

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 26, 2016

Mr. Denis McDonough
Chief of Staff
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20502

Dear Mr. McDonough:

We are writing regarding the Executive Office of the President's (EOP) information security obligations under federal law, specifically with respect to compliance with elements of the Federal Information Security Management Act of 2002,¹ as amended, and upcoming deadlines in the Federal Cybersecurity Enhancement Act of 2015 (FCEA).² Through this letter, we are requesting your full FY 2015 report under the Federal Information Security Management Act, and additional documentation related to implementation of these laws at EOP.

I. Federal Information Security Management Act

Under the Federal Information Security Management Act of 2002, as amended, each agency must develop, document, and implement an information security program with periodic testing of the program's effectiveness.³ In December 2014, Congress passed the Federal Information Security Modernization Act of 2014⁴ (collectively with the Federal Information Security Management Act of 2002, as amended, referred to as FISMA in this letter⁵). The provisions of chapter 35 of title 44, United States Code, require that the agency head—

- oversee establishment of an information security program;⁶
- designate a Chief Information Officer (CIO)⁷ and oversee designation of a senior agency information security officer;⁸

¹ Federal Information Security Management Act of 2002, Pub. L. 107-347, Tit. 3, 116 Stat. 2946–2961, *codified as amended at* 44 U.S.C. § 3551, *et seq.*

² Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N, Title II, Subtitle B (2015).

³ § 3554(b).

⁴ Federal Information Security Modernization Act of 2014, Pub. L. 113-283, 128 Stat. 3073.

⁵ Title 44 is enacted as positive law. Therefore, "FISMA" is used throughout this letter to refer to Title 44, United States Code, at subchapter 2 of chapter 35, as currently enacted.

⁶ *See, e.g.*, § 3554(a)(1)(A)–(B), (a)(2), (a)(6), (b).

⁷ § 3506(a)(2)(A).

- comply with information security standards, directives, policies, and procedures implementing FISMA;⁹ and
- acting through the CIO—
 - periodically assess the potential harm of a data breach of the agency’s information and information systems,¹⁰
 - ensure adequate security training and compliance,¹¹ and
 - conduct periodic testing (such as network penetration tests) of the information security program at least annually.¹²

A. Annual Reporting

FISMA also requires that “each year each agency shall have performed an independent evaluation of the information security program and practices of the agency”¹³ This includes national security systems,¹⁴ as well as agencies that operate them.¹⁵ For agencies with an inspector general, the inspector general will conduct the independent evaluation or hire someone to do so.¹⁶ For agencies without an inspector general, the agency head must hire an independent external auditor to conduct the evaluation.¹⁷ The agency head must then submit the results of that evaluation to the Director of the Office of Management and Budget (OMB), who in turn summarizes the results of those evaluations and submits them in OMB’s annual report to Congress and the public.¹⁸

In addition to the annual independent evaluation of each agency’s information security program and OMB’s report on agency information security generally, FISMA requires that the head of each federal agency annually submit a report on the agency’s information security to the Committee, the Director of OMB, the Comptroller General, and others.¹⁹ FISMA defines “agency” broadly to include governmental entities that may not be included in the definition of

⁸ § 3554(a)(3)(A).

⁹ § 3554(a)(1)(B).

¹⁰ § 3554(a)(2)(D).

¹¹ § 3554(a)(4), (7).

¹² § 3554(a)(2)(D), (b)(1), (b)(5).

¹³ § 3555(a)(1).

¹⁴ § 3555(a)(2)(C), (c), (e)(2). Special provisions apply to conducting evaluations of national security systems and protecting the vulnerabilities they identify, but such systems are not exempt from FISMA requirements. *E.g., id.* For example, FISMA allows for “separate presentations, as appropriate, regarding information security relating to national security systems.” § 3555(a)(2)(C).

¹⁵ § 3557(3).

¹⁶ § 3555(b)(1).

¹⁷ § 3555(b)(2).

¹⁸ § 3553(c)(3).

¹⁹ *See* § 3554(a)(1)(B) (making the head of an agency responsible for “complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines”), (c)(1) (requiring each agency submit an annual report on information security).

“agency” in other statutes. EOP is expressly referenced in the statute as included in the definition of “agency” for the purpose of FISMA, one of few such agencies.²⁰

Although FISMA does not set a specific deadline for the annual report, under implementing policies, OMB established a deadline of March 1, 2016, for agencies’ FY 2015 FISMA submissions to Congress.²¹ According to our records, the Committee has yet to receive EOP’s FISMA submission for FY 2015. It is especially troubling that EOP has yet to submit its complete FISMA report to the Committee, given the agency’s central role in overseeing other federal agencies’ FISMA compliance. EOP should be setting an example for agencies in complying with federal information security requirements, not failing in its own compliance with the law.²²

FISMA prescribes certain elements of agencies’ annual FISMA submissions in section 3554.²³ Through section 3554, Congress also authorized the Director of OMB and the Secretary of Homeland Security, in coordination with the Director, to specify additional elements for FISMA reporting to the Committee, OMB, and the other report recipients.²⁴ The agencies must include those additional elements as part of their submissions to the Committee, the Director of OMB, and others. FISMA does not authorize an agency to submit different reports to the Committee and OMB. The elements of the FISMA report for FY 2015 are:

- An assessment of the “adequacy and effectiveness of information security policies, procedures, and practices, including—
 - A description of each major information security incident or related sets of incidents . . . ;²⁵
 - The total number of information security incidents, including a description of incidents resulting in significant compromise of information security, system impact levels, types of incident, and locations of affected systems;

²⁰ See § 3554(c) (requiring the “head of each agency” submit a report annually to the Committee); 3552 (incorporating definitions in § 3502 by reference); § 3502(1) (defining the term “agency” to mean “any executive department [. . .] or other establishment in the executive branch of the Government (*including the Executive Office of the President*)” (emphasis added)).

²¹ OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, OMB M-16-03, FISCAL YEAR 2015–2016 GUIDANCE ON FEDERAL INFORMATION SECURITY AND PRIVACY MANAGEMENT REQUIREMENTS (2015) [hereinafter Office of Mgmt. & Budget, OMB M-16-03]. The Committee reserves judgment on the propriety or legality of OMB’s establishment of different reporting deadlines between congressional committees and OMB in M-16-03, given that the statute provides for a single report to multiple entities. The deadline is referenced here only to establish that even under the Administration’s policies, EOP’s FY 2015 FISMA submission is past due.

²² *E.g., Federal Agencies’ Reliance on Outdated and Unsupported Information Technology: Hearing Before the H. Comm. on Oversight & Government Reform*, 114 Cong. (2016) (statement of Tony Scott, Federal Chief Information Officer) (“If we are required to [submit a FISMA report under Sec. 3554(c)], I think it sets a bad example [that we didn’t], correct.”).

²³ § 3554(c).

²⁴ §§ 3553(b)(2)(B), 3554(a)(1)(B), (c)(1)(A)(iv).

²⁵ For more information on reporting of major incidents, see Congressional Notifications, *infra* part I. B.

- A description of each major information security incident that involved a breach of personally identifiable information, as defined by the Director [of OMB], including the number of individuals whose information was affected by the major information security incident, and a description of the information that was breached or exposed;
- Any other information as the Director [of OMB] or the Secretary, in consultation with the Director, may require.”²⁶
- “[A]n official letter signed by the head of the agency” which includes: the assessment described above, “[p]rogress towards meeting FY 2015 FISMA Metrics,” and “[p]rogress towards meeting the Cybersecurity [Cross Agency Priority] goal.”²⁷
- Answers to questions included in CyberScope for the CIO, the Inspector General (IG), and the Senior Agency Official for Privacy (SAOP),²⁸ that—if submitted to OMB via CyberScope—should be submitted to the Committee as digital copies of the CyberScope submissions (such as PDFs) or printouts.
- Privacy related documentation, including a “[d]escription of the agency’s privacy training for employees and contractors; [c]opy of the agency’s breach notification policy; [p]rogress update on reducing holdings of personally identifiable information [including social security numbers]; and [a] memorandum describing the agency’s privacy program”²⁹
- The agency’s Information Security and Continuous Monitoring (ISCM) strategy required under OMB Management Directive M-14-03.³⁰

FISMA provides that an agency’s report under the law must be submitted in unclassified form, and that to the greatest extent practicable information be included in the unclassified report.³¹ However, FISMA also authorizes each agency to include a classified annex to its FISMA report if necessary, which must be provided to the Committee, OMB, and the other

²⁶ § 3554(c)(1)(A) (dashes and numerals omitted).

²⁷ OFFICE OF MGMT. & BUDGET, OMB M-16-03 at 4–5, *supra* note 21 (providing expanded reporting requirements for agencies under 3554(c)); *see also* § 3554(c)(1)(A)(iv) (requiring submission to the Committee, the Director, and others, such additional data as the Director—or the Secretary in consultation with the Director—may require).

²⁸ § 3554(c)(1)(A); OFFICE OF MGMT. & BUDGET, OMB M-16-03 at 4–5, *supra* note 21; *see also, e.g.*, DEP’T OF HOMELAND SEC., FY 15 CIO ANNUAL FISMA METRICS, VERSION 1.2 at iii (2015) (providing the metrics which the CIO questions are based upon).

²⁹ OFFICE OF MGMT. & BUDGET, OMB M-16-03 at 4–6, *supra* note 21 (providing expanded reporting requirements for agencies under 3554(c)); *see also* § 3554(c)(1)(A)(iv) (requiring submission to the Committee, the Director, and others, such additional data as the Director—or the Secretary in consultation with the Director—may require).

³⁰ OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, OMB M-14-03, ENHANCING THE SECURITY OF FEDERAL INFORMATION AND INFORMATION SYSTEMS (2013) (requiring development of an ISCM strategy); OFFICE OF MGMT. & BUDGET, EXECUTIVE OFFICE OF THE PRESIDENT, OMB M-15-01, FISCAL YEAR 2014–2015 GUIDANCE ON IMPROVING FEDERAL INFORMATION SECURITY AND PRIVACY MANAGEMENT PRACTICES 2 (2013) (requiring provision of the ISCM strategy as part of FISMA reporting via CyberScope).

³¹ § 3554(c)(1)(B).

report recipients.³² The law also mandates that the head of the agency submit the report, and does not authorize you to delegate that responsibility to a subordinate, such as the agency's head of legislative or congressional affairs.³³

B. Congressional Notifications

In addition to the annual reporting on incidents described above, you must notify the Committee within seven days of the date on which there is a reasonable basis to conclude that a major incident occurred at EOP, including any of its subordinate agencies or offices.³⁴

Although the 7-day notification requirement only applies to *major* incidents, it is helpful to begin with an explanation of the term incident, which may include events not traditionally associated with cyber-attacks. The term “incident” includes a wide variety of potential occurrences, including one “that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system”³⁵ or an event that “constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.”³⁶ Data breaches and network intrusions are included within this definition, but neither are necessary to trigger the requirement that you notify Congress of an incident. Nor does an incident need to include a technical element or malicious activity to trigger congressional notification. For example, spillage of classified national security information onto a lower classification network or an unclassified network could trigger a notification. Similarly, the loss or theft of physical documents comprising personally identifiable information or a digital storage device that contains such information would likely both constitute an incident under FISMA, although not necessarily a major incident.

As required by the recent update to FISMA,³⁷ OMB policy provides the criteria for determining whether an “incident” rises to the level of a “major incident.”³⁸ You must notify the Committee within 7 days of there being a reasonable basis to conclude a major incident occurred.³⁹ Although a major incident is a more significant type of incident, the reasonable basis determination is not an extraordinary threshold. You can and should notify the Committee of a major incident before all facts are known, before you have completed an investigation, and before you have confirmed the full extent of the incident.⁴⁰ Within a reasonable time after notifying the Committee of a major incident, you must also provide the Committee with additional information on the incident, including:

³² *Id.*

³³ See § 3554(a)(1)(B) (making the head of an agency responsible for “complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines”); § 3554(c)(1) (requiring each agency submit an annual report on information security).

³⁴ §§ 3554(b)(7)(C)(iii)(III), 3554 (c)(1)(A)(1)(i).

³⁵ § 3552(b)(2)(A).

³⁶ § 3552(b)(2)(B).

³⁷ Federal Information Security Modernization Act of 2014, Pub. L. 113–283, §2(b), 128 Stat. 3073, 3085 (2014).

³⁸ OFFICE OF MGMT. & BUDGET, OMB M-16-03 at 7–9, *supra* note 21.

³⁹ § 3554 (b)(7)(C)(iii)(III)(aa).

⁴⁰ *Id.*

- “a description of the major information security incident or related sets of incidents;”
- descriptions of the “threats and threat actors, vulnerabilities, and impacts of the incident;”
- risk assessments of the affected information systems conducted before the date on which the incident occurred;
- the status of compliance of the affected systems with applicable security requirements at the time of the incident; and
- detection, response, and remediation actions.⁴¹

II. Federal Cybersecurity Enhancement Act of 2015

Last year, Congress also enacted the Federal Cybersecurity Enhancement Act of 2015,⁴² as part of the omnibus cybersecurity bill, the Cybersecurity Act of 2015.⁴³ FCEA requires the head of each agency to implement specific information security practices at the agency by December 18, 2016.⁴⁴ Although the deadline has not passed, we raise these now to ensure you are aware of your responsibilities under the law, and the corresponding deadline.

A. EINSTEIN Deployment

One such requirement is that the head of each agency implement the federal intrusion detection system (IDS) and intrusion prevention system (IPS) known as “EINSTEIN.”⁴⁵ EINSTEIN is currently a three-phase IDS and IPS operated by the Department of Homeland Security (DHS).⁴⁶ EINSTEIN 1 provides the ability to record and analyze netflows in and out of agencies’ networks, and enables post-incident forensic analysis.⁴⁷ EINSTEIN 2 is a signature-based IDS that logs suspected malicious traffic for review by US-CERT.⁴⁸ EINSTEIN 3A (E3A) is a signature-based IPS that identifies and blocks suspected malicious traffic before it reaches an agency’s perimeter, and includes classified indicators.⁴⁹ E3A currently operates two countermeasures—DNS sink-holing and e-mail filtering.⁵⁰

FCEA mandates that agency heads fully deploy all three iterations of EINSTEIN on their networks by December 18, 2016.⁵¹ The capabilities must be applied against all information

⁴¹ §§ 3554(b)(7)(C)(iii)(III)(bb), 3554 (c)(1)(A)(i).

⁴² Federal Cybersecurity Enhancement Act of 2015, Pub. L. No. 114-113, Div. N, Title II, Subtitle B, 129 Stat. 2242, 2963–2975.

⁴³ Consolidated Appropriations Act, 2016, Pub. L. No. 114-113, Div. N, 129 Stat. 2242, 2935–2985 (2015).

⁴⁴ Federal Cybersecurity Enhancement Act § 223(b), 225, 129 Stat. 2963, 2966, 2967–2969.

⁴⁵ Federal Cybersecurity Enhancement Act § 223(b).

⁴⁶ *E.g.*, U.S. GOV’T ACCOUNTABILITY OFF., GAO-16-294, INFORMATION SECURITY: DHS NEEDS TO ENHANCE CAPABILITIES, IMPROVE PLANNING, AND SUPPORT GREATER ADOPTION OF ITS NATIONAL CYBERSECURITY PROTECTION SYSTEM (2016) [hereinafter GAO-16-294].

⁴⁷ *E.g.*, *id.*

⁴⁸ *E.g.*, *id.*

⁴⁹ *E.g.*, *id.*

⁵⁰ *E.g.*, *id.*

⁵¹ Federal Cybersecurity Enhancement Act of 2015, Pub. L. No. 114-113, Div. N, Title II, Subtitle B, § 223(b)(1)(A), 129 Stat. 2242, 2966 (The provision mandates full deployment of EINSTEIN within one year of the

entering or leaving any information system owned by the agency that is coming from or going to another information system owned by any other entity, whether that other information system be a contractor-owned system or an information system on the public Internet with no affiliation to the agency.⁵²

FCEA also directs DHS to deploy, and agencies to implement, much-needed improvements to the EINSTEIN platform.⁵³ Congress, GAO, and internal reviews have identified areas for significant improvement with EINSTEIN—most notably that signature-based detection and perimeter-based cybersecurity is widely considered to be an insufficient cybersecurity control against advanced persistent threats.⁵⁴ Even DHS concedes that to counter modern threats, improvements are needed in EINSTEIN. For example, in response to a question from Senator Ron Johnson, Chairman of the Senate Homeland Security and Governmental Affairs Committee, the Secretary of Homeland Security acknowledged the limitations of signature-based detection in EINSTEIN—that the system cannot detect malware employing sophisticated obfuscation⁵⁵ with dynamic command and control infrastructure.⁵⁶ Phyllis Schneck, DHS's Deputy Undersecretary for Cybersecurity and Communications, who oversees the program, later stated that she recognized from her first day that EINSTEIN “is technology that’s 25 [years old].”⁵⁷

Accordingly, in FCEA Congress mandated that DHS pilot new countermeasures and non-signature based detection on EINSTEIN,⁵⁸ such as heuristic- and behavior-based detection, and that the EINSTEIN platform be expanded to scan traffic within an agency’s network, not just

date of enactment [December 18, 2015] or two months after the capabilities are made available, whichever is later. Since DHS certified availability of the capabilities to all agencies more than two months before December 18, 2016, the later and applicable deadline is December 18, 2016.).

⁵² Federal Cybersecurity Enhancement Act § 223(b)(1)(B), (b)(3) (requiring application to “all information traveling between an agency information system [defined in this section only as “an information system owned by the agency”] and any information system [other than an information system owned by the agency]”).

⁵³ Homeland Security Act of 2002, Pub. L. 107–296, § 230(b)(2), (c)(4)–(5) (as amended through Pub. L. 114–143).

⁵⁴ E.g., SEN. TOM COBURN, M.D., RANKING MEMBER, SEN. COMM. ON HOMELAND SEC. & GOVERNMENTAL AFFAIRS, A REVIEW OF THE DEPARTMENT OF HOMELAND SECURITY’S MISSIONS AND PERFORMANCE 85 (2015), available at <https://www.hsgac.senate.gov/media/minority-media/final-coburn-oversight-report-finds-major-problems-in-dhs>; U.S. GOV’T ACCOUNTABILITY OFF., GAO-16-294, *supra* note 46; see also, e.g., VERIZON, DATA BREACH INVESTIGATION REPORT 22 (2015); Tyler Thia, *Signature-based detection, protection systems ineffective*, ZDNET (June 27, 2011); Matthew Richard, *Intrusion Detection FAQ: Are there limitations of Intrusion Signatures?*, SANS INSTITUTE (Apr. 5, 2001); Arnt Brox, *Signature-Based or Anomaly-Based Intrusion Detection: The Practice and Pitfalls*, SC MAG. (May 1, 2002).

⁵⁵ Broadly, these are types of malware that change their digital signature to avoid detection by signature-based applications, like anti-virus software. They are sophisticated tools used by advanced persistent threats and can vary in difficulty of detection from oligomorphic malware to polymorphic malware to metamorphic malware.

⁵⁶ *The Homeland Security Department’s Budget Submission for Fiscal Year 2016: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 114 Cong. (2015) (question 19 for the record).

⁵⁷ E.g., Mark Rockwell, *DHS Cybersecurity Office Appeals to Industry for Innovation*, FCW, Dec. 17, 2015, <https://fcw.com/articles/2015/12/17/rockwell-dhs-cybersecurity-industry.aspx>.

⁵⁸ Homeland Security Act § 230(b)(2), (c)(4)–(5).

traffic entering or exiting it.⁵⁹ This reflects cybersecurity experts' preference to move towards zero trust models of security within networks that reduce dependence on perimeter-based security.⁶⁰ Each agency head must, in turn, implement improvements to the EINSTEIN platform (such as new countermeasures or detection tools) within six months of DHS making the improvement available to the agency.⁶¹

The mandate for deploying EINSTEIN (and subsequent improvements to EINSTEIN) require agencies apply the IDS and IPS technologies to “all information” traveling between an agency information system and any non-agency information system.⁶² To the extent that EINSTEIN capabilities include deep packet inspection, this mandate necessitates that agencies present data to EINSTEIN in a readable form, on which the capabilities can operate effectively. FCEA includes this requirement because advanced persistent threats are known to encrypt malicious traffic and disguise it as legitimate traffic, in order to evade detection and blocking.⁶³

B. Statutory Cybersecurity Requirements at Agencies

FCEA also establishes a number of specific requirements for cybersecurity, informed by best practices in the private sector and lessons learned during past breaches. Under the law, you are responsible for ensuring implementation of these cybersecurity requirements on each information system at EOP, including those of any of its subordinate agencies and offices, within one year of enactment of FCEA—December 18, 2016.⁶⁴

⁵⁹ Homeland Security Act § 230(b)(1) (requiring that the intrusion detection and prevention capabilities, which collectively refer to EINSTEIN, apply to traffic *transiting* the agency information system, in addition to traffic entering or exiting the agency information system, the former being the current configuration of EINSTEIN). Compare Federal Cybersecurity Enhancement Act of 2015, Pub. L. No. 114-113, Div. N, Title II, Subtitle B, § 223(b)(1)(A), 129 Stat. 2242, 2966 (applying the initial mandate that agencies deploy EINSTEIN only to traffic “traveling between an agency information system and any [non-agency] information system”, i.e. entering or exiting the agency’s network but not traffic solely within the agency’s internal networks or a single information system) with § 223(b)(1)(B), 129 Stat. at 2966 (requiring deployment of EINSTEIN improvements with no such limitation on application and therefore requiring application of the technology internally at an agency when such technology is made available, given the requirement of section 230(b)(2) of the Homeland Security Act that DHS make available a capability to scan and block traffic *transiting* an agency’s information systems).

⁶⁰ See, e.g., Brett Benyo, et al., *Automated Self-Adaptation for Cyber-Defense: Pushing Adaptive Perimeter Protection Inward*, in 7 IEEE COMPUTER SOCIETY, INTERNATIONAL CONFERENCE ON SELF-ADAPTATION AND SELF-ORGANIZING SYSTEMS WORKSHOPS (2013); Nicholas D. Evans, *The Importance of Zero-Trust and an Adaptive Perimeter in Cyber Fortifications*, COMPUTERWORLD, May 19, 2014, <http://www.computerworld.com/article/2476276/security0/the-importance-of-zero-trust-and-an-adaptive-perimeter-in-cyber-fortifications.html>.

⁶¹ Federal Cybersecurity Enhancement Act § 223(b)(1)(C), 129 Stat. 2963, 2966.

⁶² See § 223(b), 129 Stat. 2963 (providing that “the head of each agency shall apply and continue to utilize the [EINSTEIN] capabilities to all information traveling between an agency information system and any [other] information system . . .” with no exception for encrypted or otherwise-obfuscated data).

⁶³ See, e.g., CROWDSTRIKE, GLOBAL THREAT REPORT 50 (2015) (“in some cases [rootkits] even deploy [. . .] scripts in encrypted form via cloud services [. . .]” one exploit kit even used encryption “to prevent analysis” of the malware) INTEL SECURITY, GRAND THEFT DATA 3 (2015) (“32% of data exfiltrations were encrypted.”)

⁶⁴ Federal Cybersecurity Enhancement Act § 225(b)(1), 129 Stat. 2963, 2968 (requiring implementation by “the head of each agency”).

- **Identify sensitive data and mission critical data held** by the agency and prioritize the security of the information.⁶⁵
- **Assess access controls to such data, the need for those data to be readily accessible, and individuals' need to access those data.** This requirement is made particularly relevant in light of recent data breaches in which “flat” networks with poorly configured access controls enabled data exfiltration. For example, with the OPM data breach, digitally stored background investigation files apparently included retirees’ files that the agency was unlikely to need to access digitally in the future. Agencies should consider whether all sensitive or mission critical data needs to be digitized at all, or stored on internet- or network-connected information systems. In addition, agencies should consider logical micro-segmentation and physical segmentation of networks to limit loss of sensitive data, in the event of a successful network intrusion.⁶⁶
- **Encrypt or otherwise render such data indecipherable.** Encryption of sensitive data and mission critical data can reduce the likelihood that an adversary will be able to view it, even if the adversary is able to access or exfiltrate it.⁶⁷
- **Enable multi-factor authentication for remote access and privileged users.** Multi-factor authentication refers to the identification of a user through two or more types of information—typically something the user knows (such as a password), something the user has (such as cryptographic key), or something they are (such as a fingerprint). Multi-factor authentication reduces the potential for damage if an adversary obtains an authorized user’s network credentials.⁶⁸
- **Implement Connect.gov for members of the public to logon to EOP’s website.** To comply with the National Strategy for Trusted Identities in Cyberspace (NSTIC), the General Services Administration makes available a single-sign-on trusted identity platform, Connect.gov, to provide high-confidence authentication of individuals to agencies. Connect.gov has the added benefits of making it so users need remember only one credential for all federal agencies’ websites and of providing a pre-built, customizable authentication service at no cost to agencies.⁶⁹ Nevertheless, some agencies have chosen to implement their own authentication protocols rather than use Connect.gov, frequently to their detriment and the detriment of the public. For example, both the Internal Revenue Service’s *Get Transcript* application and the Social Security Administration’s *my Social Security* application employed custom-built identity

⁶⁵ § 225(b)(1)(A), 129 Stat. at 2968.

⁶⁶ § 225(b)(1)(B), 129 Stat. at 2968.

⁶⁷ § 225(b)(1)(C), 129 Stat. at 2968.

⁶⁸ § 225(b)(1)(E), 129 Stat. at 2968.

⁶⁹ E.g., *National Strategy for Trusted Identities in Cyberspace: Government Adoption of Connect.gov*, NIST.GOV, <http://www.nist.gov/nstic/connect-gov.html> (last accessed July 12, 2016).

verification tools and suffered security incidents as a result of their poor design.⁷⁰ Based in part on the discovery that those agencies were implementing their own, less effective authentication platforms, Congress mandated in FCEA that agencies use Connect.gov to authenticate visitors to their websites, when authentication is necessary.⁷¹

You may exempt an agency information system from any of the four cybersecurity requirements described above, but only after personally certifying to the Director of OMB and Congress each of the following:⁷²

- The operational requirements of a specified information system (which you describe in the certification) would make it *excessively burdensome* to implement the specific security requirement.⁷³
- The cybersecurity requirement is not necessary to secure the information system or information stored on or transiting that information system.⁷⁴
- EOP has taken all necessary steps to secure the information system and the information stored on or transiting it.⁷⁵

The certification process intentionally sets a high bar. The head of an agency can and should expect to be held to account if, after certifying an exception to any of these controls for an information system, that exception becomes a vector for a data breach or other security incident.

III. Production Request

In order to ensure compliance with FISMA and assist in the Committee's oversight of EOP's cybersecurity including implementation of FISMA and FCEA, please provide the following documents and information:

1. EOP's complete FISMA report, as described above; or those materials that are complete, if some elements of EOP's FISMA submission are incomplete, and the status of the remaining elements. According to the Committee's records, the Committee has yet to receive the following items from you:

⁷⁰ E.g., *The IRS Data Breach: Steps to Protect Americans' Personal Information: Hearing Before the S. Comm. on Homeland Sec. & Governmental Affairs*, 114 Cong. (2015); Brian Krebs, *Crooks Hijack Retirement Funds Via SSA Portal*, KREBSONSECURITY (Sept. 18, 2013, 8:53 pm) <http://krebsonsecurity.com/2013/09/crooks-hijack-retirement-funds-via-ssa-portal/>; see also Jared Serbu, *IRS' \$130 Million RFP to Fix ID Theft Diverges from Governmentwide Initiative*, FED. NEWS RADIO, June 8, 2015, <http://federalnewsradio.com/technology/2015/06/irs-130-million-rfp-to-fix-id-theft-diverges-from-governmentwide-initiative/>.

⁷¹ § 225(b)(1)(D), 129 Stat. at 2968.

⁷² § 225(b)(2), 129 Stat. at 2968.

⁷³ § 225(b)(2)(A)(i), 129 Stat. at 2968.

⁷⁴ § 225(b)(2)(A)(ii), 129 Stat. at 2968.

⁷⁵ § 225(b)(2)(A)(iii), 129 Stat. at 2968.

- a. Your letter to OMB with the elements described in Part I.A. above or—if no letter was submitted to OMB—your attestation that no letter was submitted to OMB;
 - b. If not included in your letter to OMB accompanying the FISMA report, a document containing the elements described in Part I.A. including information on security incidents at EOP;
 - c. EOP's strategy on Information Security and Continuous Monitoring (ISCM);
 - d. Copies of EOP's CyberScope submissions for the CIO questions, SAOP questions, and independent evaluation (inspector general) questions;
 - e. EOP's data breach response plan;
 - f. EOP's plan for reducing holdings of personally identifiable information and social security numbers;
 - g. The memorandum describing EOP's privacy program; and
 - h. The memorandum describing EOP's privacy training for employees and contractors.
2. If you believe EOP is not subject to or is otherwise exempt from FISMA, your legal interpretation of FISMA and your agency's authorizing statutes that exempts EOP from FISMA.
3. The classified annex for EOP's report submitted under Section 3554(c) for FY 2015, or your attestation that no classified annex to the report exists or was created.
4. The report of the results of each independent evaluation of information security program as required under Section 3555 for FY 2015.
5. The report of the results of each independent evaluation of an information security program involving a national security system or a classified system, as required under Section 3555 for FY 2015, or your attestation that EOP does not have or control any national security systems or classified systems.
6. The report of the results of each penetration test and red team exercise conducted against EOP's information or information systems from FY 2015 to present, or your attestation that no such test or exercise was completed.
7. Each certification you submitted to the Director of OMB or any committee of Congress pursuant to Section 225(b)(2) of the Federal Cybersecurity Enhancement Act of 2015, and your assurance that you will provide the Committee a copy of any such certification you submit to the Director of OMB or any committee of Congress in the future.
8. A list of all major incidents, as defined in FISMA, at EOP—including any of its subordinate offices, components, and agencies—from October 30, 2015, to the date of your response, or your attestation that no major incidents occurred at EOP during that period.

It would also be useful to the Committee for you to submit your input with respect to the effectiveness of FISMA and other information security laws, and implementing standards, directives, policies, and procedures—including any areas of federal law on information security that you believe are ineffective or should be updated or improved. We invite you to submit any such comments in writing in response to this letter or to have your staff provide feedback to Committee staff on a more informal basis.

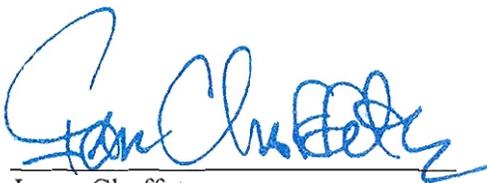
Provide these records as soon as possible, but no later than 5:00 p.m. on August 9, 2016. Should your response necessitate production of classified documents or information, please provide those as an appendix to the letter under separate cover.

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."⁷⁶ Under the Rule, the Committee is also the primary committee of legislative jurisdiction in the House of Representatives for matters related to federal information, including federal information security.⁷⁷

Please contact Liam McKenna of the majority staff at (202) 225-5074 or [REDACTED] and Krista Boyd of the minority staff at (202) 225-5051 or [REDACTED] with any questions about this request. Thank you for your attention to this matter.

Sincerely,



Jason Chaffetz
Chairman



Elijah E. Cummings
Ranking Member

Enclosure

⁷⁶ H. Rule X, clause 4 (c)(1)(2).

⁷⁷ H. Rule X, clause 1 (n)(10).

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,
SENTHOUR, 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.

2016-07-26 JEC EEC to 27 Agencies - FISMA due 8-9 (27 individual letters) have been sent to:

Title 1	First Name	Last Name	Position	Agency
The Honorable	John O.	Brennan	Director	Central Intelligence Agency
Mr.	Denis	McDonough	Chief of Staff	Executive Office of the President
The Honorable	Charlie	Bolden	Administrator	National Aeronautics and Space Administration
The Honorable	France A.	Córdova	Director	National Science Foundation
The Honorable	James R.	Clapper	Director	Office of the Director of National Intelligence
The Honorable	Gayle E.	Smith	Administrator	U.S. Agency for International Development
The Honorable	Thomas J.	Vilsack	Secretary	U.S. Department of Agriculture
The Honorable	Penny	Pritzker	Secretary	U.S. Department of Commerce
The Honorable	Ashton B.	Carter	Secretary	U.S. Department of Defense
The Honorable	John	King	Secretary	U.S. Department of Education
The Honorable	Ernest	Moniz	Secretary	U.S. Department of Energy
The Honorable	Sylvia Mathews	Burwell	Secretary	U.S. Department of Health and Human Services
The Honorable	Jeh C.	Johnson	Secretary	U.S. Department of Homeland Security
The Honorable	Julian	Castro	Secretary	U.S. Department of Housing and Urban Development
The Honorable	Sally	Jewell	Secretary	U.S. Department of the Interior
The Honorable	Loretta E.	Lynch	Attorney General	U.S. Department of Justice
The Honorable	Thomas E.	Perez	Secretary	U.S. Department of Labor
The Honorable	John F.	Kerry	Secretary	U.S. Department of State
The Honorable	Jacob J.	Lew	Secretary	U.S. Department of Treasury
The Honorable	Anthony	Foxx	Secretary	U.S. Department of Transportation
The Honorable	Robert	McDonald	Secretary	U.S. Department of Veteran Affairs
The Honorable	Gina	McCarthy	Administrator	U.S. Environmental Protection Agency
The Honorable	Denise Turner	Roth	Administrator	U.S. General Services Administration
The Honorable	Stephen G.	Burns	Chairman	U.S. Nuclear Regulatory Commission
The Honorable	Beth F.	Cobert	Acting Director	U.S. Office of Personnel Management
The Honorable	Maria	Contreras-Sweet	Administrator	U.S. Small Business Administration
The Honorable	Carolyn W.	Colvin	Acting Commissioner	U.S. Social Security Administration