JASON CHAFFETZ, UTAH
CHAIRMAN

ONE HUNDRED FIFTEENTH 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 30, 2017

The Honorable Betsy DeVos
Secretary
U.S. Department of Education
400 Maryland Avenue SW
Washington, D.C. 20202

Dear Madam Secretary:

The federal government has a responsibility to protect the personally-identifiable information (PII) Americans entrust it with each day. The stakes are particularly high at the Department of Education, an agency responsible for securing 139 million unique social security numbers and other sensitive information of students, parents and custodians across the country. Protecting that information is of paramount importance.

The Department maintains 184 information systems, more than 120 of which are operated by contractors or subcontractors.[1] Most of the names, addresses, social security numbers, and other PII on those systems are connected with the federal student aid programs authorized under Title IV of the Higher Education Act, which affects tens of millions of new Americans each year. These programs are primarily need-based, requiring applicants (students and their parents or custodians) to provide the Department with PII and other sensitive information. The Department also manages a significant portfolio of assets ($1.3 trillion) to support those student aid programs, for which it must also ensure appropriate security and continuous operations.[2] In short, the Department is responsible for both a wealth of information on millions of Americans and substantial financial assets.

Despite this critical need, cybersecurity at the Department is far short of where it should be. The Department's Inspector General (IG) has identified information security as a "major management challenge,"[3] and the Government Accountability Office (GAO) testified that the Department is one of 12 agencies for which information security controls constitute a

---

[1] *U.S. Department of Education: Information Security Review: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. 2 (Nov. 17, 2015) (statement of Kathleen S. Tighe, Inspector General, U.S. Department of Education) [hereinafter *Tighe Hearing Statement* (Nov. 17, 2015)].

[2] *Federal Student Aid Portfolio Summary*, DEP'T OF EDUCATION, https://studentaid.ed.gov/sa/about/data-center/student/portfolio (last visited Mar. 23, 2017). As of March 2017, the portfolio the Department oversees accounts for 42.3 million federal student loan borrowers holding nearly $1.3 trillion in outstanding debt obligations. This total excludes private education loan data which is not financed with public debt.

[3] OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF EDUCATION, FY2017 MANAGEMENT CHALLENGES (2016).

"significant deficiency."[4] In its FY2016 Federal Information Security Management Act (FISMA) audit, the IG scored the effectiveness of the Department and Federal Student Aid (FSA) cybersecurity programs at 53 percent, or "generally not effective."[5] While the IG credited the Department in making some progress to strengthen its information security programs, the IG found in FY2016 that "weaknesses remained and the Department and FSA's information systems continued to be vulnerable to security threats."[6]

Until December 2016, the Department had a grade of "F" on the Committee's Federal Information Technology Acquisition Reform Act (FITARA) scorecard.[7] It has since improved to a C+ but continues to receive an F in the subcategories on "Transparency and Risk Management" and "CIO Authorities."[8]

To help ensure the Department safely maintains and secures PII and other sensitive data, the Committee initiated oversight in the 114th Congress that identified a number of issues and concerns for the Department to address, many of which persist as vulnerabilities.[9] Those include:

---

[4] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-16-228T, INFORMATION SECURITY: DEPARTMENT OF EDUCATION AND OTHER FEDERAL AGENCIES NEED TO BETTER IMPLEMENT CONTROLS 13 (Nov. 17, 2015) (statement of Gregory C. Wilshusen, Director, Information Security Issues, U.S. Government Accountability Office).

[5] OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF EDUCATION, ED-OIG/A11Q0001, THE U.S. DEPARTMENT OF EDUCATION'S FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 REPORT FOR FISCAL YEAR 2016: FINAL AUDIT REPORT 3 (2016) [hereinafter *FY2016 FISMA Audit*].

[6] *Id.* at 4.

[7] *See* HOUSE COMM. ON OVERSIGHT & GOV'T REFORM, DEPARTMENT OF EDUCATION FITARA IMPLEMENTATION SCORECARD (Nov. 2015), https://oversight.house.gov/wp-content/uploads/2015/11/Ed-Scorecard.png. The Committee assembled this scorecard based on data that agencies self-reported to OMB. In 2014, FITARA was enacted to increase the roles and authorities of CIO's in making IT acquisition decisions and bolster accountability for IT investment outcomes. As part of its oversight of FITARA, the Committee graded agency implementation of FITARA. Based on available data, collected by GAO at the request of the Committee, agencies were scored in the following four areas: Data Center Consolidation, IT Portfolio Review Savings, Incremental Development, and Risk Assessment Transparency. The Department was one of three agencies to receive the letter grade "F" on the scorecard. Of the four categories considered, the Department received an "F" in all categories except "Risk Assessment" transparency where it receives a "D".

[8] HOUSE COMM. ON OVERSIGHT & GOV'T REFORM, FITARA SCORECARD 3.0 (Dec. 2016), https://oversight.house.gov/wp-content/uploads/2016/12/FULL-Scorecard.pdf.

[9] *See U.S. Department of Education: Information Security Review: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Nov. 17, 2015), https://oversight.house.gov/hearing/u-s-department-of-education-information-security-review/; *Federal Student Aid: Performance-Based Organization Review: Hearing Before the Subcomm. on Gov't Operations of the H. Comm. on Oversight & Gov't Reform and the Subcomm. on Higher Educ. & Workforce Training of the H. Comm. on Educ. & the Workforce*, 114th Cong. (Nov. 18, 2015), https://oversight.house.gov/hearing/federal-student-aid-performance-based-organization-review/; *U.S. Department of Education: Investigation of the CIO: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Feb. 2, 2016), https://oversight.house.gov/hearing/u-s-department-of-education-investigation-of-the-cio/. The Department's CIO Danny Harris retired from the Department of Education on Feb. 22, 2016, following the Feb. 2, 2016 hearing held by the Committee on Oversight and Government Reform that examined ethical misconduct of the CIO that was previously investigated by the OIG.

- In FY2015, the IG found several unauthorized connections that used outdated secure connection protocols, and in FY2016 the IG found the Department continued to use outdated secure connection protocols for many of its connections.[10] As a result, those who connect to the Department to retrieve or submit data could be unwittingly providing sensitive information to a malicious actor or be subject to a "man-in-the middle" type attack. This is an especially problematic finding given the number of individuals that connect to the Department, such as colleges and universities, loan servicers and guaranty agencies, and students or guardians.

- The Department disclosed it was operating 54 unsupported software systems.[11] These are systems whose vendors no longer provide the services and updates necessary to keep the software running efficiently and securely. Many unsupported software systems have widely known vulnerabilities that an adversary could easily find and then leverage to gain unauthorized access to the Department's systems.

- In 2015, the IG conducted a successful penetration test—a hack conducted by security experts—of the Department's network without being detected by exploiting configuration weaknesses.[12] Despite this, the IG's FY2016 audit found configuration management policies and procedures were not current with NIST and Department guidance (a condition also found in the FY2014 and FY2015 audits). Although a successful penetration test is not always cause for alarm, that it went undetected and unmitigated is of great concern.

- The IG's FY2016 audit found the Department had no mechanisms to restrict the use of unauthorized devices physically connected to its network—an open issue since the IG's FY2011 audit. Failure to restrict unauthorized devices could allow malicious users to bypass two-factor authentication, obtain Departmental Internet protocol addresses, and gain access to Departmental internal resources, all potentially without the Department knowing.[13]

- In November 2015, GAO testified the Department had a higher than average number of reported incidents that were policy violations related to mishandling of data in storage or transit compared to other federal agencies (26 percent at the Department compared to 17 percent at other major federal agencies with policy violations).[14] One of the largest threats to any organization's cybersecurity is the insider threat—employees and contractors who either intentionally or unintentionally misuse the organization's IT

---

[10] *FY2016 FISMA Audit* at 21.
[11] Letter from Danny Harris, Chief Information Officer, U.S. Dep't of Educ., to Jason Chaffetz, Chairman, House Comm. on Oversight & Gov't Reform (Jan. 29, 2016) (on file with Committee) [hereinafter *Letter from Danny Harris to Jason Chaffetz* (Jan. 29, 2016)].
[12] *Tighe Hearing Statement* (Nov. 17, 2015) at 10.
[13] *Id.* at 22.
[14] *Id.* at 6.

resources, allowing adversaries to get in the organization's systems.

- The IG found in its FY2016 audit that the Department had not established a process for assessing the knowledge, skills, and abilities of individuals with significant security responsibilities.[15]

- The Department scored a negative 14 percent on the 2015 Office of Management and Budget CyberSprint for total users using strong authentication—one of only three federal agencies to decrease.[16]

    - In February 2016, the Department testified that progress had been made, stating that 95 percent of its users were employing two-factor authentication as of January 31, 2016, and that it projected to achieve 100 percent compliance by March 2016.[17]

    - However, the IG found in its FY2016 FISMA audit that the Department did not consistently and effectively implement two-factor authentication for non-privileged users for accessing internal resources. In addition, while the Department reported 82 percent using two-factor Personal Identity Verification (PIV) or NIST Level of Assurance 4 credential, the OCIO was unable to provide evidence to support the underlying accounts and the IG could not validate the extent to which the Department uses two-factor authentication.[18]

- The IG also found that nine external network connections did not use two-factor authentication (or 19 percent). This issue was identified in both the FY2014 and FY2015 audits. Although the Department stated that this issue was addressed in December 2015, the IG was still able to find remote connections that did not require two-factor authentication.[19]

- The IG found in FY2016 that 66 of the 214 Department authorized active connections it tested (30 percent) failed to adhere to mandated encryption standards.[20]

- A number of the Department's key systems are in need of attention:

---

[15] *FY2016 FISMA Audit* at 32.
[16] Tony Scott, Office of Mgmt. & Budget, *Fact Sheet: Enhancing and Strengthening the Federal Government's Cybersecurity* (June 17, 2015, 5:44 PM), https://obamawhitehouse.archives.gov/blog/2015/06/17/fact-sheet-enhancing-and-strengthening-federal-government-s-cybersecurity. The other two agencies were the departments of Defense and Energy.
[17] *U.S. Department of Education: Investigation of the CIO: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. 6 (Feb. 2, 2016) (statement of John B. King, Jr., Acting Secretary, U.S. Department of Education).
[18] *FY2016 FISMA Audit* at 29.
[19] *Id.* at 29-30.
[20] *Id.* at 21.

- The Common Origination and Disbursement (COD) system is essential to the annual delivery of $150 billion federal student aid funds to Title IV eligible colleges and universities.[21] The IG tested the COD application during its FY2014 FISMA audit and reported several vulnerabilities, some of which were "high severity," with the expectation that the issues should be addressed immediately.[22] However, during testing for the FY2016 audit, the IG reported that the same vulnerabilities were present and the Department had not yet mitigated them.[23] Overall, the IG's vulnerability scans identified 5 high vulnerabilities, 29 medium, and 9 low.

- The Central Processing System (CPS) stores over 139 million unique Social Security Numbers of students and parents that have participated in the federal student aid system,[24] however, the Department reported in the November 2015 hearings that CPS was not equipped for Personal Identity Verification ("PIV-enabled" system) for "strong" multifactor authentication.[25] Further, the former Chief Information Officer for the Department— the individual responsible for agency-wide information security under FISMA—could not say why the CPS system was not PIV-enabled,[26] exposing a possible deficiency in the relationship between the agency CIO and the FSA CIO. The CIO also testified that CPS operates with outdated programming language (one million lines of COBOL), the use of which increases operations and maintenance costs while making securing the system more difficult.[27]

- The IG testified that within the National Student Loan Database System (NSLDS) there are 97,000 accounts or users with access to this significant data, yet only 5,000 of those who have an account have undergone a background check,[28] and the Department disclosed this system is also operating in part with outdated programming language (six million lines of COBOL).[29]

In recent years, the Department's FISMA audits have shown repeat findings and recommendations, indicating that problems are going uncorrected. The FY2016 audit was no

---

[21] *Common Origination and Disbursement (COD) Business Case*, FEDERAL IT DASHBOARD (last revised July 25, 2016), https://www.itdashboard.gov/drupal/summary/018/946#.
[22] *FY2016 FISMA Audit* at 23.
[23] *Id.*
[24] CPS supports front-end tasks, such as the annual processing of 22 million federal student aid applications (i.e., FAFSAs).
[25] *U.S. Department of Education: Information Security Review: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. at 1:28:46 (Nov. 17, 2015).
[26] *Id.*
[27] *Letter from Danny Harris to Jason Chaffetz* (Jan. 29, 2016).
[28] *U.S. Department of Education: Information Security Review: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. at 1:23:32 (Nov. 17, 2015). NSLDS is FSA's comprehensive and integrated solution for managing student aid history regarding Title IV loans, grants, and enrollment data.
[29] *Letter from Danny Harris to Jason Chaffetz* (Jan. 29, 2016).

exception, containing 11 findings, 5 of which were repeat findings from previous FISMA audits. The FY2016 audit also made 15 recommendations, 6 of which are repeat recommendations.[30] This raises questions that warrant additional oversight by the Committee, especially given the volume of personal and sensitive information the Department stores about individuals and the hundreds of billions of dollars at stake.

To assist the Committee, please provide the following documents and information as soon as possible, but no later than 5:00 p.m. on April 13, 2017:

1. The Department's plan for addressing each outstanding finding and recommendation made by the IG's FY2016 FISMA audit, including target dates for completion;

2. Identify the actions, including a description thereof, that the Department has taken to reduce the prevalence of policy violations since FY2016;

3. Identify the 54 software systems that remain unsupported, as well as any additional software systems not previously identified by the Department that are currently unsupported; and

4. A description of the state of deployment of Continuous Diagnostic and Mitigation (CDM)[31] tools as of March 1, 2017.

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. Please note that Committee Rule 16(b) requires counsel representing an individual or entity before the Committee or any of its subcommittees, whether in connection with a request, subpoena, or testimony, promptly submit the attached notice of appearance to the Committee.

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.

---

[30] *FY2016 FISMA Audit* at 5. The Committee asked the Department to explain the prevalence of repeat findings and recommendations, and the Department explained: "Some corrective actions require multi-year projects and funding. Additionally, repeat findings are typically the result of a lack of resources, and staff turnover, which require additional training to complete the corrective action plan prior to a follow on inspection occurring. Often, repeat findings show improvement but a need for further development. The Department continues to make necessary changes as we move toward removing specific findings completely from yearly FISMA audits." *U.S. Department of Education: Information Security Review: Hearing Before the H. Comm. on Oversight & Gov't Reform*, 114th Cong. (Nov. 17, 2015).

[31] CDM provides hardware, software, and services to federal civilian agencies (.gov) so they can better manage and secure their information systems.

If you have questions about this request, please contact Katie Bailey or Mike Flynn of the Majority staff at (202) 225-5074, and Katie Teleky or Tim Lynch of the Minority staff at (202) 225-5051. Thank you for your prompt attention to this matter.

Sincerely,

Jason Chaffetz
Chairman

Elijah E. Cummings
Ranking Member

Will Hurd
Chairman
Subcommittee on Information Technology

Robin L. Kelly
Ranking Member
Subcommittee on Information Technology

Mark Meadows
Chairman
Subcommittee on Government Operations

Gerald E. Connolly
Ranking Member
Subcommittee on Government Operations

Enclosures

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.

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM
U.S. HOUSE OF REPRESENTATIVES
115TH CONGRESS

NOTICE OF APPEARANCE OF COUNSEL

Counsel submitting: _____

Bar number: _____ State/District of admission: _____

Attorney for: _____

Address: _____

Telephone: (_____) _____ - _____

Pursuant to Rule 16 of the Committee Rules, notice is hereby given of the entry of the undersigned as counsel for _____ in (select one):

- (●) **All matters before the Committee**
- ( ) **The following matters (describe the scope of representation):**

_____

_____

All further notice and copies of papers and other material relevant to this action should be directed to and served upon:

Attorney's name: _____

Attorney's email address: _____

Firm name (where applicable): _____

Complete Mailing Address: _____

_____

I agree to notify the Committee within 1 business day of any change in representation.

_____ _____

Signature of Attorney **Date**