

Congress of the United States
House of Representatives

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515-6143

MAJORITY (202) 225-5074

MINORITY (202) 225-5051

<http://oversight.house.gov>

November 2, 2016

The Honorable David S. Ferriero
Archivist of the United States
National Archives and Records Administration
8601 Adelphi Road
College Park, MD 20740

Dear Mr. Ferriero:

On July 5, 2016, the Director of the Federal Bureau of Investigation announced the completion of the Bureau's criminal investigation into former Secretary of State Hillary Clinton's use of an unclassified personal email server to conduct official business, including to send and receive "very sensitive, highly classified" national security information.¹ The FBI's investigation identified approximately 193 individual emails with information classified as Confidential, Secret, or Top Secret at the time they were sent, as well as an additional 2,000 emails containing information subsequently classified as Confidential.² Although the FBI last week informed this Committee that it was examining new pertinent emails, and thus reopening its criminal investigation,³ I am writing to request information regarding the government's security investigation of Secretary Clinton and other State Department staff who improperly transmitted classified national security information on an unsecure system.

Protection of classified information from unauthorized disclosure is essential to the protection of our national security and one of the most important responsibilities of any individual with a security clearance. All classified national security information is information which, by definition, if released to someone without an appropriate clearance and a need to know, could reasonably be expected to cause damage to the national security.⁴ The levels of collateral classification are distinguished by the degree of damage expected—the loss of Secret information is expected to cause "grave damage to the national security" and the loss of Top Secret information is expected to cause "exceptionally grave damage to the national security."⁵

¹ James Comey, Dir., Fed. Bureau of Investigation, Statement on the Investigation of Secretary Hillary Clinton's Use of a Personal E-mail System (July 5, 2016) (prepared remarks).

² FED. BUREAU OF INVESTIGATION, LETTERHEAD MEMORANDUM: CLINTON E-MAIL INVESTIGATION 20 (July 2016).

³ Letter from James Comey, Dir., Fed. Bureau of Investigation, to Jason Chaffetz, et al., Chairman, H. Comm. on Oversight & Gov't Reform (Oct. 28, 2016).

⁴ Exec. Order No. 13,526 at § 1.2, 3 C.F.R. § 707 (2009).

⁵ *Id.*

The FBI identified seven email chains that contained information classified at the Top Secret, Special Access Program level at the time they were sent,⁶ perhaps the most sensitive and restrictive category of classified national security information. As representatives for the Central Intelligence Agency (CIA) and National Security Agency (NSA) testified in a hearing before this Committee, losing Special Access Program information could have severe consequences for the United States and those who serve our country by revealing and endangering human sources abroad and jeopardizing critical means of monitoring our adversaries' communications.⁷ Betraying just how sensitive some of these emails are, the Inspector General for the Intelligence Community, who is charged with overseeing many of the classified programs at the CIA and NSA, testified that some of the programs in Secretary Clinton's emails were so highly classified that neither he nor anyone on his staff were even cleared to access them.⁸ Instead, the investigators had to request special access to the programs.⁹

The federal government requires such extraordinary protections for classified information precisely because of the consequences if it falls into the wrong hands. Those protections include storage of classified national security information on information systems, which must be specially designed, configured, and operated to ensure classified information does not move from a classified system to an unclassified system.¹⁰ Classified information systems are logically and physically separated from unclassified information systems for just that purpose. They must also be formally authorized before being connected with other classified information systems or processing classified information, and they must undergo rigorous security assessments.¹¹

Secretary Clinton's emails were not stored on a secure system, let alone a system authorized for classified information. When asked what was protecting Secretary Clinton's email servers, Director Comey told the Committee: "Well, not much."¹² Director Comey also acknowledged that Secretary Clinton's storage of classified information on her personal email server "ma[de] America's secrets vulnerable to hostile elements."¹³ The Director went on to explain that even a commercial email service like Gmail, or the official but unclassified email servers at the Department of State, were more secure than Secretary Clinton's servers.¹⁴ Just two

⁶ FED. BUREAU OF INVESTIGATION, LETTERHEAD MEMORANDUM: CLINTON E-MAIL INVESTIGATION 20 (July 2016).

⁷ *Classifications and Redactions in FBI's Investigative File: Hearing before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Sept. 12, 2016).

⁸ *Oversight of the State Department: Hearing before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (July 7, 2016).

⁹ *Id.*

¹⁰ See generally OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ICD 503, INTELLIGENCE COMMUNITY INFORMATION TECHNOLOGY SYSTEMS SECURITY RISK MANAGEMENT (2015); CMTE. ON NAT'L SEC. SYSTEMS, CNSS DIRECTIVE NO. 502, NATIONAL DIRECTIVE ON SECURITY OF NATIONAL SECURITY SYSTEMS (2004).

¹¹ OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, ICD 503, INTELLIGENCE COMMUNITY INFORMATION TECHNOLOGY SYSTEMS SECURITY RISK MANAGEMENT (2015); CMTE. ON NAT'L SEC. SYSTEMS, CNSS DIRECTIVE NO. 502, NATIONAL DIRECTIVE ON SECURITY OF NATIONAL SECURITY SYSTEMS (2004).

¹² *Oversight of the State Department: Hearing before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (July 7, 2016).

¹³ *Id.*

¹⁴ James Comey, Dir., Fed. Bureau of Investigation, Statement on the Investigation of Secretary Hillary Clinton's Use of a Personal E-mail System (July 5, 2016) (prepared remarks).

days earlier, Director Comey explained in a public statement that there is a culture of carelessness at the State Department with respect to handling classified information. He stated:

While not the focus of our investigation, [FBI] also developed evidence that the security culture of the State Department in general, and with respect to use of unclassified e-mail systems in particular, was generally lacking in the kind of care for classified information found elsewhere in the government.¹⁵

Although the FBI's investigation focused on whether Secretary Clinton's "exceptionally careless" treatment of classified national security information amounted to criminal mishandling of classified information, Director Comey agreed the security violations raised "an important question . . . that's worth asking."¹⁶ He explained that if an FBI agent had done the same thing, the matter would be taken very seriously and there would be a security review, an adjudication of the agent's continued suitability for a security clearance, and disciplinary action that could include termination and clearance revocation.¹⁷

Indeed, when a security violation occurs—including "spillage" of classified information onto an unclassified system—the head of an agency must take appropriate corrective action, up to and including formal discipline and revocation of the employee's security clearance.¹⁸ Under certain circumstances, the head of the agency must also notify the Director of the Information Security Oversight Office (ISOO) within the National Archives and Records Administration of the violation—namely when an officer or employee negligently, willfully, or knowingly discloses classified information to an unauthorized person.¹⁹ Similarly, if the Director of ISOO finds that a security violation occurs, the Director is required to notify the head of the agency.²⁰ Executive Order 13526, which sets out these requirements, also charges ISOO with oversight of compliance throughout the executive branch with the order and its implementing directives.²¹

With that in mind, the Committee is seeking documents and communications that will help us understand whether, and the extent to which the executive branch is properly investigating the security violations identified by the FBI, and whether the Department of State complies with Executive Order 13526 and its implementing directives.

¹⁵ *Id.*

¹⁶ *Oversight of the State Department: Hearing before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (July 7, 2016); James Comey, Dir., Fed. Bureau of Investigation, Statement on the Investigation of Secretary Hillary Clinton's Use of a Personal E-mail System (July 5, 2016) (prepared remarks).

¹⁷ *Oversight of the State Department: Hearing before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (July 7, 2016)

¹⁸ Exec. Order No. 13,526 at § 5.5, 3 C.F.R. § 707 (2009); e.g., CMTE. ON NAT'L SEC. SYSTEMS, CNSS POL'Y NO. 18, NATIONAL POLICY ON CLASSIFIED INFORMATION SPILLAGE (2006).

¹⁹ Exec. Order No. 13,526 at § 5.5(e)(2), 3 C.F.R. § 707 (2009).

²⁰ *Id.* at § 5.5(a).

²¹ *Id.* at §§ 5.2(b)(2), (4), (6).

The Honorable David Ferriero

November 2, 2016

Page 4

To assist the Committee in its oversight of this matter, please provide: all documents and communications referring or relating to violations or noncompliance with laws, policies, protocols, procedures, or recommendations on information security where the violation or noncompliance is alleged to have occurred between January 21, 2009 and February 1, 2013 at the Department of State. "Violations or noncompliance" includes both notifications and confirmed instances as well as allegations or complaints of violations or noncompliance. "Policies" includes executive orders and directives.

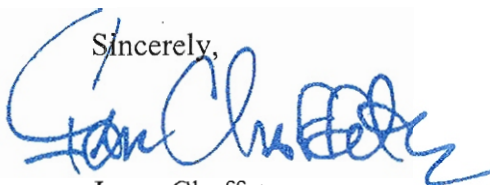
Additionally, provide a briefing to committee staff on federal agencies' efforts to investigate these instances or allegations of violations or noncompliance, mitigate the damage caused by them, and improve security procedures to prevent similar incidents in the future.

Provide all responsive documents and communications and the briefing as soon as possible, but no later than 5:00 p.m. on November 16, 2016. An attachment to this letter defines additional relevant terms and provides information about responding to the Committee's request. When producing documents to the Committee, please deliver production sets to the Majority staff in Room 2157 of the Rayburn House Office Building and the Minority staff in Room 2471 of the Rayburn House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

The Committee on Oversight and Government Reform is the principal oversight committee of the House of Representatives and may at "any time" investigate "any matter" as set forth in House Rule X. Rule X also provides that the Committee has legislative jurisdiction over public information and records.

Please have your staff contact Liam McKenna of my staff at (202) 225-5074 with any questions about this request. Thank you for your attention to this matter.

Sincerely,



Jason Chaffetz
Chairman

Enclosure

cc: The Honorable Elijah E. Cummings, Ranking Minority Member

Responding to Committee Document Requests

1. In complying with this request, you are required to produce all responsive documents that are in your possession, custody, or control, whether held by you or your past or present agents, employees, and representatives acting on your behalf. You should also produce documents that you have a legal right to obtain, that you have a right to copy or to which you have access, as well as documents that you have placed in the temporary possession, custody, or control of any third party. Requested records, documents, data or information should not be destroyed, modified, removed, transferred or otherwise made inaccessible to the Committee.
2. In the event that any entity, organization or individual denoted in this request has been, or is also known by any other name than that herein denoted, the request shall be read also to include that alternative identification.
3. The Committee's preference is to receive documents in electronic form (i.e., CD, memory stick, or thumb drive) in lieu of paper productions.
4. Documents produced in electronic format should also be organized, identified, and indexed electronically.
5. Electronic document productions should be prepared according to the following standards:
 - (a) The production should consist of single page Tagged Image File ("TIF"), files accompanied by a Concordance-format load file, an Opticon reference file, and a file defining the fields and character lengths of the load file.
 - (b) Document numbers in the load file should match document Bates numbers and TIF file names.
 - (c) If the production is completed through a series of multiple partial productions, field names and file order in all load files should match.
 - (d) All electronic documents produced to the Committee should include the following fields of metadata specific to each document:

BEGDOC, ENDDOC, TEXT, BEGATTACH, ENDATTACH,
PAGECOUNT, CUSTODIAN, RECORDTYPE, DATE, TIME, SENTDATE,
SENTTIME, BEGINDATE, BEGINTIME, ENDDATE, ENDTIME, AUTHOR, FROM,
CC, TO, BCC, SUBJECT, TITLE, FILENAME, FILEEXT, FILESIZE,
DATECREATED, TIMECREATED, DATELASTMOD, TIMELASTMOD,
INTMSGID, INTMSGHEADER, NATIVELINK, INTFILPATH, EXCEPTION,
BEGATTACH.
6. Documents produced to the Committee should include an index describing the contents of the production. To the extent more than one CD, hard drive, memory stick, thumb drive, box or folder is produced, each CD, hard drive, memory stick, thumb drive, box or folder should contain an index describing its contents.

7. Documents produced in response to this request shall be produced together with copies of file labels, dividers or identifying markers with which they were associated when the request was served.
8. When you produce documents, you should identify the paragraph in the Committee's schedule to which the documents respond.
9. It shall not be a basis for refusal to produce documents that any other person or entity also possesses non-identical or identical copies of the same documents.
10. If any of the requested information is only reasonably available in machine-readable form (such as on a computer server, hard drive, or computer backup tape), you should consult with the Committee staff to determine the appropriate format in which to produce the information.
11. If compliance with the request cannot be made in full by the specified return date, compliance shall be made to the extent possible by that date. An explanation of why full compliance is not possible shall be provided along with any partial production.
12. In the event that a document is withheld on the basis of privilege, provide a privilege log containing the following information concerning any such document: (a) the privilege asserted; (b) the type of document; (c) the general subject matter; (d) the date, author and addressee; and (e) the relationship of the author and addressee to each other.
13. If any document responsive to this request was, but no longer is, in your possession, custody, or control, identify the document (stating its date, author, subject and recipients) and explain the circumstances under which the document ceased to be in your possession, custody, or control.
14. If a date or other descriptive detail set forth in this request referring to a document is inaccurate, but the actual date or other descriptive detail is known to you or is otherwise apparent from the context of the request, you are required to produce all documents which would be responsive as if the date or other descriptive detail were correct.
15. Unless otherwise specified, the time period covered by this request is from January 1, 2009 to the present.
16. This request is continuing in nature and applies to any newly-discovered information. Any record, document, compilation of data or information, not produced because it has not been located or discovered by the return date, shall be produced immediately upon subsequent location or discovery.
17. All documents shall be Bates-stamped sequentially and produced sequentially.
18. Two sets of documents shall be delivered, one set to the Majority Staff and one set to the Minority Staff. When documents are produced to the Committee, production sets shall be delivered to the Majority Staff in Room 2157 of the Rayburn House Office Building and the Minority Staff in Room 2471 of the Rayburn House Office Building.

19. Upon completion of the document production, you should submit a written certification, signed by you or your counsel, stating that: (1) a diligent search has been completed of all documents in your possession, custody, or control which reasonably could contain responsive documents; and (2) all documents located during the search that are responsive have been produced to the Committee.

Definitions

1. The term “document” means any written, recorded, or graphic matter of any nature whatsoever, regardless of how recorded, and whether original or copy, including, but not limited to, the following: memoranda, reports, expense reports, books, manuals, instructions, financial reports, working papers, records, notes, letters, notices, confirmations, telegrams, receipts, appraisals, pamphlets, magazines, newspapers, prospectuses, inter-office and intra-office communications, electronic mail (e-mail), contracts, cables, notations of any type of conversation, telephone call, meeting or other communication, bulletins, printed matter, computer printouts, teletypes, invoices, transcripts, diaries, analyses, returns, summaries, minutes, bills, accounts, estimates, projections, comparisons, messages, correspondence, press releases, circulars, financial statements, reviews, opinions, offers, studies and investigations, questionnaires and surveys, and work sheets (and all drafts, preliminary versions, alterations, modifications, revisions, changes, and amendments of any of the foregoing, as well as any attachments or appendices thereto), and graphic or oral records or representations of any kind (including without limitation, photographs, charts, graphs, microfiche, microfilm, videotape, recordings and motion pictures), and electronic, mechanical, and electric records or representations of any kind (including, without limitation, tapes, cassettes, disks, and recordings) and other written, printed, typed, or other graphic or recorded matter of any kind or nature, however produced or reproduced, and whether preserved in writing, film, tape, disk, videotape or otherwise. A document bearing any notation not a part of the original text is to be considered a separate document. A draft or non-identical copy is a separate document within the meaning of this term.
2. The term “communication” means each manner or means of disclosure or exchange of information, regardless of means utilized, whether oral, electronic, by document or otherwise, and whether in a meeting, by telephone, facsimile, email (desktop or mobile device), text message, instant message, MMS or SMS message, regular mail, telexes, releases, or otherwise.
3. The terms “and” and “or” shall be construed broadly and either conjunctively or disjunctively to bring within the scope of this request any information which might otherwise be construed to be outside its scope. The singular includes plural number, and vice versa. The masculine includes the feminine and neuter genders.
4. The terms “person” or “persons” mean natural persons, firms, partnerships, associations, corporations, subsidiaries, divisions, departments, joint ventures, proprietorships, syndicates, or other legal, business or government entities, and all subsidiaries, affiliates, divisions, departments, branches, or other units thereof.

5. The term “identify,” when used in a question about individuals, means to provide the following information: (a) the individual's complete name and title; and (b) the individual's business address and phone number.
6. The term “referring or relating,” with respect to any given subject, means anything that constitutes, contains, embodies, reflects, identifies, states, refers to, deals with or is pertinent to that subject in any manner whatsoever.
7. The term “employee” means agent, borrowed employee, casual employee, consultant, contractor, de facto employee, independent contractor, joint adventurer, loaned employee, part-time employee, permanent employee, provisional employee, subcontractor, or any other type of service provider.