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

July 24, 2015

The Honorable Beth Cobert
Acting Director
U.S. Office of Personnel Management
1900 E Street NW
Washington, DC 20415-1000

Dear Ms. Cobert:

The recently disclosed security breaches at the Office of Personnel Management (OPM) raise numerous questions not only about OPM's response to the breaches, but also about the agency's overall information system security and incident response capabilities. To gain a greater understanding of OPM's actions leading up to and following identification of the breaches, the Committee held three hearings on June 16, June 24, and July 15, 2015. Even after these hearings, many questions remain unanswered, particularly questions related to the topics noted below.

CyTech Services. Recent media reports indicated that CyTech Services discovered the OPM breach, when carrying out a demonstration of security software.[1] In response to these allegations, OPM stated, "the assertion that CyTech was somehow responsible for the discovery of the intrusion into OPM's network during a product demonstration is inaccurate."[2] The allegation that a contractor providing a demonstration to OPM discovered the breach, and not the agency itself, is concerning and calls into question OPM's incident response activities and the use of information security tools on OPM's systems.

Inspector General Audit Alert. OPM recently initiated a plan to update its IT infrastructure. According to a June 17, 2015 Inspector General (IG) Audit Alert, OPM is in the process of developing a new network infrastructure environment to strengthen and improve security capabilities.[3] According to the IG's Audit Alert, OPM awarded a sole source contract with a justification for other than full and open competition. The IG questioned using a sole source contract for the later phases of this network infrastructure project.[4] The first phase of this

---

[1] Damian Paletta, *Cybersecurity Firm Says It Found Spyware on Government Network in April,* WALL ST. J., June 15, 2015, *available at* http://www.wsj.com/articles/firm-tells-of-spyware-discovery-in-government-computers-1434369994.
[2] *Id.*
[3] U.S. Office of Personnel Mgmt. Office of the Inspector Gen., *Flash Audit Alert – U.S. Office of Personnel Management's Infrastructure Improvement Project* (June 17, 2015) (Report No. 4A-CI-00-15-055).
[4] *Id.*

multi-phase project is known as the "Shell."[5] The prime contractor for this project, Imperatis, signed the contract to begin this multi-phase project in June 2014.

Homeland Security Presidential Directive 12. In 2004, Homeland Security Presidential Directive 12 (HSPD-12) was issued to increase the security of federal facilities and information systems. HSPD-12 ordered the government to establish a government-wide standard for secure and reliable forms of ID for employees and contractors to access government-controlled facilities and information systems. In 2011, OMB directed agency heads to assist in completing adoption of the federal Personal Identity Verification (PIV) smart card credentials.[6] Later that year, the Government Accountability Office found that agencies "have made limited progress in implementing the electronic capabilities of PIV credentials for logical access to Federal Information Systems."[7]

To assist the Committee's effort to understand OPM's overall information system security and incident response capabilities, as well as the other identified issues, please provide the following documents and information:

1. Please provide the following information for the data breach announced on June 4, 2015 and, separate and distinct information for the data breach announced on July 9, 2015:

    a. The specific date or dates on which OPM[8] detected the breach;

    b. The specific date or dates on which OPM identified associated malware, malicious code, or malicious logic;

    c. All documents, including any summaries or analysis, identifying the malicious code or malicious logic used in conducting the breach;

    d. The date or dates on which OPM contacted the Federal Bureau of Investigations (FBI) and/or the Department of Homeland Security's U.S. Computer Emergency Readiness Team (DHS/US-CERT) to conduct incident response and remediation activities;

    e. The date or dates on which the FBI and/or US-CERT made site visits to OPM for purposes of incident response and remediation activities;

---

[5] *Id.*
[6] Office of Mgmt. and Budget, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for Common Identification Standard for Federal Employees and Contractors (Feb. 3, 2011) *available at* https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf
[7] Gov't Accountability Office, *Personal ID Verification Agencies Should Set a Higher Priority on Using the Capabilities of Standardized Identification Cards* at 28 (Sept. 2011) (GAO-11-751).
[8] References to "OPM," within this letter do not include OPM contractors, vendors, or other private sector entity working for or under contract with OPM.

f. Related US-CERT reports and/or recommendations to OPM;

g. The date or dates on which OPM began forensic analysis of the information technology environment, including, but not limited to, imaging, reviewing logs for malicious code or network traffic related to this breach, remediation activities; and

h. The names and titles of any and all individuals, including any third party contractors, providing incident response services.

2. All OPM building (1900 E Street, NW, Washington, D.C.) visitor logs identifying any visitors from Imperatis, CyTech, US-CERT, or the FBI from April 1 to July 10, 2015.

3. A copy of the most recent curriculum vitae, resume, or similar documentation concerning Mr. Jeff Wagner, Information Security Director at OPM, identifying his current and prior positions at OPM, as well as professional experience prior to obtaining employment with at OPM.

4. The date or dates on which CyTech gave a demonstration to OPM.

5. All instructions provided by OPM or contractor personnel to CyTech for the demonstration, including the expected length of time of the demonstration.

6. A description of all locations on OPM's information technology environment, including endpoint and server identification information, that were tested with the CyTech security technology.

7. A description of the results of this demonstration, including any malware or other malicious code identified.

8. The names and titles of all contractors and OPM staff and executives who participated in the demonstration.

9. The names and titles of all contractors and OPM staff and executives who participated, managed, or subsequently briefed on the results of the demonstration.

10. All documents detailing any OPM request for quotations (RFQs) for purchases from Cytech, including but not limited to any RFQs for emergency purchases and actual purchases for the company's products or services.

11. A description of how OPM uninstalled CyTech's technology from the OPM network, including the date or dates on which technology used by CyTech to conduct demonstrations at OPM were uninstalled from OPM information technology environment; a description of each OPM's network endpoints and/or servers that CyTech

technology was uninstalled from; and the names and titles of any OPM employees that conducted the work to uninstall these technologies.

12. A description of how the statement that CyTech "discovered the intrusion when carrying out a demonstration of security software" is false.

13. All documents and communications regarding any press releases or public statements, including drafts, concerning media reports that CyTech discovered the OPM breach.

14. A list of all subcontractors for the new network infrastructure environment known as the "Shell" under development by OPM.

15. A list of all vendors that have tested their security tools on the OPM system(s), including the dates of any such testing, since June 2014, when OPM awarded the new network infrastructure contract.

16. A list of all security tools and the number of licenses purchased since Imperatis and OPM began testing security tools on the OPM system(s).

17. The number and percentage of OPM employees and contractors with and without PIV card credentials.

18. The number and percentage of OPM employees and contractors that can use their PIV card credentials to access OPM information systems.

19. The number of software licenses purchased by OPM to enable the use of PIV card credentials to access OPM information systems, by type and date of purchase.

20. The number of PIV card software licenses that are activated, current and operational, and the date such licenses were activated.

21. All maintenance and service agreements associated with PIV card installation and their expiration dates.

22. A detailed description of each step taken by OPM to update, improve or further deploy PIV card credentials in connection with the White House "30-Day Cyber Sprint."

Please provide all requested information and documents as soon as possible, but no later than 5:00 p.m. on August 17, 2015.

An attachment to this letter provides additional 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 investigative committee in the U.S. House of Representatives. Pursuant to House Rule X, the Committee has authority to investigate "any matter" at "any time."

Please contact Jennifer Hemingway or Julie Dunne of the Committee staff at (202) 225-5074 with any questions about this request. Thank you for your attention to this matter.

Sincerely,

Jason Chaffetz
Chairman

Elijah E. Cummings
Ranking Member

Enclosure

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.