special Counsel (Sep. 1, 2017).
[3] *Id.*
[4] *Id.*
[5] *Id.*
[6] Comm. staff email with the Office of Special Counsel (Sep. 6, 2017).
[7] Non-Disclosure Agreement Re: U.S. Office of Special Counsel ("OSC") Complaint No. HA-17-0515, Jan. 17, 2017 [herein after FBI Identity NDA]; Non-Disclosure Agreement Regarding Deliberative Processed Privileged Material Re: U.S. Office of Special Counsel ("OSC") Complaint No. HA-17-0515, Feb. 15, 2017 [herein after Deliberative Process NDA]; Non-Disclosure Agreement Regarding Attorney Client Privileged Material Re: U.S. Office of Special Counsel ("OSC") Complaint No. HA-17-0515, Feb. 23, 2017[herein after Attorney-Client NDA].
[8] *See* Attorney-Client NDA paragraph 5, *supra* note 8; *see also*, Deliberative Process NDA paragraph 5, *supra* note 10; *see also* FBI Identity paragraph 5 NDA, *supra* note 13.

If OSC sought to produce information to Congress, the NDAs require the agency to redact the protected information and provide the FBI an opportunity "to review a read-through version of the redacted report and any other records [OSC] intends to release to propose additional redactions that may be necessary to protect [the specified] information and any other law enforcement sensitive information before making such disclosure."[9]

Any reliance upon these non-disclosure agreements to withhold information from the Committee would be inappropriate. The Supreme Court has long recognized Congress's right—rooted in the Constitution—to oversee and investigate the operations of the federal government. The congressional power of inquiry and the processes to enforce it are "an essential and appropriate auxiliary of the legislative function."[10] "The scope of [Congress's] power of inquiry," in the words of the Supreme Court, "is as penetrating and far-reaching as the potential power to enact and appropriate under the Constitution."[11] Courts consistently hold that an agency may not deny Congress information on the basis of an NDA or confidentiality clause.[12] In addition, the Consolidated Appropriations Act of 2017 states that no funds may be used to enforce an NDA if the agreement does not expressly exempt the disclosure of information to Congress.[13] OSC's NDAs in this matter do not contain the required language.

The Committee has conducted oversight of the FBI's investigation into Secretary Clinton's use of a private email system.[14] The information in OSC's possession could further explain the scope, course, and nature of the FBI's investigation. In particular, the information may shed light on the FBI's decision-making process during the FBI's investigation, the FBI's interactions with other federal entities, the FBI's distinction between "extreme carelessness" and "gross negligence," and the potential harm done by Secretary Clinton's use of a private email server. Information obtained by the Committee in this matter could also inform the Committee's oversight of Hatch Act compliance by federal agencies and personnel. In addition, the revelation about the NDAs raise questions about OSC's practices and procedures, as well as OSC's use of NDAs in other matters.

---

[9] *Id.* at paragraph 7. Contrarily, the NDAs included language that nothing in the NDAs "prevents OSC from disclosing [protected] information to the President of the United States, FBI Director Comey, or other officials within the Department of Justice as part of any report of OSC's findings or recommendations." *Id.* at paragraph 8.
[10] *McGrain v. Daugherty*, 273 U.S. 135, 174 (1927).
[11] *Eastland v. U.S. Servicemen's Fund*, 421 U.S. 491, 504, n. 15 (1975) (quoting Barenblatt v. United States, 360 U.S. 109, 111 (1959)).
[12] *See* Morton Rosenberg, When Congress Comes Calling 83 (2017).
[13] Pub. L. 115-31 § 744 (2017).
[14] *See* letter from Sen. Ron Johnson, Chairman, S. Comm. on Homeland Security and Governmental Affairs, to James Comey, Director, Federal Bureau of Investigation, Nov. 7, 2016; letter from Sen. Ron Johnson, Chairman, S. Comm. on Homeland Security and Governmental Affairs, to James Comey, Director, Federal Bureau of Investigation, July 15, 2016.

For these reasons, I respectfully request the following information and material in unredacted form:

1. Has OSC ever executed an NDA limiting the release of information obtained in a Hatch Act investigation? If so, when?

2. Please explain why OSC executed NDAs for purposes of its Hatch Act investigation of former FBI Director Comey.

3. Please explain which federal entities participated in any manner in OSC's Hatch Act investigation of former FBI Director Comey.

4. Please produce all documents and communications referring or relating to the OSC's Hatch Act investigation of former FBI Director Comey (case number HA-17-0515), including but not limited to the full, unredacted transcripts of OSC's interviews of Trisha Anderson and Jim Rybicki.

5. Please produce all communications between OSC and other federal entities referring or relating to the OSC's Hatch Act investigation of former FBI Director Comey (case number HA-17-0515).

Please provide this information as soon as possible but no later than 5:00 p.m. on September 21, 2017.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of the Government,"[15] Additionally, S. Res. 62 (115th Congress) authorizes the Committee to examine "the efficiency and economy of all branches of the Government including the possible existence of fraud, misfeasance, malfeasance, collusion, mismanagement, incompetence, corruption, or unethical practices . . . ."[16]

Thank you for your attention to this matter. If you have any questions about this request, please contact Brian Downey or Kyle Brosnan of the Committee staff at (202) 224-4751.

Sincerely,

Ron Johnson
Chairman

[15] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[16] S. Res. 62 § 12, 115th Cong. (2017).

cc: The Honorable Claire McCaskill
Ranking Member

Enclosure

United States Senate
WASHINGTON, DC 20510

December 6, 2017

The Honorable Michael E. Horowitz
Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Inspector General Horowitz:

We understand that the Department of Justice Office of Inspector General (DOJ OIG) continues its review of the actions of DOJ and the Federal Bureau of Investigation (FBI) in advance of the 2016 presidential election.[1] As part of this review, your office discovered that a senior FBI agent allegedly exchanged electronic text messages "that expressed anti-Trump political views" with an FBI colleague.[2] We write to seek more information about the OIG's discovery of these electronic text messages and the actions you took in response.

According to reports, FBI employees Peter Strzok and Lisa Page were involved in the exchange of text messages that exhibited political bias.[3] Mr. Strzok was involved in the FBI's investigation into former Secretary of State Hillary Clinton's handling of classified information through her use of a private email server. Mr. Strzok personally participated in the FBI's interviews of Secretary Clinton, Huma Abedin, Cheryl Mills, Heather Samuelson, and Jake Sullivan.[4] Mr. Strzok most recently worked for Special Counsel Robert Mueller.[5] Mr. Mueller's office announced that it removed Mr. Strzok from the investigation after learning of the allegations.[6]

To understand OIG's discovery of these text exchanges, we respectfully request the following information:

1. When and how did OIG become aware of the text messages between Peter Strzok and Lisa Page?

---

[1] The Department of Justice Office of Inspector General released the following statement in response to inquiries today, (2017), https://oig.justice.gov/press/2017/2017-12-02.pdf (last visited Dec 5, 2017).
[2] Michael S. Schmidt, Matt Apuzzo and Adam Goldman, *Mueller Removed Top Agent in Russia Inquiry Over Possible Anti-Trump Texts*, N.Y. TIMES, Dec. 2, 2017, https://www.nytimes.com/2017/12/02/us/politics/mueller-removed-top-fbi-agent-over-possible-anti-trump-texts.html.
[3] Karoun Demirjian and Devlin Barret, *Top FBI official assigned to Mueller's Russia probe said to have been removed after sending anti-Trump texts*, WASH. POST, Dec. 2, 2017, https://www.washingtonpost.com/world/national-security/two-senior-fbi-officials-on-clinton-trump-probes-exchanged-politically-charged-texts-disparaging-trump/2017/12/02/9846421c-d707-11e7-a986-d0a9770d9a3e_story.html?utm_term=.93899dad030d
[4] Fed. Bureau of Investigation, 302s of Clinton Investigation (2015-16) (on file with Comm.).
[5] Michael S. Schmidt, Matt Apuzzo and Adam Goldman, *Mueller Removed Top Agent in Russia Inquiry Over Possible Anti-Trump Texts*, N.Y. TIMES, Dec. 2, 2017 https://www.nytimes.com/2017/12/02/us/politics/mueller-removed-top-fbi-agent-over-possible-anti-trump-texts.html.
[6] *Id.*

2. When and how did OIG notify the Special Counsel Robert Mueller of the text messages?

3. Did OIG refer these allegations to the U.S. Office of Special Counsel to pursue a potential Hatch Act inquiry? If not, why not?

4. In connection with the OIG's review of the actions of DOJ and the FBI in advance of the 2016 presidential election, has the OIG received any similar allegations involving other government officials?

Please respond as soon as possible but no later than 5:00 p.m. on December, 13, 2017, so that the Committees may begin to receive responsive information.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of the Government."[7] Additionally, S. Res. 62 (115th Congress) authorizes the Committee to examine "the efficiency and economy of all branches and functions of Government with particular references to the operations and management of Federal regulatory policies and programs."[8]

If you have any questions about this request, please ask your staff to contact Brian Downey of Chairman Johnson's staff at (202) 224-4751 or Josh Flynn-Brown of Chairman Grassley's staff at (202) 224-5225. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs

Charles E. Grassley
Chairman
Committee on the Judiciary

cc: The Honorable Claire McCaskill
Ranking Member
Committee on Homeland Security and Governmental Affairs

The Honorable Dianne Feinstein
Ranking Member
Committee on the Judiciary

---

[7] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[8] S. Res. 62 § 12, 115th Cong. (2017).

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

December 6, 2017

The Honorable Rod J. Rosenstein
Acting Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Acting Attorney General Rosenstein:

I understand the Department of Justice (DOJ) is reviewing thousands of electronic text messages sent and received by Federal Bureau of Investigation (FBI) employees Peter Strzok and Lisa Page for production to Congress.[1] These text messages exchanged between Strzok and Page reportedly "expressed anti-Trump political views."[2] I write to seek more information about your awareness of these text messages and what actions, if any, you took in response.

Strzok reportedly "helped lead" the FBI's investigation into former Secretary of State Hillary Clinton's handling of classified information through her use of a private email server.[3] During the FBI's investigation of Secretary Clinton, Strzok participated in interviews of Clinton, Huma Abedin, Cheryl Mills, Heather Samuelson, and Jake Sullivan.[4] In addition, Strzok reportedly edited then-FBI Director James Comey's statement about Secretary Clinton, changing the description of her actions from "grossly negligent" to "extremely careless."[5]

After you tapped Robert Mueller as special counsel to examine potential Russian interference in the 2016 election,[6] Strzok reportedly began "play[ing] a major role" in the investigation.[7] Mueller removed Strzok from the investigation after becoming aware of the text message allegations.[8]

To understand your awareness of these text messages and the Department's actions in response, I respectfully request the following information:

---

[1] *See, e.g.*, Jake Gibson, *'Over 10,000 texts' between ex-Mueller officials found, after discovery of anti-Trump messages*, Fox News, Dec. 6, 2017.
[2] Michael S. Schmidt, Matt Apuzzo & Adam Goldman, *Mueller removed top agent in Russia inquiry over possible anti-Trump texts*, N.Y. Times, Dec. 2, 2017.
[3] *Id.*
[4] Fed. Bureau of Investigation, 302s of Clinton Investigation (2015-16) (on file with Comm.).
[5] Laura Jarrett & Evan Perez, *FBI agent dismissed from Mueller probe changed Comey's description of Clinton to 'extremely careless,'* CNN, Dec. 4, 2017.
[6] Devlin Barrett, Sari Horowitz, & Matt Zapotosky, *Deputy attorney general appoints special counsel to oversee probe of Russian interference in election*, Wash. Post, May 18, 2017.
[7] Schmidt, Apuzzo & Goldman, *supra* note 2.
[8] *Id.*.

1. When and how did you become aware of the text messages allegedly exchanged between FBI employees Peter Strzok and Lisa Page?

2. When and how did the Special Counsel Robert Mueller notify you of the allegations and the decision to remove Peter Strzok?

3. Did you or the Special Counsel Robert Mueller refer these allegations to the U.S. Office of Special Counsel to pursue a potential Hatch Act inquiry? If not, why not?

4. Is the Department aware of any similar text messages sent or received by Peter Strzok during any other investigation?

5. Is the Department aware of any similar allegations involving other government officials?

6. Please produce all documents and communications sent or received by Peter Strzok and Lisa Page referring or relating to candidates for the 2016 presidential election or indicative of political bias.

Please respond as soon as possible but no later than 5:00 p.m. on December 13, 2017, so that the Committee may begin to receive responsive information.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of the Government."[9] Additionally, S. Res. 62 (115th Congress) authorizes the Committee to examine "the efficiency and economy of all branches and functions of Government with particular references to the operations and management of Federal regulatory policies and programs."[10]

If you have any questions about this request, please contact Brian Downey of the Committee staff at (202) 224-4751. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Claire McCaskill
Ranking Member

Enclosure

---

[9] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[10] S. Res. 62 § 12, 115th Cong. (2017).

United States Senate

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

December 13, 2017

The Honorable Christopher Wray
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue
Washington, DC 20535

Dear Director Wray:

The Committee on Homeland Security and Governmental Affairs is continuing its oversight of the Office of Special Counsel's (OSC) Hatch Act investigation of former Federal Bureau of Investigation (FBI) Director James Comey. According to OSC, non-disclosure agreements it executed at the FBI's request prevent OSC from complying in full with the Committee's oversight. Accordingly, I write to request your assistance in better understanding the FBI's actions.

On November 1, 2016, OSC opened an investigation to determine whether Director Comey violated the Hatch Act when he made public statements about the FBI's investigation of former Secretary of State Hillary Clinton's use of a private email server.[1] Over the ensuing months, OSC conducted an extensive Hatch Act investigation of this matter:

- **November 4, 2016:** OSC asked Director Comey to preserve evidence.[2]
- **November 14, 2016**: OSC requested information from Director Comey.[3]
- **December 5, 2016**: The Department of Justice (DOJ) informed OSC that the FBI General Counsel's Office (OGC) was recused from the investigation and that the Executive Office of U.S. Attorneys (EOUSA) would serve as OSC's liaison.[4]
- **December 22, 2016**: EOUSA provided OSC with an initial document production. An email accompanying the production indicated that FBI would not cooperate with OSC's investigation without restrictions on the release of information.[5]
- **January 17, 2017**: OSC executed a non-disclosure agreement (NDA), limiting the release of information concerning the identity of FBI employees.[6]

---

[1] Letter from Tristan Leavitt, Acting Special Counsel, to Sen. Ron Johnson, Chairman, S. Comm. on Homeland Security and Gov't Affairs, Sept. 21, 2017. OSC ultimately received 32 allegations alleging Director Comey violated the Hatch Act through his handling of the Clinton email investigation.

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] Non-Disclosure Agreement Re: U.S. Office of Special Counsel ("OSC") Complaint No. HA-17-0515, Jan. 17, 2017 [hereinafter "FBI Identity NDA"]

- **February 15, 2017**: OSC executed a second NDA, which limited the release of information that the FBI deemed to be deliberative in nature.[7]
- **February 23, 2017**: OSC executed a third NDA, limiting the release of information that the FBI deemed to be covered by the attorney-client privilege.[8] According to OSC, OSC had never before executed NDAs during a Hatch Act investigation.[9]
- **March through April 2017**: EOUSA produced documents and emails to OSC.[10]
- **May 1, 2017**: OSC interviewed FBI attorney Trisha Anderson.[11]
- **May 9, 2017**: OSC interviewed FBI chief of staff James Rybicki.[12]
- **May 9, 2017**: Director Comey is removed from federal service.
- **May 10, 2017**: The date of OSC's scheduled interview with FBI General Counsel James Baker. This interview did not occur.
- **May 18, 2017**: OSC closed its Hatch Act investigation concerning Director Comey.[13]
- **May 31, 2017**: The date of OSC's scheduled interview with Director Comey. This interview did not occur.

On September 8, 2017, I wrote to OSC, requesting the case file of its Hatch Act investigation of former Director Comey.[14] The Committee continues to receive responsive documents from OSC on a rolling basis. However, OSC has informed the Committee that the NDAs prohibit OSC from fully complying with my request.[15] For example, OSC produced a document containing a list of names mentioned in OSC's interview of Mr. Rybicki.[16] OSC redacted five names pursuant to the NDAs.[17] At the Committee's request, OSC asked FBI if the FBI would waive the NDAs with respect to this document and authorize OSC to produce an unredacted document to the Committee.[18] The FBI declined and "specifically requested [OSC] continue to abide by the terms of the NDAs."[19]

---

[7] Non-Disclosure Agreement Regarding Deliberative Processed Privileged Material Re: U.S. Office of Special Counsel ("OSC") Complaint No. HA-17-0515, Feb. 15, 2017 [hereinafter "Deliberative Process NDA"];
[8]Non-Disclosure Agreement Regarding Attorney Client Privileged Material Re: U.S. Office of Special Counsel ("OSC") Complaint No. HA-17-0515, Feb. 23, 2017 [hereinafter "Attorney-Client NDA"].
[9] Under the terms of the NDAs, OSC restricted itself from releasing information without "prior written authorization from the Department of Justice. *See* Attorney-Client NDA paragraph 5; *see also*, Deliberative Process NDA paragraph 5; *see also* FBI Identity NDA at ¶ 5. If OSC sought to produce information to Congress, the NDAs required OSC to redact the protected information and provide the FBI an opportunity "to review a read-through version of the redacted report and any other records [OSC] intends to release to propose additional redactions that may be necessary to protect [the specified] information and any other law enforcement sensitive information before making such disclosure." *Id.* at ¶ 7.
[10] *Id.*
[11] Letter from Tristan Leavitt to Chairman Johnson, *supra* note 1. *See also* email from OSC staff to Comm. Staff, Sept. 11, 2017.
[12] *Id.*
[13] *Id.* OSC historically closes Hatch Act investigations of individuals who separate from federal service.
[14] Letter from Sen. Ron Johnson, Chairman, S. Comm. on Homeland Security and Gov't Affairs to Adam Miles, Acting Special Counsel, U.S. Office of Special Counsel, Sept. 8, 2017.
[15] *See*, letter from Tristian Leavitt to Chairman Johnson, *supra* note 1.
[16] "Transcript Request Form" *OSC Case Number & Name: HA-17-0515 (Comey, James)* submitted to Comm. on Oct. 20, 2107.
[17] *Id.*
[18] Email from OSC staff to Comm. staff, Dec. 12, 2017.
[19] Email from OSC staff to Comm. staff, Dec. 12, 2017.

The FBI's continued reliance upon the NDAs prevents OSC from fully complying with the Committee's inquiry and impedes the Committee's ability to execute its oversight responsibilities. Accordingly, I respectfully request that you please authorize OSC to produce unredacted copies of all material—including transcripts of all OSC interviews with FBI personnel—in relation to OSC's Hatch Act investigation concerning former Director Comey. In addition, to assist the Committee in understanding the FBI's actions in response to OSC's Hatch Act investigation, I respectfully request the following information and material:

1. Please explain the basis for the recusal of the FBI's Office of General Counsel from OSC's Hatch Act Investigation concerning former Director Comey.

2. Please explain why the Executive Office of U.S. Attorney was chosen to facilitate FBI's cooperation with OSC's investigation.

3. Please explain whether the FBI had any involvement with the conception, drafting, or execution of the non-disclosure agreements with OSC.

Please provide this information as soon as possible but no later than 5:00 p.m. on December 27, 2017. Any classified information provided in response to this letter should be provided under separate cover through the Office of Senate Security.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of the Government,"[20] Additionally, S. Res. 62 (115th Congress) authorizes the Committee to examine "the efficiency and economy of all branches of the Government including the possible existence of fraud, misfeasance, malfeasance, collusion, mismanagement, incompetence, corruption, or unethical practices . . . ."[21]

Thank you for your attention to this matter. If you have any questions about this request, please contact Kyle Brosnan or Brian Downey of the Committee staff at (202) 224-4751.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Claire McCaskill – Ranking Member
Enclosure

---

[20] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[21] S. Res. 62 § 12, 115th Cong. (2017).

United States Senate

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

December 14, 2017

The Honorable Christopher Wray
Director
Federal Bureau of Investigation
935 Pennsylvania Avenue
Washington, DC 20535

Dear Director Wray:

The Committee on Homeland Security and Governmental Affairs is continuing its oversight of the Office of Special Counsel's (OSC) Hatch Act investigation of former Federal Bureau of Investigation (FBI) Director James Comey. I write to request additional material concerning the public statements made by Director Comey in reference to the FBI's investigation of former Secretary of State Hillary Clinton's use of a private email server. I appreciate your cooperation with this request.

On November 17, 2017, the FBI produced documents that it had previously transmitted to OSC as part of OSC's Hatch Act investigation of Director Comey.[1] These documents help to inform the Committee's understanding of both OSC's and the FBI's investigations. However, these documents raise additional questions about both investigations.

The FBI's production included early drafts of Director Comey's public statement, ultimately delivered on July 5, 2016, clearing Secretary Clinton of criminal wrongdoing in her use of a private email server.[2] On May 2, 2016, Director Comey emailed a draft statement to FBI Deputy Director Andrew McCabe, FBI General Counsel James Baker, and FBI Chief of Staff James Rybicki—a full two months before the FBI had completed over a dozen interviews, including its interview with Secretary Clinton.[3] The drafting of this statement began before the FBI immunized key witnesses to the investigation, including Cheryl Mills and Heather Samuelson.[4] The immunity agreements with Ms. Mills and Ms. Samuelson, executed on June

---

[1] Letter from Gregory A. Brower to Sen. Ron Johnson, Chairman, S. Comm. on Homeland Security and Governmental Affairs (Nov. 17, 2017).

[2] Documents FBI produced to the Committee on Nov. 17, 2017 marked SJC 000028-000271 [herein after "FBI documents"]. For clarity, I have attached the entire document containing track-changed edits to Director Comey's original draft July 5 statement. This document is marked SJC 000031-000037.

[3] FBI documents, *supra* note 2 at SJC 000140.; Letter from Sen. Charles Grassley, Chairman, S. Comm. on Judiciary, to Christopher Wray, Director, Federal Bureau of Investigation, Aug. 30, 2017. The FBI conducted an interview of Secretary Clinton on July 2, 2016.

[4] Comm. review of Justice Dep't immunity agreements with Cheryl Mills & Heather Samuelson, (Sept. 27, 2016).

10, 2016, also included side agreements requiring the FBI to destroy evidence on devices turned over to the FBI.[5]

According to documents produced by the FBI, FBI employees exchanged proposed edits to the draft statement. On May 6, Deputy Director McCabe forwarded the draft statement to other senior FBI employees, including Peter Strzok, E.W. Priestap, Jonathan Moffa, and an employee in the Office of General Counsel whose name has been redacted.[6] While the precise dates of the edits and identities of the editors are not apparent from the documents, the edits appear to change the tone and substance of Director Comey's statement in at least three respects.[7]

1. *Repeated edits to reduce Secretary Clinton's culpability in mishandling classified information*

The original draft of Director Comey's remarks included a statement that could be read as a finding of criminality in Secretary Clinton's handling of classified material:

> *There is evidence to support a conclusion that Secretary Clinton, and others, used the private email server in a manner that was grossly negligent with respect to the handling of classified information.*[8]

The edited statement deleted the reference to gross negligence—a legal threshold for mishandling classified material[9]—and instead replaced it with an exculpatory sentence:

> *Although we did not find clear evidence that Secretary Clinton or her colleagues intended to violate laws governing the handling of classified information, there is evidence that they were extremely careless in their handling of very sensitive, highly classified information.*[10]

This change appeared in the statement as Director Comey delivered it on July 5, 2016.[11]

Further, the original draft of Director Comey's statement connected the volume of classified material on Secretary Clinton's private server with a finding of criminality. It read:

---

[5] *Id.*; *see also FBI agreed to destroy laptops of Clinton aides with immunity deal, lawmaker says*, Fox News, Oct. 3, 2016.
[6] FBI documents, *supra* note 2 at SJC 000028-29.
[7] *Id.*
[8] FBI documents, *supra* note 2 at SJC 0000142.
[9] *See* 18 U.S.C. § 793.
[10] FBI documents, *supra* note 2 at SJC 000034
[11] *Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System*, July 5, 2016, *available at* https://www.fbi.gov/news/pressrel/press-releases/statement-by-fbi-director-james-b-comey-on-the-investigation-of-secretary-hillary-clinton2019s-use-of-a-personal-e-mail-system [hereinafter Comey July 5 statement].

> *Similarly, the sheer volume of information that was properly classified as Secret at the time it was discussed on email (that is, excluding the "up classified" emails) supports an inference that the participants were grossly negligent in their handling of that information.*[12]

This statement was edited to deemphasize the amount of classified information and, again, to remove a reference to gross negligence. The edited version read:

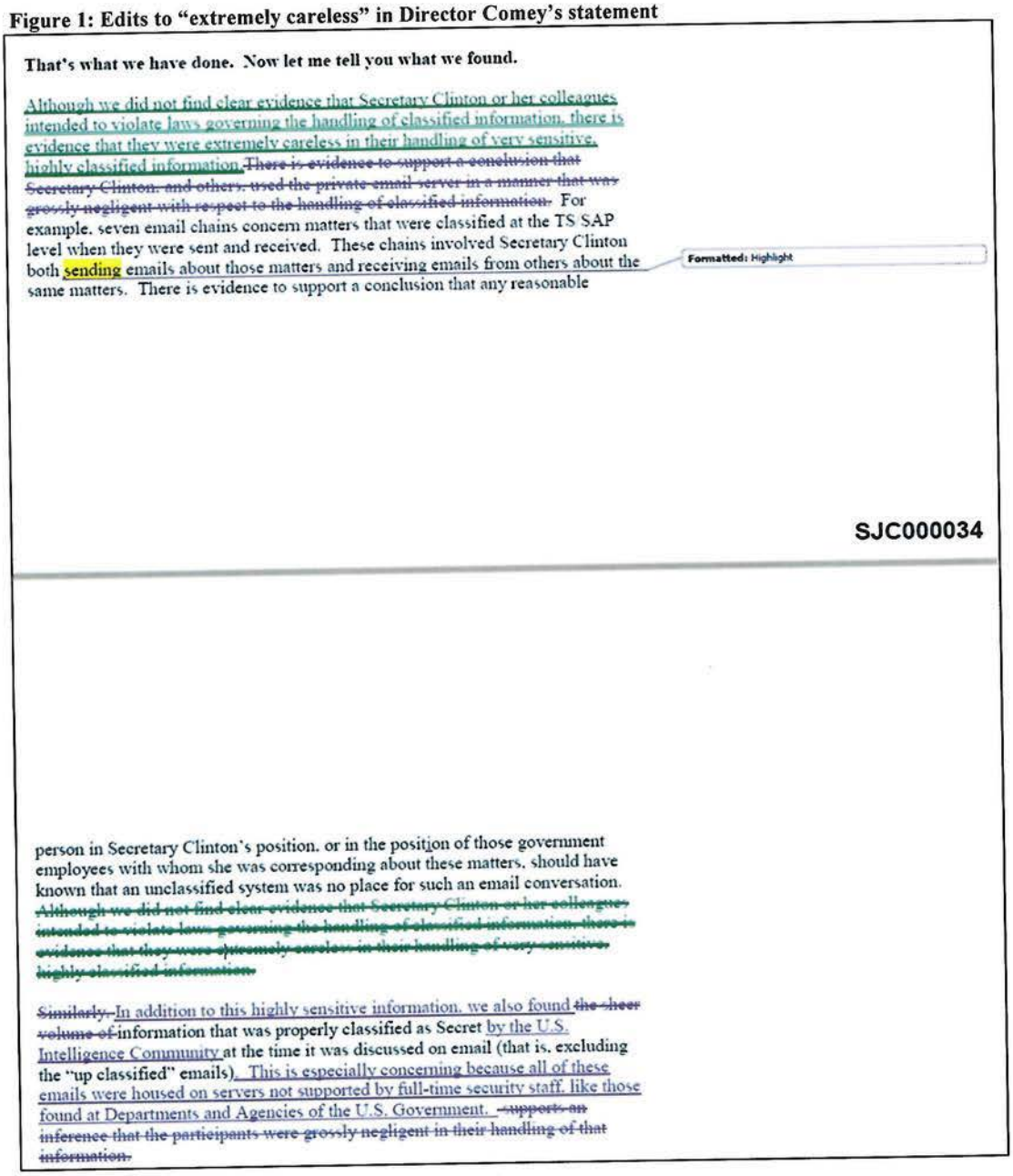
> *In addition to this highly sensitive information, we also found information that was properly classified as Secret by the U.S Intelligence Community at the time it was discussed on email (that is, excluding the 'up classified emails).*[13]

The edited version also contained a sentence that read, "This is especially concerning because all of these emails were housed on servers not supported by full-time security staff, like those found at the Departments and Agencies of the U.S. Government."[14] This sentence was not included in the statement as delivered by Director Comey on July 5.[15]

---

[12] FBI documents, *supra* note 2 at SJC 0000142
[13] FBI documents, *supra* note 2 at SJC 000035
[14] FBI documents, *supra* note 2 at SJC 000035.
[15] Comey July 5 statement, *supra* note 11.

Figure 1: Edits to "extremely careless" in Director Comey's statement



That's what we have done. Now let me tell you what we found.

Although we did not find clear evidence that Secretary Clinton or her colleagues intended to violate laws governing the handling of classified information, there is evidence that they were extremely careless in their handling of very sensitive, highly classified information. ~~There is evidence to support a conclusion that Secretary Clinton, and others, used the private email server in a manner that was grossly negligent with respect to the handling of classified information.~~ For example, seven email chains concern matters that were classified at the TS SAP level when they were sent and received. These chains involved Secretary Clinton both sending emails about those matters and receiving emails from others about the same matters. There is evidence to support a conclusion that any reasonable

Formatted: Highlight

SJC000034

person in Secretary Clinton's position, or in the position of those government employees with whom she was corresponding about these matters, should have known that an unclassified system was no place for such an email conversation. ~~Although we did not find clear evidence that Secretary Clinton or her colleagues intended to violate laws governing the handling of classified information, there is evidence that they were extremely careless in their handling of very sensitive, highly classified information.~~

~~Similarly,~~ In addition to this highly sensitive information, we also found ~~the sheer volume of~~ information that was properly classified as Secret by the U.S. Intelligence Community at the time it was discussed on email (that is, excluding the "up classified" emails). This is especially concerning because all of these emails were housed on servers not supported by full-time security staff, like those found at Departments and Agencies of the U.S. Government. ~~, supports an inference that the participants were grossly negligent in their handling of that information.~~

In addition, the original draft of Director Comey's statement stated that the FBI had found evidence of potential violations of the gross negligence statute and of the statute governing misdemeanor mishandling of classifed information:

> *Although there is evidence of potential violations of the statute proscribing gross negligence in the handling of classified information and of the statute proscribing misdemeanor hishandling, my judgment is that no reasonable prosecutor would bring such a case. At the outset, we are not aware of a case where anyone has been charged solely based on the "gross negligence" prohibition in the statute.*

> *In looking back at our investigations in similar circumstances, we cannot find a case that would support bringing criminal charges on these facts. All the cases prosecuted involved some combination of: (1) clearly intentional misconduct; (2) vast quantities of materials exposed in such a way as to support an inference of intentional misconduct; (3) indications of disloyalty to the United States; or (4) efforts to obstruct justice. We see none of that here.*[16]

The edited version removed Director Comey's specific reference to potential violations of the gross negligence and misdemeanor mishandling statutes. The edits changed the first sentence of the quoted text to read:

> *Although there is evidence of potential violations of the statutes regarding the handling of classified information, my judgment is that no reasonable prosecutor would bring such a case.*[17]

A comment bubble accompanying the edit, in which the editor wrote, "we changed none of this text, we simply reordered it. The original text is below, struck out."[18] The editor did not address the deletion of references in the original draft to evidence of potential violations of the gross negligence or misdemeanor statutes.

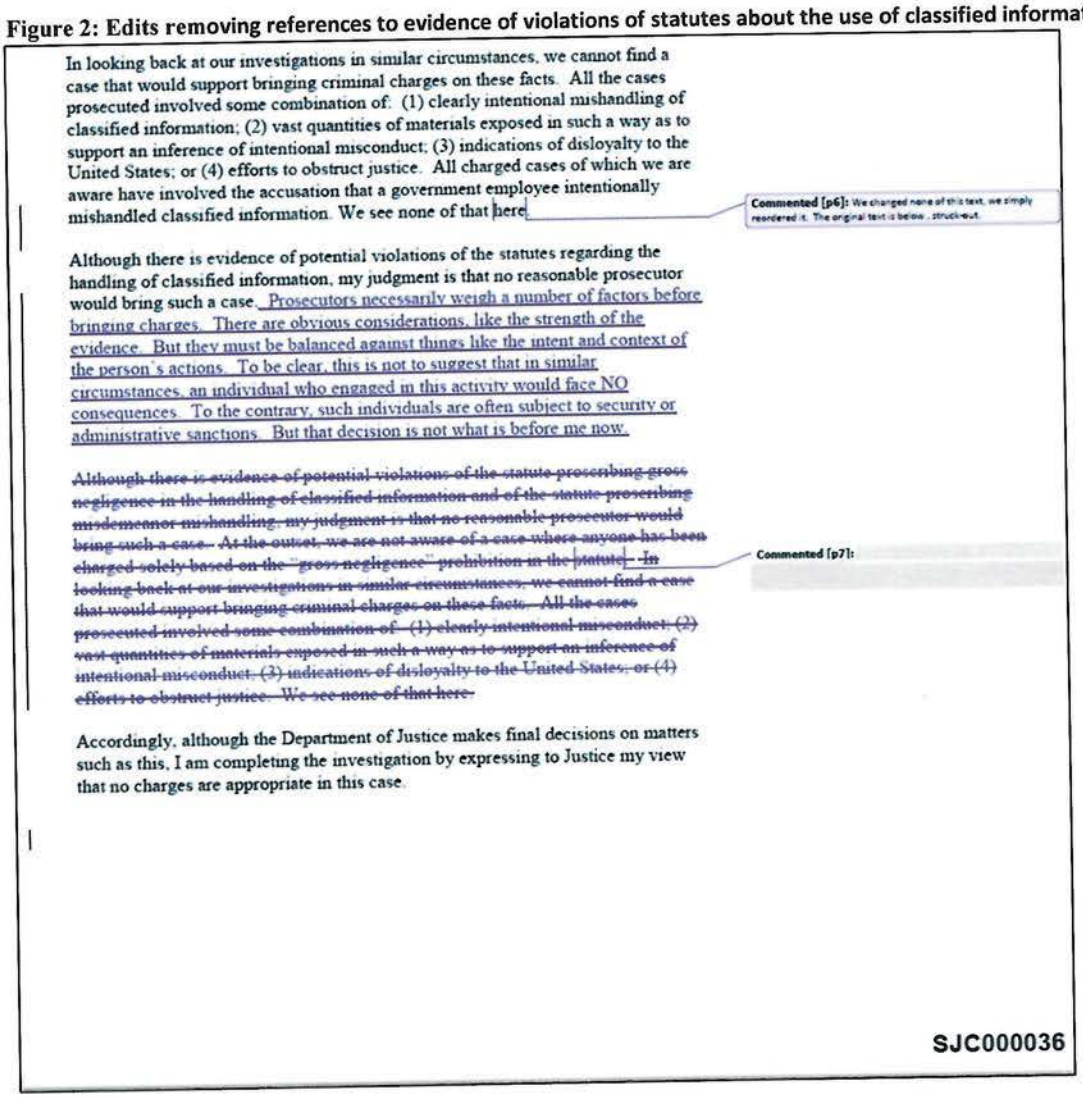
Director Comey's public remarks on July 5 lacked any specific reference to the FBI finding of evidence potential violations of the "gross negligence" and "misdemeanor mishandling" statutes. Instead, Director Comey stated:

> *Although there is evidence of potential violations of the statutes regarding the handling of classified information, our judgment is that no reasonable prosecutor would bring such a case. . . .*[19]

---

[16] FBI documents, *supra* note 2 at SJC 000036.
[17] FBI documents, *supra* note 2 at SJC 000036.
[18] FBI documents, *supra* note 2 at SJC 000036.
[19] Comey July 5 statement, *supra* note 11.

Figure 2: Edits removing references to evidence of violations of statutes about the use of classified information



In looking back at our investigations in similar circumstances, we cannot find a case that would support bringing criminal charges on these facts. All the cases prosecuted involved some combination of: (1) clearly intentional mishandling of classified information; (2) vast quantities of materials exposed in such a way as to support an inference of intentional misconduct; (3) indications of disloyalty to the United States; or (4) efforts to obstruct justice. All charged cases of which we are aware have involved the accusation that a government employee intentionally mishandled classified information. We see none of that here.

Commented [p6]: We changed none of this text, we simply reordered it. The original text is below, struck-out.

Although there is evidence of potential violations of the statutes regarding the handling of classified information, my judgment is that no reasonable prosecutor would bring such a case. Prosecutors necessarily weigh a number of factors before bringing charges. There are obvious considerations, like the strength of the evidence. But they must be balanced against things like the intent and context of the person's actions. To be clear, this is not to suggest that in similar circumstances, an individual who engaged in this activity would face NO consequences. To the contrary, such individuals are often subject to security or administrative sanctions. But that decision is not what is before me now.

~~Although there is evidence of potential violations of the statute prescribing gross negligence in the handling of classified information and of the statute prescribing misdemeanor mishandling, my judgment is that no reasonable prosecutor would bring such a case. At the outset, we are not aware of a case where anyone has been charged solely based on the "gross negligence" prohibition in the [statute]. In looking back at our investigations in similar circumstances, we cannot find a case that would support bringing criminal charges on these facts. All the cases prosecuted involved some combination of: (1) clearly intentional misconduct; (2) vast quantities of materials exposed in such a way as to support an inference of intentional misconduct; (3) indications of disloyalty to the United States; or (4) efforts to obstruct justice. We see none of that here.~~

Commented [p7]:

Accordingly, although the Department of Justice makes final decisions on matters such as this, I am completing the investigation by expressing to Justice my view that no charges are appropriate in this case.

SJC000036

2. *Edits to remove reference to the Intelligence Community's role in identifying vulnerabilities related to Secretary Clinton's private email server*

Director Comey's original statement acknowledged the FBI had worked with its partners in the Intelligence Community to assess potential damage from Secretary Clinton's use of a private email server. The original statement read:

> *[W]e have done extensive work with the assistance of our colleagues elsewhere in the Intelligence Community to understand what indications there might be of compromise by hostile actors in connection with the private email operation.*[20]

The edited version removed the reference to the intelligence community:

[20] FBI documents, *supra* note 2 at SJC 000142.

> *[W]e have done extensive work to understand what indications there might be of compromise by hostile actors in connection with the personal e-mail operation.*[21]

Director Comey delivered this edited statement in his July 5 remarks.[22] It is unclear why FBI staff removed the reference to working with the Intelligence Community during the editing process for Director Comey's statement.

3. *Edits to downgrade the likelihood that hostile actors had penetrated Secretary Clinton's private server*

Finally, the original draft of Director Comey's statement included a conclusion that it was "reasonably likely" that hostile actors had penetrated Secretary Clinton's private server. Director Comey's original statement read:

> *With respect to potential computer intrusion by hostile actors, we did not find direct evidence that Secretary Clinton's personal email system, in its various configurations since 2009, was successfully hacked. But, given the nature of the system and of the actors potentially involved, we assess that we would be unlikely to see such direct evidence. We do assess that hostile actors gained access to the private email accounts of individuals with whom Secretary Clinton was in regular contact from her private account. We also assess that Secretary Clinton's use of a private email domain was both known by a large number of people and readily apparent. Given the combination of factors, we assess it is reasonably likely that hostile actors gained access to Secretary Clinton's private email account.*[23]

This statement was edited to downgrade the assessment that it was "reasonably likely" that hostile actors had gained access to Secretary Clinton's private email account. Instead, the edited statement simply read it was "possible" that those events occurred—the formulation Director Comey ultimately used in his public statement on July 5.[24] Director Comey's July 5 statement ultimately read:

> *With respect to potential computer intrusion by hostile actors, we did not find direct evidence that Secretary Clinton's personal e-mail domain, in its various configurations since 2009, was successfully hacked. But, given the nature of the system and of the actors potentially involved, we assess that we would be unlikely to see such direct evidence. We do assess that hostile actors gained access to the private commercial e-mail accounts of people with whom Secretary Clinton was in regular contact from her personal account. We also assess that Secretary Clinton's use of a personal e-mail domain was both known by a large number of people and readily apparent. She also used her personal e-mail extensively while outside the United States, including sending and receiving work-related e-mails in*

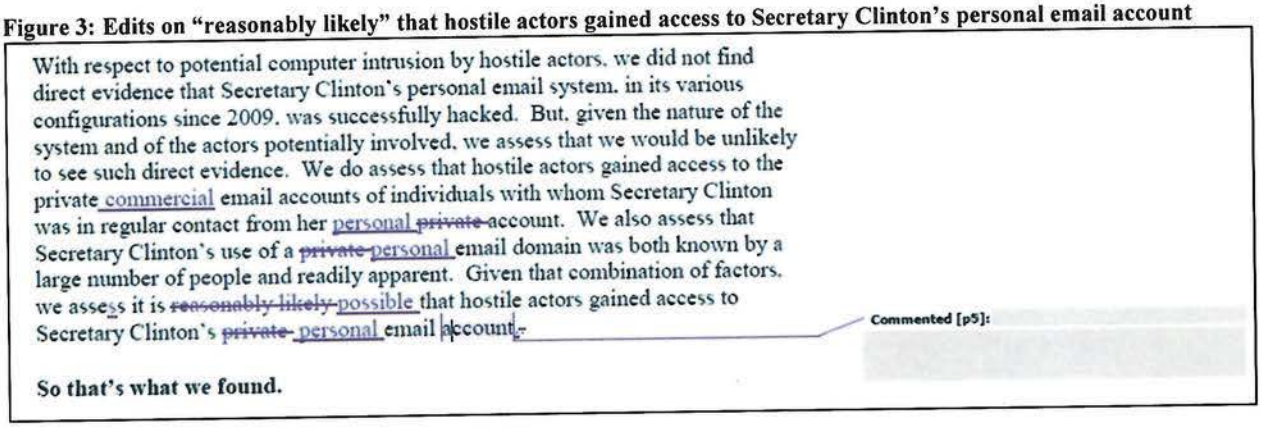
---

[21] FBI documents, *supra* note 2 at SJC 000034.
[22] Comey July 5 statement, *supra* note 11.
[23] FBI documents, *supra* note 2 at SJC 0000143.
[24] FBI documents, *supra* note 2 at SJC 000035.

> *the territory of sophisticated adversaries. Given that combination of factors, we assess it is possible that hostile actors gained access to Secretary Clinton's personal e-mail account.*[25]

The edited statement contains a comment bubble at the conclusion of the changed paragraph; however the FBI redacted the comment.[26]

Figure 3: Edits on "reasonably likely" that hostile actors gained access to Secretary Clinton's personal email account


With respect to potential computer intrusion by hostile actors, we did not find direct evidence that Secretary Clinton's personal email system, in its various configurations since 2009, was successfully hacked. But, given the nature of the system and of the actors potentially involved, we assess that we would be unlikely to see such direct evidence. We do assess that hostile actors gained access to the private commercial email accounts of individuals with whom Secretary Clinton was in regular contact from her personal ~~private~~ account. We also assess that Secretary Clinton's use of a ~~private~~ personal email domain was both known by a large number of people and readily apparent. Given that combination of factors, we asses it is ~~reasonably likely~~ possible that hostile actors gained access to Secretary Clinton's ~~private~~ personal email account.

Commented [p5]:

So that's what we found.

Although it is not readily apparent from the draft statement, media reports suggest that Mr. Strzok changed the language from "grossly negligent" to "extremely careless" in the draft statement.[27] Mr. Strzok also participated in the FBI's interview of Secretary Clinton on July 2, 2016.[28] Other documents produced by the Justice Department show during the FBI's investigation of Secretary Clinton, Mr. Strzok described then-candidate Trump as an "idiot" and that his candidacy would be "good for Hillary."[29] On March 4, 2016, he wrote that "Hillary should win 100,000,000-0" in a hypothetical election with Trump.[30] In addition, while exchanging text messages with Lisa Page in August 2016, Mr. Strzok wrote: "I want to believe the path you threw out to consideration in Andy's office—***that there's no way he gets elected—but I'm afraid we can't take that risk***. It's like an insurance policy in the unlikely event you die before you're 40 . . . ."[31]

---

[25] Comey July 5 statement, *supra* note 11.
[26] FBI documents, *supra* note 2 at SJC 000035.
[27] Laura Jarrett and Evan Perez, *FBI agent dismissed from Mueller probe changed Comey's description of Clinton to 'extremely careless'*, CNN, Dec. 4, 2017, http://www.cnn.com/2017/12/04/politics/peter-strzok-james-comey/index.html.
[28] Fed. Bureau of Investigation, 302 of FBI interview with Hillary Clinton, July 2, 2016, *available at* https://vault.fbi.gov/hillary-r.-clinton/Hillary%20R.%20Clinton%20Part%2002%20of%2016/view.
[29] Letter from Stephen E. Boyd, Ass't Attn'y Gen. for the Office of Legislative Affairs, U.S. Dep't of Justice, to Sen. Ron Johnson, Chairman, S. Comm. on Homeland Security and Governmental Affairs, Dec. 12, 2017. Mr. Boyd's letter was accompanied by a production of 375 text message communications between Mr. Strzok and Lisa Paige, another FBI employee dated August 16, 2015 to December 1, 2016 [herein after referred to as "text messages." Text messages at 8-9; text messages at 10.
[30] Text messages at 11
[31] Text messages at 43 (emphasis added).

In summary, the edits to Director Comey's public statement, made months prior to the conclusion of the FBI's investigation of Secretary Clinton's conduct, had a significant impact on the FBI's public evaluation of the implications of her actions. This effort, seen in light of the personal animus toward then-candidate Trump by senior FBI agents leading the Clinton investigation and their apparent desire to create an "insurance policy" against Mr. Trump's election, raise profound questions about the FBI's role and possible interference in the 2016 presidential election and the role of the same agents in Special Counsel Mueller's investigation of President Trump. Given these circumstances, the Committee has additional questions about the process by which the FBI edited Director Comey's public statement of July 5, 2016. I respectfully request the following information and material:

1. Please provide the names of the Department of Justice (DOJ) employees who comprised the "mid-year review team" during the FBI's investigation of Secretary Clinton's use of a private email server?

2. Please identify all FBI, DOJ, or other federal employees who edited or reviewed Director Comey's July 5, 2016 statement. Please identify which individual made the marked changes in the documents produced to the Committee.

3. Please identify which FBI employee repeatedly changed the language in the draft statement that described Secretary Clinton's behavior as "grossly negligent" to "extremely careless." What evidence supported these changes?

4. Please identify which FBI employee edited the draft statement to remove the reference to the Intelligence Community. On what basis was this change made?

5. Please identify which FBI employee edited the draft statement to downgrade the FBI's assessment that it was "reasonably likely" that hostile actors had gained access to Secretary Clinton's private email account to merely that than intrusion was "possible." What evidence supported these changes?

6. Please provide unredacted copies of the drafts of Director Comey's statement, including comment bubbles, and explain the basis for the redactions in the material produced to date.

Please provide this information as soon as possible but no later than 5:00 p.m. on December 28, 2017. Any classified information provided in response to this letter should be provided under separate cover through the Office of Senate Security.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of the Government,"[32] Additionally, S. Res. 62 (115th Congress) authorizes the Committee to examine "the efficiency and economy of all

[32] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).

branches of the Government including the possible existence of fraud, misfeasance, malfeasance, collusion, mismanagement, incompetence, corruption, or unethical practices . . . ."[33]

Thank you for your attention to this matter. If you have any questions about this request, please contact Kyle Brosnan or Brian Downey of the Committee staff at (202) 224-4751.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Claire McCaskill
Ranking Member

Enclosure

[33] S. Res. 62 § 12, 115th Cong. (2017).

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

January 20, 2018

The Honorable Christopher Wray
Director
Federal Bureau of Investigation
935 Pennsylvania Ave, NW
Washington, D.C. 20535

Dear Director Wray:

The Committee on Homeland Security and Governmental Affairs is continuing its oversight of the Federal Bureau of Investigation (FBI) and the FBI's investigation of classified information on former Secretary of State Hillary Clinton's private email server. I write to request information about the loss of FBI records connected to this investigation, and how the FBI oversees its employees' use of private email accounts for official business.

On January 19, 2018, the Department of Justice produced 384 pages of text messages exchanged between FBI employees Lisa Page and Peter Strzok.[1] According to a cover letter accompanying the documents, the FBI did not preserve text messages between Ms. Page and Mr. Strzok between approximately December 14, 2016 and May 17, 2017.[2] The cover letter explained:

> The Department wants to bring to your attention that the FBI's technical system for retaining text messages sent and received on FBI mobile devices failed to preserve text messages for Mr. Strzok and Ms. Page from December 14, 2016 to approximately to May 17, 2017. The FBI has informed [the Department of Justice] that many FBI-provided Samsung 5 mobile devices did not capture or store text messages due to misconfiguration issues related to rollouts, provisioning, and software upgrades that conflicted with the FBI's collection capabilities. The result was that data that should have been automatically collected and retained for long-term storage and retrieval was not collected.[3]

The loss of records from this period is concerning because it is apparent from other records that Mr. Strzok and Ms. Page communicated frequently about the investigation. In February 2016, Ms. Page texted Mr. Strzok that then-candidate Trump "simply can not [*sic*] be

---

[1] Letter from Stephen Boyd, Assistant Attorney Gen. for Legislative Affairs, Dep't of Justice, to Sen. Ron Johnson, Chairman, S. Comm. on Homeland Security and Gov't Affairs, Jan. 19, 2018. The letter also included 384 pages of text messages between Mr. Strzok and Ms. Page [herein after "Jan. 19 production."].

[2] *Id.*

[3] *Id.*

president."[4] On May 4, 2016—after then-Director Comey began drafting his July 5 statement clearing Secretary Clinton—Ms. Page and Mr. Strzok communicated about "pressure" building to finish the FBI's investigation following candidate Trump's likely nomination:

> **Ms. Page:** And holy shit Cruz just dropped out of the race. It's going to be a Clinton Trump race. Unbelievable.
>
> **Mr. Strzok:** What?!?!??
>
> **Ms. Page:** You heard it right my friend.
>
> **Mr. Strzok:** I saw trump [*sic*] won, figured it would be a bit
>
> **Mr. Strzok:** Now the pressure really starts to finish MYE....
>
> **Ms. Page:** It sure does. We need to talk about follow up call tomorrow. We still never have.[5]

The reference to the "MYE" by Mr. Strzok refers to the "midyear exam," the FBI's case name for the Clinton investigation.[6]

In addition, Mr. Strzok and Ms. Page discussed the drafting of Director Comey's July 5 statement exonerating Secretary Clinton. On June 30, 2016, FBI personnel circulated a draft of Director Comey's statement that noted that Secretary Clinton had emailed with President Obama from the private server while abroad in the "territory of sophisticated adversaries."[7] The passage read:

> We also assess that Secretary Clinton's use of a personal email domain was both known by a large number of people and readily apparent. She also used her personal email extensively while outside the United States, including from the territory of sophisticated adversaries. **That use included an email exchange with the President while Secretary Clinton was on the territory of such an adversary.** Given that combination of factors, we assess it is possible that hostile actors gained access to Secretary Clinton's personal email account.[8]

The same afternoon, after FBI officials edited the draft to replace "the President" with "another senior government official,"[9] Mr. Strzok sent a text message to Ms. Page notifying her of the change. The exchange read:

---

[4] Jan. 19 production at 58.
[5] Jan. 19 production at 114.
[6] Olivia Beavers, *Comey began drafting Clinton statement months in advance*, The Hill, Oct. 16, 2017.
[7] Documents FBI produced to the Committee on Nov. 17, 2017 marked SJC 000028-000271 [herein after "FBI documents"].
[8] FBI documents at SJC 000064
[9] FBI documents at SJC 000078

Mr. Strzok: K. Rybicki just sent another version.

Ms. Page: Bill just popped his head in, hopefully to talk to him.

Mr. Strzok: Hope so. Just left Bill. Talked about the speech, the [redacted] stuff relating to the case, and what I told you about earlier.

Mr. Strzok: He changed President to "another senior government official."[10]

Director Comey's statement as ultimately delivered on July 5 omitted a reference to either President Obama or "another senior government official."[11]

The conversations between Ms. Page and Mr. Strzok also appear to suggest that then-Attorney General Lynch was aware that Director Comey would not recommend criminal charges in the Clinton investigation prior to Attorney General Lynch's announcement that she would accept whatever recommendation the FBI made.[12] On July 1, 2016—the same day as Attorney General Lynch's announcement, but before the FBI had interviewed Secretary Clinton and before Director Comey had announced his recommendation—Ms. Page and Mr. Strzok exchanged the following messages:

Mr. Strzok: Holy cow....nyt breaking Apuzzo, Lync [*sic*] will accept whatever rec D[13] and career prosecutors make. No political appointee input.

Mr. Strzok: Lynch. Timing not great, but whatever. Wonder if that's why the no coordination language added.

Ms. Page: No way. This is a purposeful leak following the airplane snafu.

Mr. Strzok: Timing looks like hell. Will appear to be choreographed. All major news networks literally leading with "AG to accept FBI D's recommendation."

---

[10] Jan. 19 production at 166.

[11] *Statement by FBI Director James B. Comey on the Investigation of Secretary Hillary Clinton's Use of a Personal E-Mail System*, July 5, 2016, *available at* https://www.fbi.gov/news/pressrel/press-releases/statement-by-fbi-director-james-b-comey-on-the-investigation-of-secretary-hillary-clinton2019s-use-of-a-personal-e-mail-system Director Comey's July 5 statement read: "We do assess that hostile actors gained access to the private commercial e-mail accounts of people with whom Secretary Clinton was in regular contact from her personal account. We also assess that Secretary Clinton's use of a personal e-mail domain was both known by a large number of people and readily apparent. She also used her personal e-mail extensively while outside the United States, including sending and receiving work-related e-mails in the territory of sophisticated adversaries. Given that combination of factors, we assess it is possible that hostile actors gained access to Secretary Clinton's personal e-mail account."

[12] Mark Landler, Matt Apuzzo, and Amy Chozick, *Loretta Lynch to Accept F.B.I. Recommendations in Clinton Email Inquiry,* NY TIMES, July 1, 2016, https://www.nytimes.com/2016/07/02/us/politics/loretta-lynch-hillary-clinton-email-server.html?mtrref=www.google.com&gwh=63C838733CD90850AA3927C0C6A1982D&gwt=pay.

[13] "D" refers to former FBI Director James Comey

Ms. Page: Yeah, that is awful timing. Nothing we can do about it.

Mr. Strzok: What I meant was, did DOJ tell us yesterday they were doing this, so D added that language.

Mr. Strzok: Yep. I told Bill the same thing. Delaying just makes it worse.

Ms. Page: And yes. I think we had some warning of it. I know they sent some statement to rybicki, bc he called andy.

Ms. Page: **And yeah, it's a real profile in couragw [*sic*], since she knows no charges will be brought.**[14]

In addition, the text messages appear to suggest that Ms. Page and Mr. Strzok used non-FBI-issued devices to discuss FBI business. For example, in April 2016, Ms. Page texted Mr. Strzok, "so look, you say we text on that phone when we talk about hillary [sic.] because it can't be traced, you were just venting [because] you feel bad that you're gone so much but it can't be helped right now."[15] Mr. Strzok replied, "Right. But did you say anything other than work? I did, [redacted]."[16] In addition, Ms. Page and Mr. Strzok reference several times about emailing each other on Gmail.[17]

Under federal law, the head of each federal agency is required to preserve all records documenting the decision-making process and essential transactions of the agency.[18] In light of the Department of Justice's notification that FBI records from the Clinton investigation are missing, and as the Senate committee with jurisdiction over federal records, I ask that you please produce the following information and material:

1. Please explain the scope and scale of all records lost, destroyed, or otherwise alienated during the midyear examination investigation.

2. Does the FBI have any records of communications between Ms. Page and Mr. Strzok between December 14, 2016 and May 17, 2017? If so, please provide those communications.

3. Has the FBI conducted searches of Mr. Strzok and Ms. Page's non-FBI-issued communication devices or accounts to determine whether federal records exist on those

---

[14] Jan. 19 production at 167.
[15] Jan. 19 production at 94.
[16] *Id.*
[17] *See, e.g.* November 10, 2016 text from Ms. Page: "Hey without thinking I replied to the email you sent me on Gmail. But it went to your Verizon. So please clear. Let me know if you want me to send it again somewhere else." Jan. 19 production at 321; *see also* October 4, 2015 text from Mr. Strzok: "It's going to be ok at work. And haven't emailed you here, although I just did on gmail." Jan. 19 production at 18.
[18] 44 U.S.C. § 3101.

nonofficial accounts? Please explain how the FBI is complying with federal records requirements with respect to these devices.

4. Has the FBI produced text messages to the Department of Justice Office of Inspector General (DOJ OIG) of any other FBI employees in furtherance of the DOJ OIG's review of the Clinton email investigation? If so, please identify which FBI employees' communications were produced.

5. Has the FBI produced Microsoft Lync conversations between Ms. Page and Mr. Strzok to the DOJ OIG? Please explain.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of the Government,"[19] Additionally, S. Res. 62 (115th Congress) authorizes the Committee to examine "the efficiency and economy of all branches of the Government including the possible existence of fraud, misfeasance, malfeasance, collusion, mismanagement, incompetence, corruption, or unethical practices . . . ."[20]

Thank you for your attention to this matter. If you have any questions about this request, please contact Kyle Brosnan or Brian Downey of the Committee staff at (202) 224-4751.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Claire McCaskill
Ranking Member

Enclosure

[19] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[20] S. Res. 62 § 12, 115th Cong. (2017).

United States Senate
WASHINGTON, DC 20510

January 23, 2018

The Honorable Michael E. Horowitz
Inspector General
U.S. Department of Justice
950 Pennsylvania Avenue, N.W.
Washington, D.C. 20530-0001

Dear Inspector General Horowitz:

The Committee on Homeland Security and Governmental Affairs and the Committee on the Judiciary are conducting oversight of the Federal Bureau of Investigation (FBI) and the FBI's investigation of classified information on former Secretary of State Hillary Clinton's private email server. We write to request information about the loss of FBI records connected to this investigation.

On January 12, 2017, the Department of Justice Office of Inspector General (DOJ OIG) announced an investigation of "allegations that Department or FBI policies or procedures were not followed in connection with, or in actions leading up to or related to, the FBI Director's public announcement on July 5, 2016, and the Director's letters to Congress on October 28 and November 6, 2016 and that certain underlying investigative decisions were based on improper considerations."[1]

On December 6, 2017, we wrote to you concerning the DOJ OIG discovery of text messages between FBI employees Lisa Page and Peter Strzok.[2] Your response, dated December 13, 2017, suggested that DOJ OIG received all text messages between Ms. Page and Mr. Strzok from November 30, 2016 to July 28, 2017. You wrote:

> In gathering evidence for the OIG's ongoing 2016 election review, we requested, consistent with standard practice, that the FBI produce text messages from the FBI-issued phones of certain FBI employees involved in the Clinton email investigation based on search terms we provided. After finding a number of politically-oriented text messages between Page and Strzok, the OIG sought from the FBI all text messages between Strzok and Page from their FBI-issued phones through November 30, 2016, which covered the entire period of the Clinton e-mail server investigation. The FBI produced these text messages on July 20, 2017. Following our review of those text messages, **the OIG expanded our request to the FBI to include all text messages between Strzok and Page from November 30, 2016, through the date of the document request, which was**

[1] DOJ OIG Announces Initiation of Review, Jan. 12, 2017, available at https://oig.justice.gov/press/2017/2017-01-12.pdf.

[2] Letter from Sen. Ron Johnson, Chairman, S. Comm. on Homeland Security and Gov't Affairs, and Sen. Charles Grassley, Chairman, S. Comm. on Judiciary, to Michael E. Horowitz, Inspector Gen., Dep't of Justice (Dec. 6, 2017).

> **July 28, 2017. The OIG received these additional messages on August 10, 2017.**[3]

On January 19, 2018, the Department of Justice produced to Congress 384 pages of text messages exchanged between Ms. Page and Mr. Strzok.[4] According to a cover letter accompanying the documents, the FBI did not preserve text messages between Ms. Page and Mr. Strzok between approximately December 14, 2016 and May 17, 2017.[5] The cover letter explained:

> **The Department wants to bring to your attention that the FBI's technical system for retaining text messages sent and received on FBI mobile devices failed to preserve text messages for Mr. Strzok and Ms. Page from December 14, 2016 to approximately to May 17, 2017.** The FBI has informed [the Department of Justice] that many FBI-provided Samsung 5 mobile devices did not capture or store text messages due to misconfiguration issues related to rollouts, provisioning, and software upgrades that conflicted with the FBI's collection capabilities. The result was that data that should have been automatically collected and retained for long-term storage and retrieval was not collected.[6]

These statements—that DOJ OIG requested "all text messages between Strzok and Page from November 30, 2016, [to] July 28, 2017,"[7] received them on August 10, 2017, and that the FBI "failed to preserve text messages from Mr. Strzok and Ms. Page from December 14, 2016, to approximately May 17, 2017"[8]—need to be reconciled. During a phone call on January 22, 2018, DOJ OIG staff indicated that the FBI did not produce text messages between Mr. Strzok and Ms. Page from December 14, 2016, to May 17, 2017.[9]

Accordingly, to understand fully the scope of text messages in the possession of the DOJ OIG, we respectfully request that you please provide the following information and material:

1. Is it accurate that the FBI failed to provide to DOJ OIG text messages between Mr. Strzok and Ms. Page from December 14, 2016, to May 17, 2017 due to technical errors that prevented the texts from being archived in the FBI's records preservation system?

---

[3] Letter from Michael E. Horowitz, Inspector Gen., Dep't of Justice, to Sen. Ron Johnson, Chairman S. Comm. on Homeland Security and Gov't Affairs, and Sen. Charles Grassley, Chairman, S. Comm. on Judiciary (Dec. 13, 2017).
[4] Letter from Stephen Boyd, Assistant Attorney Gen. for Legislative Affairs, Dep't of Justice, to Sen. Ron Johnson, Chairman, S. Comm. on Homeland Security and Gov't Affairs (Jan. 19, 2018). The letter also included 384 pages of text messages between Mr. Strzok and Ms. Page.
[5] *Id.*
[6] *Id.*
[7] Letter from Michael E. Horowitz, *supra* note 3.
[8] Letter from Stephen Boyd, *supra* note 4.
[9] Phone call with Dep't of Justice Off. of Inspector Gen. staff (Jan. 22, 2018).

a. Has the FBI also been unable to provide the texts from any other source, such as the physical phones, carrier records, or any other source?

b. Has the OIG requested texts of other FBI personnel during the same time period? If so, has the FBI also been unable to produce texts of others as well or is the missing text problem limited to these two employees?

c. On what date did the OIG request access to messages for that time period from the FBI?

d. Did the FBI notify the OIG of the missing text messages between Mr. Strzok and Ms. Page? If so, on what date? If not, how and on what date did the OIG discover that messages were missing?

e. Did the DOJ OIG notify the office of the Deputy Attorney General of the missing text messages between Mr. Strzok and Ms. Page? If so, on what date?

f. Please explain why the DOJ OIG did not notify Congress of the missing text messages.

2. Please produce all communications between DOJ OIG, DOJ, and the FBI referring or relating to the missing text messages.

3. The Attorney General said in a statement yesterday that your office was already undertaking a review of the circumstances that led to the FBI's failure to preserve and provide texts to the OIG. On what date did that review begin, and what is the scope and methodology of that OIG review?

4. Has the DOJ OIG been successful in retrieving any of the missing text messages from any other source?

5. Does the OIG have the necessary authorities, resources, and capabilities to obtain the missing texts from another source? If not, please identify any gaps in your office's ability to do so.

6. In the most recent batch of texts, Mr. Strzok and Ms. Page frequently indicate that they are also communicating about work-related matters via apparently personal accounts on Apple's encrypted iMessage texting system, as well as through Gmail. Does the OIG have the necessary authorities, resources, and capabilities to obtain any federal records that may reside in those personal accounts? If not, please explain any gaps in your ability to do so.

7. Has the OIG asked Mr. Strzok or Ms. Page to voluntarily provide any information from their personal accounts? If so, have they been cooperative? If the OIG has not asked, please explain why not.

8. Has the DOJ OIG interviewed Mr. Strzok or Ms. Page?

9. Has the DOJ OIG interviewed employees of the FBI's Information Technology office regarding the loss of text messages?

Please respond to this letter as soon as possible but no later than January 29, 2018.

Thank you for your attention to this matter. If you have any questions about this request, please contact Kyle Brosnan or Brian Downey of the Senate Homeland Security and Governmental Affairs Committee staff at (202) 224-4751 or Josh Flynn-Brown of the Senate Judiciary Committee staff at (202) 224-5225.

Sincerely,

Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs

Charles E. Grassley
Chairman
Committee on the Judiciary

cc: The Honorable Claire McCaskill
Ranking Member
Committee on Homeland Security and Governmental Affairs

The Honorable Dianne Feinstein
Ranking Member
Committee on the Judiciary

United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

January 31, 2018

The Honorable Rod J. Rosenstein
Acting Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530

Dear Acting Attorney General Rosenstein:

The Committee on Homeland Security and Governmental Affairs is continuing its oversight of the Federal Bureau of Investigation (FBI) and the FBI's investigation of classified information on former Secretary of State Hillary Clinton's private email server. On January 19, 2018, the Department of Justice (DOJ) produced to the Committee 384 pages of text messages exchanged between FBI officials Lisa Page and Peter Strzok.[1] I write to request additional information about FBI records connected to this investigation.

According to DOJ's cover letter accompanying the documents, the FBI failed to preserve text messages between Ms. Page and Mr. Strzok between approximately December 14, 2016, and May 17, 2017.[2] The Department later reported that phones of nearly ten percent of the FBI's 35,000 employees experienced similar issues.[3] On January 25, 2018, the Department of Justice Office of Inspector General (OIG) notified the Committee that it had "succeeded in using forensic tools to recover" the lost text messages exchanged between Mr. Strzok and Ms. Page, and that the OIG would provide the messages to the Department.[4] The OIG noted it had no objection to the Department providing the recovered messages to Congress.[5]

According to text messages produced to the Committee, Ms. Page and Mr. Strzok make references to communicating with other FBI employees via text message, phone call, email, and voice mail.[6] Additional text messages suggest that FBI officials used non-official email accounts

---

[1] Letter from Stephen Boyd, Assistant Attorney Gen. for Legislative Affairs, Dep't of Justice, to Sen. Ron Johnson, Chairman, S. Comm. on Homeland Security and Gov't Affairs, Jan. 19, 2018. The letter also included 384 pages of text messages between Mr. Strzok and Ms. Page.

[2] *Id.*

[3] Jake Gibson, *Thousands of FBI cellphones affected by glitch that lost Strzok-Page texts, officials say*, Fox News, Jan. 24, 2018, http://www.foxnews.com/politics/2018/01/24/thousands-fbi-cellphones-affected-by-glitch-that-lost-strzok-page-texts-officials-say.html.

[4] Letter from Michael E. Horowitz, Inspector Gen., Dep't of Justice, to Sen. Ron Johnson, Chairman, S. Comm. on Homeland Security and Gov't Affairs, and Sen. Charles Grassley, Chairman, S. Comm. on Judiciary, Jan. 25, 2018.

[5] *Id.*

[6] *See* Text messages between Peter Strzok and Lisa Page (June 10, 2016) ("Okay, let me text andy."). [DOJ-PROD-148]; text messages between Peter Strzok and Lisa Page (May 15, 2016) ("[Redacted] just texted. Dd flying with the DAG on the bird. So he'll be back for mye.") [DOJ-PROD-129]; text messages between Peter Strzok and Lisa Page (Jan. 28, 2016) ("And Andy just texted me the following...") [DOJ-PROD-50]; text message from Lisa Page to

and messaging programs to communicate about official business. For example, Ms. Page and Mr. Strzok wrote on April 10, 2016:

Mr. Strzok: [Redacted] I find I'm increasingly profoundly bothered by JBs[7] [*sic*] call and the lack of ANY heads up. Deeply. It was wrong given what I had already been asked to do. Gonna sleep on it and see where I am in the morning.

Mr. Strzok: Because you know where I was on Thursday or Friday night – when I was complaining about everyone expecting me to deliver the hard message while they vacillated in discussing with their counterparts. About how my sense of justness and character was at odds with waiting until Sat to say something. And rightfully, you point out stop being so prima donna-ish and just do it. And I do. And then I find out an hour later that in addition to what I was asked to do, JB went to counsel and had the discussion he did. And I'm the one facing the music. From some who I have known for a long time. Nobody else pays the price. Nobody else will have the same straight hard discussion. Yet, I'm the only one who violated his sense of integrity to swallow hard and deliver the message.

Mr. Strzok: I'm not sure if I want to be part of this

Ms. Page: You are part of this and that's not going to change. But I think you have every right to be angry and frustrated about bring left out of the loop on your investigation, especially when you're going to be left holding the bag. And I think you're entitled to say something to Baker about that, though on this one I would probably discuss with Bill first.

Ms. Page: I'm sorry [redacted]. Big big case, big big problems. But God knows you're still the right guy to do it.

Mr. Strzok: ***Gmailed you two drafts of what I'm thinking of sending Bill, would appreciate your thoughts. Second (more recent) is updated so you can skip the first.*** [8]

Peter Strzok (Apr. 20, 2016) ("Hey check your vm before you talk to your MYE team. Jim spoke to beth this am, nfi.") [DOJ-PROD-105]; text message from Peter Strzok to Lisa Page (Sept. 26, 2016) ("Randy called him after he couldn't reach Toscas. So now Laufman is calling him all the time.") [DOJ-PROD-14]; text message from Peter Strzok to Lisa Page (June 30, 2016) ("Also just emailed JR asking if D might want to call US Atty at some point.") [DOJ-PROD-166].

[7] "JB" likely refers to then-FBI General Counsel James Baker.

[8] [DOJ-PROD-102]; *see also* text message from Lisa Page to Peter Strzok (Nov. 10, 2016) ("Hey without thinking I replied to the email you sent me on Gmail. . . .") [DOJ-PROD-321]; text from Peter Strzok to Lisa Page (Sept. 15, 2015) ("Also, Bill did not tell Andy about the loss. Background reasons why, which make sense. I can fill you in

While it is unclear exactly what Mr. Strzok and Ms. Page were discussing in this exchange, Mr. Strzok appears to be expressing his frustrations with an investigation. On April 10, 2016, *Fox News* aired an interview with President Obama—taped earlier in the week in Chicago—in which President Obama noted that he "continued to believe that [Secretary Clinton] has not jeopardized America's national security."[9] According to an early draft of Director Comey's exoneration statement, Secretary Clinton emailed with President Obama while in the "territory of sophisticated adversary."[10] Notes from the FBI's interview with Secretary Clinton confirm that she emailed President Obama from Russia.[11] Although it is unclear whether Mr. Strzok's frustration was related to the President's comments, the timing of the communication raises questions about the FBI's handling of the Clinton email server investigation.

Questions also remain about the preservation of FBI records in this matter. In one series of text messages produced to the Committee, Mr. Strzok and Ms. Page hint at broader record-retention issues with the FBI's Samsung mobile devices and that FBI employees sought to procure iPhones for their use. Specifically, Ms. Page and Mr. Strzok wrote in August 2016:

Ms. Page: Have a meeting with turgal[12] about getting iphone in a day or so

Mr. Strzok: Oh hot damn. I'm happy to pilot that . . . We get around our security/monitoring issues?

Ms. Page: No, he's proposing that we just stop following them. Apparently the requirement to capture texts came from omb, but we're the only org (I'm told) who is following that rule. His point is, if no one else is doing it why should we.

Ms. Page: Helps that Dd[13] had a terrible time with his phone [redacted] which made him concerned for our folks all over the place.

Ms. Page: These phones suck as much as they do because of the program we use to capture texts, full stop.

---

on imessage later if you want."). [DOJ-PROD-258]; text message from Lisa Page to Peter Strzok (June 7, 2016) ("Think I'm going to pull up eras in about 15, so we can always text there. . . .") [DOJ-PROD-144]; Text message from Peter Strzok to Lisa Page (Dec. 13, 2016) ("Text from reporter: retrieving my password for skype. I forgot it. Text from reporter an hour and 31 minutes later: thanks man. Awesome as usual.") [DOJ-PROD-338].

[9] *Exclusive: President Barack Obama on 'Fox News Sunday,'* Fox News, Apr. 10, 2016. The interview occurred at the University of Chicago Law School. *Id.* According to the President's daily schedule, he was at the University of Chicago Law School on Thursday, April 7, 2016. *See* White House, What's Happening, April 7, 2016 Schedule, https://obamawhitehouse.archives.gov/blog?page=28#.

[10] *See* FBI Documents at SJC 000064.

[11] FBI Records: The Vault, *Hillary R. Clinton*, FD-302a(Rev. 10-6-95) Part 2 at 2, https://vault.fbi.gov/hillary-r.-clinton/Hillary%20R.%20Clinton%20Part%2002%20of%2017/view.

[12] "[T]urgal" likely refers to Executive Assistant Director for the Information and Technology Branch James Turgal. *See, e.g.*, Press Release,*FBI Announces Executive Appointments*, Feb. 11, 2016, https://www.fbi.gov/news/pressrel/press-releases/fbi-announces-executive-appointments-2.

[13] "Dd" likely refers to FBI Deputy Director Andrew McCabe.

Mr. Strzok: No doubt.

Mr. Strzok: I'm not convinced short of OPR, that text capture capability really deters anything.

Mr. Strzok: If I want to copy/take classified, I'm sure as hell not going to do it on this phone.

Ms. Page: I thought it was more from a discovery perspective.

Mr. Strzok: Probably. So just make a rule no texts of a discoverable nature. Like you said, what are CBP, DEA, others doing?

Ms. Page: I'm told – thought I have seen – that there is an IG report that says everyone is failing. But one has changed anything, so why not just join in the failure.[14]

The Justice Department Inspector General has requested "that the FBI produce text messages from the FBI-issued phones of certain FBI employees involved in the Clinton e-mail investigation . . . ."[15] On January 29, 2017 FBI Deputy Director Andrew McCabe reportedly resigned following "a private meeting with FBI Director Christopher A. Wray during which Wray expressed concern about the findings of an investigation by the Justice Department's Inspector General."[16]

Accordingly, I respectfully request that the Department produce all text messages newly recovered sent or received by Peter Strzok and Lisa Page for the period December 14, 2016, to May 17, 2017. In addition, to ensure the Committee has a complete understanding of the FBI's investigation, I respectfully request the following information and material:

1. Please produce all documents and communications, including but not limited to emails, memoranda, notes, text messages, iPhone instant messages, and voicemails, for the period January 1, 2015, to the present referring or relating to the FBI's Midyear Exam investigation, the presence of classified information on Secretary of State Clinton's private email server, or candidates for the 2016 presidential election for the following custodians:

---

[14] Text messages between Lisa Page and Peter Strzok (Aug. 30, 2016) [DOJ-PROD-231-232].
[15] Letter from Michael E. Horowitz, Inspector Gen., Dep't of Justice, to Sen. Ron Johnson, Chairman, S. Comm. on Homeland Security and Gov't Affairs, and Sen. Charles Grassley, Chairman, S. Comm. on Judiciary, Jan. 25, 2018.
[16] *Devlin Barrett and Matt Zapotosky*, FBI's Andrew McCabe leaving deputy director job amid internal investigation. WASH POST, Jan. 29, 2018, https://www.washingtonpost.com/world/national-security/fbis-andrew-mccabe-leaving-deputy-director-job-will-retire-in-march/2018/01/29/35b1bbd4-051c-11e8-b48c-b07fea957bd5_story.html?hpid=hp_rhp-top-table-main_mccabe-112pm%3Ahomepage%2Fstory&utm_term=.cb2738fa2278.

a. James Comey;
b. James Rybicki;
c. Andrew McCabe;
d. John Giaclone
e. James Turgal;
f. David Bowdich;
g. Jonathan Moffa;
h. Peter Strzok;
i. Lisa Page;
j. Trisha Anderson;
k. E.W. Priestap;
l. George Toscas;
m. Randy Coleman;
n. Brian Brooks;
o. Michael Kortan; and
p. James Baker.

2. Please explain whether any of the individuals identified in question 1 have been affected by the apparent Samsung device software glitch that lost the text messages[17] of Mr. Strzok and Ms. Page.

3. Please provide the calendars of the individuals named in question 1 from January 1, 2015 to the present.

4. Please explain how and when the Department of Justice became aware that the FBI failed to retain communications of FBI employees between approximately December 14, 2016 and May 17, 2017.

5. Has the FBI experienced similar failures to retain communications on other employee issued-devices?

6. Did the FBI issue iPhones for any individual on the midyear exam team? Please explain.

7. Please provide the email(s) Secretary Clinton sent President Obama while she was located in the "territory of a sophisticated adversary."

Please provide this information as soon as possible but no later than February 14, 2018. Please provide an unclassified response to the greatest extent possible. If a full response requires the production of classified information, please provide this material under separate cover via the Office of Senate Security.

[17] Letter from Stephen Boyd, Assistant Attorney Gen. for Legislative Affairs, Dep't of Justice, to Sen. Ron Johnson, Chairman, S. Comm. on Homeland Security and Gov't Affairs, Jan. 19, 2018.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of the Government,"[18] Additionally, S. Res. 62 (115th Congress) authorizes the Committee to examine "the efficiency and economy of all branches of the Government including the possible existence of fraud, misfeasance, malfeasance, collusion, mismanagement, incompetence, corruption, or unethical practices . . . ."[19]

Thank you for your attention to this matter. If you have any questions about this request, please contact Kyle Brosnan or Brian Downey of the Committee staff at (202) 224-4751.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Claire McCaskill
Ranking Member

Enclosure

[18] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[19] S. Res. 62 § 12, 115th Cong. (2017).

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

October 28, 2016

Honorable Richard M. Burr
Chairman
Select Committee on Intelligence

Honorable Devin Nunes
Chairman
Permanent Select Committee on Intelligence

Honorable Charles E. Grassley
Chairman
Committee on the Judiciary

Honorable Robert Goodlatte
Chairman
Committee on the Judiciary

Honorable Richard Shelby
Chairman
Committee on Appropriations
Subcommittee on Commerce, Justice, Science and Related Agencies

Honorable John Culberson
Chairman
Committee on Appropriations
Subcommittee on Commerce, Justice, Science and Related Agencies

Honorable Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs

Honorable Jason Chaffetz
Chairman
Committee on Oversight and Government Reform

Dear Messrs Chairmen:

In previous congressional testimony, I referred to the fact that the Federal Bureau of Investigation (FBI) had completed its investigation of former Secretary Clinton's personal email server. Due to recent developments, I am writing to supplement my previous testimony.

In connection with an unrelated case, the FBI has learned of the existence of emails that appear to be pertinent to the investigation. I am writing to inform you that the investigative team briefed me on this yesterday, and I agreed that the FBI should take appropriate investigative steps designed to allow investigators to review these emails to determine whether they contain classified information, as well as to assess their importance to our investigation.

Although the FBI cannot yet assess whether or not this material may be significant, and I cannot predict how long it will take us to complete this additional work, I believe it is important to update your Committees about our efforts in light of my previous testimony.

Sincerely yours,

James B. Comey
Director

1 – Honorable Dianne Feinstein
Vice Chairman
Select Committee on Intelligence
United States Senate
Washington, DC 20510

1 – Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary
United States Senate
Washington, DC 20510

1 – Honorable Barbara Mikulski
Ranking Member
Committee on Appropriations
Subcommittee on Commerce, Justice, Science
and Related Agencies
United States Senate
Washington, DC 20510

1 – Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, DC 20510

1 – Honorable Adam B. Schiff
Ranking Member
Permanent Select Committee on Intelligence
U.S. House of Representatives
Washington, DC 20515

1 – Honorable John Conyers, Jr.
Ranking Member
Committee on the Judiciary
U.S. House of Representatives
Washington, DC 20515

1 – Honorable Michael Honda
Ranking Member
Committee on Appropriations
Subcommittee on Commerce, Justice, Science
and Related Agencies
U.S. House of Representatives
Washington, DC 20515

1 – Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and
Government Reform
U.S. House of Representatives
Washington, DC 20515

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535

November 6, 2016

Honorable Richard M. Burr
Chairman
Select Committee on Intelligence

Honorable Devin Nunes
Chairman
Permanent Select Committee on Intelligence

Honorable Charles E. Grassley
Chairman
Committee on the Judiciary

Honorable Robert Goodlatte
Chairman
Committee on the Judiciary

Honorable Richard Shelby
Chairman
Committee on Appropriations
Subcommittee on Commerce, Justice,
Science and Related Agencies

Honorable John Culberson
Chairman
Committee on Appropriations
Subcommittee on Commerce, Justice,
Science and Related Agencies

Honorable Ron Johnson
Chairman
Committee on Homeland Security and
Governmental Affairs

Honorable Jason Chaffetz
Chairman
Committee on Oversight and
Government Reform

Dear Messrs. Chairmen:

I write to supplement my October 28, 2016 letter that notified you the FBI would be taking additional investigative steps with respect to former Secretary of State Clinton's use of a personal email server. Since my letter, the FBI investigative team has been working around the clock to process and review a large volume of emails from a device obtained in connection with an unrelated criminal investigation. During that process, we reviewed all of the communications that were to or from Hillary Clinton while she was Secretary of State.

Based on our review, we have not changed our conclusions that we expressed in July with respect to Secretary Clinton.

I am very grateful to the professionals at the FBI for doing an extraordinary amount of high-quality work in a short period of time.

Sincerely yours,

James B. Comey
Director

cc: See next page

1 – Honorable Dianne Feinstein
Vice Chairman
Select Committee on Intelligence

1 – Honorable Patrick J. Leahy
Ranking Member
Committee on the Judiciary

1 – Honorable Barbara Mikulski
Ranking Member
Committee on Appropriations
Subcommittee on Commerce, Justice,
Science and Related Agencies

1 – Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security and
Governmental Affairs

1 – Honorable Adam B. Schiff
Ranking Member
Permanent Select Committee on Intelligence

1 – Honorable John Conyers, Jr.
Ranking Member
Committee on the Judiciary

1 – Honorable Michael Honda
Ranking Member
Committee on Appropriations
Subcommittee on Commerce, Justice,
Science, and Related Agencies

1 – Honorable Elijah E. Cummings
Ranking Member
Committee on Oversight and
Government Reform

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, D.C. 20530*

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, DC 20510

DEC 1 2 2017

Dear Chairman Johnson,

This responds to the Committee's request that the Department of Justice (Department) provide the Committee with copies of text message communications between Federal Bureau of Investigation (FBI) employees Peter Strzok and Lisa Page. We are sending letters and identical enclosures to a number of Congressional Committees that have made similar requests.

As you may know, on January 12, 2016, the Department of Justice's Office of Inspector General (OIG) publicly announced that the OIG would review "allegations that Department or FBI policies or procedures were not followed in connection with, or in actions leading up to or related to, the FBI Director's public announcement on July 5, 2016,[1] and the Director's letters to Congress on October 28 and November 6, 2016, and that certain underlying investigative decisions were based on improper considerations.[2]" As part of that review, the OIG obtained, among other things, text messages between Mr. Strzok and Ms. Page.

The Department expected the documents provided herein to be provided as part of a completed OIG report. However, public reporting about the existence of the text messages prompted Congressional Committee requests for the text messages. Please find enclosed an initial disclosure of approximately 375 text message communications, dated August 16, 2015 to December 1, 2016, that have been identified as pertinent to the OIG review referenced above. The enclosed documents contain minimal redactions that protect the privacy interests of third parties and sensitive law enforcement information, and remove irrelevant information. The Department continues to review documents and will provide pertinent documents as they become available.

---

[1] On that date, then-FBI Director James B. Comey announced that the FBI was recommending to the Department of Justice that no charges should be filed relating to former Secretary of State Hillary Clinton's use of a private email server.

[2] DOJ OIG Announces Initiation of Review, January 12, 2017, available at: https://oig.justice.gov/press/2017/2017-01-12.pdf

As has been publicly reported, Mr. Strzok previously served on the investigative team led by Special Counsel Robert Mueller. The OIG informed the Special Counsel of the existence of the enclosed text messages on or about July 27, 2017. Mr. Mueller immediately concluded that Mr. Strzok could no longer participate in the investigation, and he was removed from the team.

This extraordinary accommodation of providing the enclosed documents is unique to the facts and circumstances of this particular matter. The Department appreciates the work of the OIG on this matter, looks forward to the findings and recommendations arising from that review, and will take appropriate action as warranted.

Sincerely,

Stephen E. Boyd
Assistant Attorney General

cc: The Honorable Claire McCaskill
Ranking Member

Enclosures

U.S. Department of Justice

Office of the Inspector General

December 13, 2017

The Honorable Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs
340 Dirksen Senate Office Building
United States Senate
Washington, DC 20510

The Honorable Charles E. Grassley
Chairman
Committee on the Judiciary
224 Dirksen Senate Office Building
United States Senate
Washington, DC 20515

Dear Chairmen Johnson and Grassley:

Thank you for your letter of December 6, 2017, requesting information regarding the Office of the Inspector General's discovery of certain electronic text messages in connection with its review of the actions of the Department of Justice and the Federal Bureau of Investigation (FBI) in advance of the 2016 presidential election. Our responses to the questions presented in your letter are set forth below.

1. When and how did OIG become aware of the text messages between Peter Strzok and Lisa Page?

In gathering evidence for the OIG's ongoing 2016 election review, we requested, consistent with standard practice, that the FBI produce text messages from the FBI-issued phones of certain FBI employees involved in the Clinton e-mail investigation based on search terms we provided. After finding a number of politically-oriented text messages between Page and Strzok, the OIG sought from the FBI all text messages between Strzok and Page from their FBI-issued phones through November 30, 2016, which covered the entire period of the Clinton e-mail server investigation. The FBI produced these text messages on July 20, 2017. Following our review of those text messages, the OIG expanded our request to the FBI to include all text messages between Strzok and Page from

November 30, 2016, through the date of the document request, which was July 28, 2017. The OIG received these additional messages on August 10, 2017.

2. When and how did OIG notify the Special Counsel Robert Mueller of the text messages?

On July 27, 2017, upon our identification of many of the political text messages, the Inspector General met with the Deputy Attorney General and the Special Counsel to inform them of the texts that we had discovered, and provided them with a significant number of the texts, so that they could take any management action they deemed appropriate.

3. Did OIG refer these allegations to the U.S. Office of Special Counsel to pursue a potential Hatch Act inquiry? If not, why not?

The Hatch Act, and its associated regulations, identify authorized and prohibited political activities for most executive department employees, including FBI employees. The Hatch Act permits expressions of personal opinions about candidates and issues. In contrast, political activity, which is defined as "activity directed toward the success or failure of a political party, candidate for partisan political office, or partisan political group" is prohibited in certain contexts. We are cognizant of these issues and will determine whether there is a basis to refer the allegations, along with relevant evidence we have gathered, regarding Page's and Strzok's text messages to the Office of Special Counsel upon completion of our review.

4. In connection with the OIG's review of the actions of DOJ and the FBI in advance of the 2016 presidential election, has the OIG received any similar allegations involving other government officials?

The OIG's review is ongoing, and we currently are in the process of completing our witness interviews and document review. Thereafter, we intend to issue a public report with our findings on these and the other issues we are reviewing, and we would be pleased to discuss them with you at that time.

Thank you for your continued support for the work of my Office. If you

have any questions, please do not hesitate contact me or Greg Sabina, my Advisor for Legislative Affairs, at (202) 514-3435.

Sincerely,

Michael E. Horowitz
Inspector General

cc: The Honorable Claire McCaskill
Ranking Member, Committee on Homeland Security and Governmental Affairs
United States Senate

The Honorable Dianne Feinstein
Ranking Member, Committee on the Judiciary
United States Senate

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535-0001

December 28, 2017

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

I am writing in response to your letter to Director Wray dated December 13, 2017, concerning the Office of Special Counsel's ("OSC") now closed investigation of former FBI Director James Comey.

The following information is responsive to the three enumerated requests on page 3 of your letter. First, the recusal in question was of the FBI's Office of the General Counsel ("OGC"), and was based upon the possibility of an apparent or actual conflict of interest resulting from certain OGC attorneys' participation in meetings and decisions pertinent to the underlying subject matter of the OSC investigation. (However, some personnel within the OGC were excluded from the recusal.) Second, the Executive Office for U.S. Attorneys ("EOUSA") was involved in the FBI's cooperation with the OSC investigation because the above-referenced recusal caused the Office of the Deputy Attorney General ("ODAG") to authorize and direct the General Counsel's Office of EOUSA to assume responsibility for coordinating the FBI's cooperation with the OSC investigation. ODAG chose the General Counsel's Office of EOUSA for this task because that office had the requisite resources and experience to effectively engage with OSC. OGC personnel who were excluded from the recusal assisted EOUSA personnel in engaging with OSC. Third, these same personnel from both EOUSA and FBI OGC were involved in the conception, drafting, and execution of the non-disclosure agreements with OSC.

As for your letter's request that the FBI authorize OSC to produce unredacted copies of the previously produced materials, please note that the FBI has already released to the Committee, all of the records produced by the FBI to OSC, with only minimal redactions for privacy, security, attorney-client communications, non-relevant information, and information deemed to be law enforcement sensitive. Limited law enforcement sensitive information was either withheld or redacted because of the need to protect prosecutorial decision-making and the integrity of future cases.

Finally, we are also in receipt of your letter dated December 14, 2017, and are working to gather the information you have requested. We hope to be able to provide a substantive response very shortly.

I hope you find this information useful. Please do not hesitate to contact this office if we may provide additional assistance.

Sincerely,

Gregory A. Brower
Assistant Director
Office of Congressional Affairs

1 - The Honorable Claire McCaskill
Ranking Member
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, DC 20510

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, D.C. 20530*

JAN 05 2018

The Honorable Ron Johnson
Chairman
Committee on Homeland Security
And Governmental Affairs
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

This further responds to your letter to the Deputy Attorney General dated December 6, 2017, pertaining to the public reports of text messages exchanged between Federal Bureau of Investigation employees Peter Strzok and Lisa Page. On December 12, 2017, the Department delivered to the Committee text messages responsive to your request. In the transmittal letter, the Department confirmed that review of the text messages is ongoing and committed to providing additional relevant text messages in the future.

The Office of the Inspector General (OIG) informed the Office of the Deputy Attorney General (ODAG) and the Special Counsel of the existence of the previously provided text messages on or about July 27, 2017. Mr. Mueller immediately concluded that Mr. Strzok could no longer participate in the investigation, and he was removed from the team. The Department continues to review the text messages and will evaluate whether Mr. Strzok sent or received similar text messages pertaining to any other investigation during the relevant time period. The Department's OIG and Office of Professional Responsibility investigate non-frivolous allegations of misconduct, and neither of them has brought to the attention of the Department's leadership any allegations regarding similar conduct.

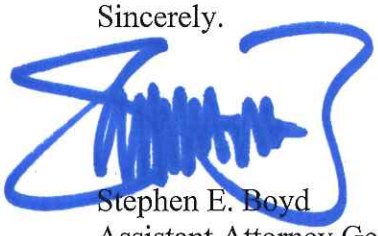
As the Inspector General noted to you in his letter of December 13, 2017, he has not made a referral to the Office of Special Counsel (OSC). In January 2017, the OIG initiated a "review of allegations regarding certain actions by the Department of Justice (Department) and the Federal Bureau of Investigation (FBI) in advance of the 2016 election."[1] As he noted in his letter to you, he will make a determination whether to refer the matter to OSC upon completion of that review. The Department will consider the OIG's findings in making its own determination about a possible referral to OSC. Consistent with statutory requirements, the

[1]DOJ OIG Announces Initiation of Review, January 12, 2017, available at: https://oig.justice.gov/press/2017/2017-01-12.pdf

Department would certainly cooperate with any independent review undertaken by OSC with respect to this matter.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

Sincerely.



Stephen E. Boyd
Assistant Attorney General

cc: The Honorable Claire McCaskill
Ranking Member

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, D.C. 20530*

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and Governmental Affairs
United States Senate
Washington, DC 20510

JAN 19 2018

Dear Chairman Johnson:

This responds to your request to the Department of Justice (Department) to provide the Committee with copies of text message communications between Federal Bureau of Investigation (FBI) employees Peter Strzok and Lisa Page.

As you may know, on January 12, 2016, the Department's Office of Inspector General (OIG) publicly announced that the OIG would review "allegations that Department or FBI policies or procedures were not followed in connection with, or in actions leading up to or related to, the FBI Director's public announcement on July 5, 2016,[1] and the Director's letters to Congress on October 28 and November 6, 2016, and that certain underlying investigative decisions were based on improper considerations.[2]" As part of that review, the OIG obtained, among other things, text messages between Mr. Strzok and Ms. Page.

In December 2017, we provided you with an initial production of approximately 375 text message communications, dated August 16, 2015 to December 1, 2016. In response to the requests for the texts messages, the Department collected all text messages between Mr. Strzok and Ms. Page available from the FBI for the period July 1, 2015 to July 28, 2017,[3] which was the same period requested by the OIG. The Department began reviewing those documents in an effort to provide you those messages that were either work-related or that provided any insight into the political views of the participants.

---

[1] On that date, then-FBI Director James B. Comey announced that the FBI was recommending to the Department of Justice that no charges should be filed relating to former Secretary of State Hillary Clinton's use of a private email server.

[2] DOJ OIG Announces Initiation of Review, January 12, 2017, available at: https://oig.justice.gov/press/2017/2017-01-12.pdf

[3] Although the request included texts through July 28, 2017, there were no text messages between Mr. Strzok and Ms. Page after July 1, 2017, and the messages after June 25, 2017, were personal in nature.

The Department is not providing text messages that were purely personal in nature. Furthermore, the Department has redacted from some work-related text messages portions that were purely personal. The Department's aim in withholding purely personal text messages and redacting personal portions of work-related text messages was primarily to facilitate the Committee's access to potentially relevant text messages without having to cull through large quantities of material unrelated to either the investigation of former Secretary of State Hillary Clinton's use of a personal email server or the investigation into Russian efforts to interfere with the 2016 Presidential election. Also, the withholding of personal information in some instances avoids unnecessary embarrassment or harassment to third parties that could result from public release of such information. The Department redacted the names of employees who are not SES-level employees, and in some instances, redacted SES employees' names to avoid unwarranted attention to those individuals when comments were gratuitous and did not provide relevant information to ongoing Congressional inquiries.

In a few instances, the Department has redacted portions of work-related texts that concern other investigations. Finally, the Department consulted with the Special Counsel's Office (SCO) and made some redactions related to the structure, operation, and substance of the SCO investigation because it is ongoing.

To avoid any concern that the Department has withheld relevant information, if a Committee has specific questions about why a particular text was partially redacted or about the nature of personal text messages withheld, the Department will work with that Committee to either further describe or disclose redacted information in a closed setting. Although the original spreadsheet contained only what the Department believed to be work-related text messages, subsequent reviews identified some additional personal text messages within that document. Therefore, the document produced today contains a small number of fully redacted messages that were determined to be personal messages subsequent to their initial inclusion in the previously provided spreadsheet. The enclosed document also excludes columns of information that contained only technical information such as phone numbers or email addresses in an effort to provide a more readily reviewable set of documents. In the attached, the "Inbox" documents are from Mr. Strzok to Ms. Page, and the "Outbox" documents are from Ms. Page to Mr. Strzok.

The Department wants to bring to your attention that the FBI's technical system for retaining text messages sent and received on FBI mobile devices failed to preserve text messages for Mr. Strzok and Ms. Page from December 14, 2016 to approximately to May 17, 2017. The FBI has informed us that many FBI-provided Samsung 5 mobile devices did not capture or store text messages due to misconfiguration issues related to rollouts, provisioning, and software upgrades that conflicted with the FBI's collection capabilities. The result was that data that should have been automatically collected and retained for long-term storage and retrieval was not collected. This problem should have been corrected with the rollout of the Samsung 7s in 2017.

Mr. Strzok's Samsung 5 phone last connected to the storage system on June 18, 2016. He received his new Samsung 7 phone on or about July 5, 2017. Ms. Page's Samsung 5 phone last connected to the storage system on December 13, 2016. She received her new Samsung 7 phone on or about May 22, 2017.[4]

The Office of Inspector General pieced together the text messages between Mr. Strzok and Ms. Page from June 18, 2016, to December 13, 2016, using the data from Ms. Page's phone until the connection to the storage system stopped on December 13, 2016. On May 17, 2017, Ms. Page's data collection re-initiated when she received her new phone.

Please let this office know if you have any questions regarding this production.

Very truly yours,

Stephen E. Boyd
Assistant Attorney General

cc: The Honorable Claire McCaskill
Ranking Member

Enclosure

[4] Although FBI identified May 22, 2017 as the issued date for Ms. Page's phone, collection resumed on May 18, 2017. The FBI has not yet been able to account for this discrepancy.

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535-0001

January 22, 2018

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, DC 20510

Dear Chairman Johnson:

I am writing in response to your letter dated December 14, 2017, in which you raise several questions concerning the FBI's recent investigation of Secretary Clinton's use of a private email server. The following information is responsive to the six enumerated requests on page 9 of your letter.

In response to requests 1 and 2, the SES-level members of the "mid-year review team" who were involved in reviewing and recommending edits to former Director Comey's July 5, 2016 statement included the following individuals: James Rybicki, Andrew McCabe, David Bowdich, Michael Steinbach, E.W. Priestap, Peter Strzok, Jonathan Moffa, James Baker, and Trisha Anderson. In addition to these individuals, three non-SES level FBI attorneys were involved in the process of reviewing and recommending edits to the former Director's statement.

With respect to the specific edits referenced in requests 3, 4, and 5 on page 9 of your letter, these edits were recommended by members of the mid-year team identified in the paragraph above based on the team's assessment of the case. While members of the team recommended certain edits to the statement, the ultimate decision making authority with respect to the content of the statement rested with former Director Comey.

Finally, the redactions made to the drafts of Director Comey's statements produced to date were based upon attorney-client communications, and information deemed to be law enforcement sensitive. Law enforcement sensitive information was either withheld or

redacted because of the need to protect prosecutorial decision-making and the integrity of future cases.

Thank you for your continued support of the FBI, its mission, and its people.

Sincerely,

Gregory A. Brower
Assistant Director
Office of Congressional Affairs

cc: The Honorable Claire McCaskill
Ranking Member
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, DC 20510

U.S. Department of Justice

Office of the Inspector General

January 25, 2018

The Honorable Ron Johnson
Chairman
Committee on Homeland Security
and Governmental Affairs
340 Dirksen Senate Office Building
United States Senate
Washington, DC 20510

The Honorable Charles E. Grassley
Chairman
Committee on the Judiciary
224 Dirksen Senate Office Building
United States Senate
Washington, DC 20510

Dear Chairmen Johnson and Grassley:

Thank you for your letter dated January 23, 2018, in which you requested information regarding the Federal Bureau of Investigation's (FBI) preservation of text messages for FBI employees Lisa Page and Peter Strzok. You requested a response by January 29, 2018.

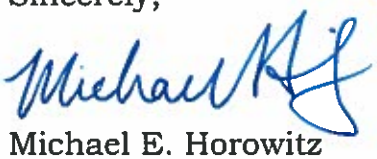
I understand that in its letter to you dated January 19, 2018, the Department of Justice (Department) reported that the FBI's technical system for retaining text messages sent from or to FBI-issued mobile devices failed to capture text messages between Ms. Page and Mr. Strzok during the period from December 14, 2016, to May 17, 2017. The Office of the Inspector General (OIG) had similarly been advised by the FBI that this failure prevented the FBI from producing to the OIG text messages between Ms. Page and Mr. Strzok during the period from December 14, 2016, to May 17, 2017.

The OIG has been investigating this matter and, this week, succeeded in using forensic tools to recover text messages from FBI devices, including text messages between Mr. Strzok and Ms. Page that were sent or received between December 14, 2016, and May 17, 2017. Our effort to recover any additional text messages is ongoing. We will provide copies of the text messages that we recover from these devices to the Department so that the Department's leadership can take any management action it deems appropriate. Proceeding in this manner is consistent with the OIG's process for handling Department information. As I have noted with respect to other Department information produced to the OIG

by the Department as part of our review, I would have no objection to the Department providing its own records to your Committees in response to a Congressional oversight request should Department leadership deem it appropriate to do so, and consistent with applicable law and Department policy.

I hope this information is helpful to the Committees and that it serves to clarify my letter to you dated December 13, 2017. Consistent with the OIG's practice, I look forward to providing the Department, Congress, and the public with a report detailing our findings, which will be responsive to additional questions in your letter, as soon as our work has been completed. We also would be pleased to discuss with your Committees whether the OIG has the necessary authorities, resources, and capabilities to obtain this type of evidentiary information.

Sincerely,



Michael E. Horowitz
Inspector General

cc: The Honorable Claire McCaskill
Ranking Member, Committee on Homeland Security and Governmental Affairs

The Honorable Dianne Feinstein
Ranking Member, Committee on the Judiciary

The Honorable Trey Gowdy
Chairman, Committee on Oversight and Government Reform

The Honorable Elijah Cummings
Ranking Member, Committee on Oversight and Government Reform

The Honorable Bob Goodlatte
Chairman, Committee on the Judiciary

The Honorable Jerrold Nadler
Ranking Member, Committee on the Judiciary

The Honorable Richard Shelby
Chairman, Subcommittee on Commerce, Justice, Science, and Related Agencies
Committee on Appropriations

The Honorable Jeanne Shaheen
Ranking Member, Subcommittee on Commerce, Justice, Science,
and Related Agencies
Committee on Appropriations

The Honorable John Culberson
Chairman, Subcommittee on Commerce, Justice, Science,
and Related Agencies
Committee on Appropriations

The Honorable José Serrano
Ranking Member, Subcommittee on Commerce, Justice, Science,
and Related Agencies
Committee on Appropriations

The Honorable Rod J. Rosenstein
Deputy Attorney General

The Honorable Christopher A. Wray
Director, Federal Bureau of Investigation

U.S. Department of Justice

Federal Bureau of Investigation

Washington, D.C. 20535-0001

February 2, 2018

The Honorable Ron Johnson
Chairman
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

Thank you for your letter dated January 20, 2018, and your staff's follow-up emails on January 22nd and 24th.

As explained in Assistant Attorney General Stephen Boyd's letter dated January 19, 2018, the FBI's mobile logging software is designed to collect text messages sent and received on FBI mobile devices, which are retained for audit purposes. This software apparently experienced a partial failure that contributed to some number of text messages not being collected and retained from various devices. This failure affected up to twenty percent of FBI mobile devices over a period of time. As further explained in a letter from the DOJ Office of Inspector General ("OIG") dated January 25, 2018, the OIG has apparently succeeded in using forensic tools to recover some number of text messages from FBI devices, including text messages between Mr. Strzok and Ms. Page that were sent or received between December 14, 2016, and May 17, 2017.

Please keep in mind that the mere fact that the text messages were to be collected by this technical process is not an indication that the messages constituted records under the Federal Records Act. The texts are collected for audit purposes, and the FBI does not apply a separate retention policy specific to text messages. However, employees are required to adhere to the record keeping policies in place if any of these text messages are deemed records. The FBI has not conducted searches of non-FBI mobile devices or accounts that may belong to Ms. Page or Mr. Strzok.

The FBI does have copies of electronic communications consisting of emails, Lync instant messages, and mobile text messages between Ms. Page and Mr. Strzok which were sent and received on FBI devices. These communications were produced to the OIG and we will process and produce these communications to you on a rolling basis. The FBI has also produced text messages of additional employees to the OIG. However, pending further review of these messages, we cannot provide a comprehensive list of these employees.

The Honorable Ron Johnson

In response to your other specific requests, the following information is provided. Between December 2016 and June 2017, [redacted] was the carrier for FBI-issued mobile devices assigned to Mr. Strzok and Ms. Page, respectively. The FBI considers the numbers associated with specific FBI phones to be law enforcement sensitive and, for that reason, they are not released publicly. The email addresses for Ms. Page and Mr. Strzok that would have been used on the FBI's unclassified systems are [redacted] and [redacted]. These email addresses, although unclassified, are also generally considered law enforcement sensitive. We are providing them to you with the understanding that they will be kept in the strictest confidence, treated as law enforcement sensitive, and not released publicly. The FBI cannot confirm Ms. Page's or Mr. Strzok's personal email address(es).

Finally, pursuant to long-standing DOJ and FBI practice, to protect their privacy, safety, and security the FBI cannot identify the three non-SES attorneys who participated in the editing of former Director Comey's July 5, 2016, statement.

We hope this answers your inquiries and thank you for your continued support of the FBI, its mission, and its people.

Sincerely,

Gregory A. Brower
Assistant Director
Office of Congressional Affairs

1 - The Honorable Claire McCaskill
Ranking Member
Committee on Homeland Security and
Governmental Affairs
United States Senate
Washington, DC 20510