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

April 27, 2016

The Honorable John A. Koskinen
Commissioner
Internal Revenue Service
Washington, D.C. 20528

Dear Commissioner Koskinen:

The security breach that the Internal Revenue Service announced on May 26, 2015 and the IRS's response to the breach have raised serious concerns about the agency's overall information system security and incident response performance.

Taxpayers used the IRS's "Get Transcript" system 47 million times during the 2014-15 tax filing season.[1] The IRS has claimed that nearly 1.5 percent, or 734,000, of those requests were fraudulent, perpetrated by hackers using stolen taxpayer personally identifiable information (PII). The sensitive information disclosed included social security information, dates of birth, street addresses, and tax returns.[2] The IRS initially estimated that hackers compromised the PII of approximately 100,000 taxpayers.[3] That estimate has since tripled. In August 2015, the IRS announced that the number of taxpayers affected by the breach had risen to 334,000.[4] In February 2016, the IRS announced that an expanded review found at least 734,000 taxpayers whose PII was compromised in the breach.[5]

A recent Government Accountability Office (GAO) report found key faults in the IRS's security program, including a lack of network visibility, accountability, and overall inconsistencies in information security enforcement. Additionally, GAO found shortcomings in testing and evaluation are preventing the IRS from being "fully aware of vulnerabilities that could adversely affect critical applications and data."[6]

---

[1] Internal Revenue Serv., *IRS Statement on "Get Transcript"* (Feb. 26, 2016) *available at* https://www.irs.gov/uac/Newsroom/IRS-Statement-On-Get-Transcript (last accessed Apr. 4, 2016).

[2] Government Accountability Office, *IRS Needs to Further Improve Controls over Financial and Taxpayer Data*, (Mar. 2016, GAO-160398) *available at* http://www.gao.gov/assets/680/676097.pdf (last accessed Apr. 4, 2016).

[3] Internal Revenue Serv., *IRS Statement on the "Get Transcript" Application* (May 26, 2015) *available at* https://www.irs.gov/uac/Newsroom/IRS-Statement-on-the-Get-Transcript-Application (last accessed Apr. 4, 2016).

[4] Internal Revenue Serv., *Additional IRS Statement on the "Get Transcript" Incident* (Aug. 17, 2015) *available at* https://www.irs.gov/uac/Newsroom/Additional-IRS-Statement-on-the-Get-Transcript-Incident (last accessed Mar. 22, 2016).

[5] Internal Revenue Serv., *IRS Statement on "Get Transcript"* (Feb. 26, 2016) *available at* https://www.irs.gov/uac/Newsroom/IRS-Statement-On-Get-Transcript (last accessed Apr. 4, 2016).

[6] Government Accountability Office, *IRS Needs to Further Improve Controls over Financial and Taxpayer Data*, (Mar. 2016, GAO-160398) *available at* http://www.gao.gov/assets/680/676097.pdf (last accessed Apr. 4, 2016).

The agency's apparent inability to accurately assess the scope of the 2015 breach and continuing problems in its information security program raises questions about whether the IRS can protect the data in its systems and respond to cyber fraud. Despite assurances that the IRS has instituted new security procedures for the "Get Transcript" application, questions remain about the detection of the breach, the source of the inaccurate initial estimate of the number of affected taxpayers, and the IRS's response to the incident. GAO's recent reports have amplified the importance of these questions and highlighted the urgent need to address them.

To assist the Committee's effort to address these questions, please provide the following documents and information:

1. For the data breach announced on May 26, 2015:

    a. All documents and communications referring or relating to the initial discovery of, response to, or analysis that led to the identification of the breach;

    b. All documents and communications referring or relating to the malicious code or malicious logic that caused the breach and whether that malicious code or logic was known to the National Cybersecurity and Communications Integration Center;

    c. US-CERT reports and/or recommendations related to the breach; and

    d. Documents sufficient to identify any third party contractors who were involved in providing incident response services when IRS conducted incident response and remediation activities;

2. All documents referring or relating to IRS policies and procedures governing cybersecurity incident identification, handling, and response;

3. All documents and communications, including, but not limited to, internal memos, audit logs, forensic analyses, and/or recommendations, referring or relating to the extended data review of the 2015 tax filing season that resulted in a revised number of compromised records announced on August 17, 2015; and

4. All documents and communications, including, but not limited to, internal memos, audit logs, forensic analyses, and/or recommendations, referring or relating to the extended data review of the 2014 and 2015 tax filing season that resulted in a revised number of compromised records announced on February 26, 2016.[7]

---

[7] Internal Revenue Serv., *IRS Statement on "Get Transcript"* (Feb. 26, 2016) *available at* https://www.irs.gov/uac/Newsroom/IRS-Statement-On-Get-Transcript (last accessed Mar. Apr. 4, 2016).

Provide these records as soon as possible, but no later than 5:00 p.m. on May 12, 2016. Please also provide a briefing for Committee staff on this matter no later than May 13, 2016.

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 provides additional information about responding to the Committee's request.

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 Mike Flynn 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 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.