JASON CHAFFETZ, UTAH
CHAIRMAN

ONE HUNDRED FOURTEENTH CONGRESS

ELIJAH E. CUMMINGS, MARYLAND
RANKING MINORITY MEMBER

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

March 3, 2015

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

Dear Mr. Secretary:

The Committee is conducting oversight of a series of recent cyber-attacks against the State Department's e-mail network. According to recent press reports, the State Department confirmed that hackers breached the unclassified e-mail system three months ago, with indications that the hackers may have ties to Russia.[1] The State Department reportedly has been unable to remove the hackers from the network, and the intrusions have persisted.[2] According to the *Wall Street Journal*, "Each time investigators find a hacker tool and block it . . . the intruders tweak it slightly to attempt to sneak past defenses."[3]

Ranking Member Cummings requested information about this attack from the State Department on November 17, 2014.[4] Then-Chairman Darrell Issa also asked for information about this attack from the Office of Management and Budget (OMB) on November 20, 2014.[5] Shaun Donovan, the Director of OMB, responded on December 10, 2014, stating:

> OMB regularly, in consultation with Federal partners, issues Federal cybersecurity policy guidance that is consistent with the latest technology and cyber risks. OMB continues to update this guidance as appropriate to ensure that agencies have the best practices and techniques at their disposal. . . . I encourage the Committee to contact agencies directly for information related to recent cybersecurity incidents impacting their respective IT systems.[6]

---

[1] Danny Yadron, *Three Months Later, State Department Hasn't Rooted Out Hackers,* WALL ST. J., Feb. 19, 2015.
[2] *Id.*
[3] *Id.*
[4] Letter from Hon. Elijah E. Cummings, Ranking Member, H. Comm. on Oversight and Gov't Reform, to Hon. John F. Kerry, Secretary of State (Nov. 17, 2014).
[5] Letter from Hon. Darrell Issa, Chairman, H. Comm. on Oversight and Gov't Reform, to Hon. Shaun Donovan, Director, Office of Management and Budget, and Lisa Schlosser, Acting Fed. Chief Info. Officer, Office of Management and Budget (Nov. 20, 2014).
[6] Letter from Hon. Shaun Donovan, Director, Office of Management and Budget, to Hon. Darrell Issa, Chairman, H. Comm. on Oversight and Gov't Reform (Dec. 10, 2014) at 2.

Pursuant to Director Donovan's recommendation to seek information about specific cybersecurity incidents directly from the affected agency, and in light of recent reports the State Department has been unable to permanently remove hackers from its network, we are writing to request information about this matter. To assist the Committee, please provide responses to the following questions as soon as possible, but no later than 5:00 p.m. March 11, 2015:

1. What actions has the State Department taken to remove the hackers responsible for the cyber-attack three months ago from the Department's network?

2. What information was compromised as a result of this attack?

3. What vulnerabilities has the State Department identified that allowed this attack to happen, and allowed the hackers to remain in the network for so long?

4. What safeguards has the Department put in place to prevent the network from being hacked again?

5. How has the Department proactively shared its lessons-learned with other Executive Branch agencies to prevent similar attacks in the future?

Please also make arrangements to brief Committee staff on this matter as soon as possible, but no later than March 15, 2015.

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.

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. An attachment to this letter contains additional instructions for responding to Committee document requests.

If you have any questions about this request, please contact Art Arthur or David Ehredt of the Committee Staff at (202) 225-5074. Thank you for your attention to this matter.

Sincerely,

Jason Chaffetz
Chairman

Elijah E. Cummings
Ranking Minority Member

Ron DeSantis
Chairman
Subcommittee on National Security

Stephen F. Lynch
Ranking Minority Member
Subcommittee on National Security

Will Hurd
Chairman
Subcommittee on Information Technology

Robin L. Kelly
Ranking Minority Member
Subcommittee on Information Technology

Enclosure

cc: The Honorable Edward Royce, Chairman
House Foreign Affairs Committee

The Honorable Eliot Engel, Ranking Minority Member
House Foreign Affairs Committee

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.