LAMAR S. SMITH, Texas
CHAIRMAN

EDDIE BERNICE JOHNSON, Texas
RANKING MEMBER

Congreſs of the United States
House of Representatives

COMMITTEE ON SCIENCE, SPACE, AND TECHNOLOGY

2321 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6301
(202) 225–6371
www.science.house.gov

July 19, 2016

Ms. Beth F. Cobert
Acting Director
U.S. Office of Personnel Management
1900 E Street, N.W.
Washington, DC 20415-1000

Dear Ms. Cobert,

Over the past year, the Committee on Science, Space, and Technology has held several cybersecurity hearings in response to federal data breaches, particularly those that occurred at the Office of Personnel Management (OPM). These hearings have afforded the Committee opportunities to review OPM's and other agencies' compliance with federal information security standards and guidelines, and to identify and understand reasons for inconsistencies in their respective cybersecurity postures.

A recently released U.S. Government Accountability Office (GAO) report accentuates the Committee's particular concerns about OPM's cybersecurity posture.[1] The report reviewed security controls of federal agencies' high impact systems, and according to GAO, "the 18 agencies having high-impact systems identified cyber-attacks from 'nations' as the most serious and most frequently-occurring threat to the security of their systems."[2] The report further elaborates that nations, "including nation-state, state-sponsored, and state-sanctioned programs use cyber tools as part of their information-gathering and espionage activities. In addition, several nations are aggressively working to develop information warfare doctrine, programs, and capabilities."[3]

High impact systems are defined as systems that warrant increased security because they "hold sensitive information, the loss of which could cause individuals, the government, or the nation catastrophic harm."[4] GAO selected four agencies with high impact systems for further review, including notably the Office of Personnel Management. The GAO report notes that the

[1] GAO-16-501, "Agencies Need to Improve Controls over Selected High-Impact Systems," May 2016, available at: http://www.gao.gov/assets/680/677293.pdf; (hereinafter referred to as GAO Report).

[2] Ibid.

[3] Ibid.

[4] Ibid.

four agencies selected for additional review "had not always effectively implemented access controls. These control weaknesses included those protecting system boundaries, identifying and authenticating users, authorizing access needed to perform job duties, and auditing and monitoring system activities."[5]

The identification of foreign nations as one of the most serious cyber threats to agencies underscores concerns that were raised after last year's OPM breach over the potential access to OPM's sensitive data by foreign nationals. According to news reports at the time, it appears that some of OPM's contractors may have given "foreign governments direct access to data long before the recent reported breaches."[6] In one instance, an "administrator for the project 'was in Argentina and his co-worker was physically located in the [People's Republic of China]. Both had direct access to every row of data in every database: they were root.'"[7] Additionally, a different team working on the database was led by two employees with passports from the People's Republic of China.[8] In other words, an agency that identifies foreign nations as the source of the most serious and frequently occurring threat, either failed to realize that foreign nationals had access to its database, or knew it and failed to correct the situation.

The National Institute of Standards and Technology (NIST) provides federal agencies with standards and guidelines on personnel security, including the following minimum security requirement to protect "the confidentiality, integrity, and availability of federal information systems and the information processed, stored, and transmitted by those systems"[9]:

> *Personnel Security (PS): Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that organizational information and information systems are protected during and after personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.*[10]

In addition to this standard, NIST provides the following guidance:

> *Supplemental Guidance: This control enhancement denies individuals who lack appropriate security clearances (i.e., individuals who do not possess security clearances or possess security clearances at a lower level than required) or who are not U.S. citizens, visual and electronic access to any classified information, Controlled Unclassified Information (CUI), or any other sensitive information contained on*

[5] Ibid.

[6] Sean Gallagher, *Encryption "Would Not Have Helped" At OPM, Says DHS Official*, ARSTechnica, June 16, 2015, available at: http://arstechnica.com/security/2015/06/encryption-would-not-have-helped-at-opm-says-dhs-official.

[7] Ibid.

[8] Ibid.

[9] NIST Federal Information Processing Standards Publication 200, "Minimum Security Requirements for Federal Information and Information Systems," March 2006, available at: http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

[10] Ibid.

> *organizational information systems. Procedures for the use of maintenance personnel can be documented in security plans for the information systems.*[11]

NIST defines sensitive information as "information where the loss, misuse, or unauthorized access or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act)."[12] Further, an October 2015 Office of Management and Budget (OMB) memorandum provides a definition for major information security incidents or 'major incidents' that involves multiple factors including Controlled Unclassified Information (CUI) Privacy which refers to confidentiality of personal information or personally identifiable information (PII).[13] These definitions would apply to the OPM data breach which led to the unauthorized access of individuals' "name, Social Security number, address, date and place of birth, residency, educational, and employment history, personal foreign travel history, information about immediate family as well as business and personal acquaintances, and other information used to conduct and adjudicate [one's] background investigation."[14]

More than a year after the attack, OPM's approach to cybersecurity continues to raise questions. For example, the GAO report identifies pushback from OPM staff to some of the recommendations it made in the report, specifically relating to systems owned and operated by contractors. According to OPM, "it approaches security through contractor oversight"[15] for such systems. But as GAO explains in its report, the Federal Information Security Modernization Act of 2014 (FISMA 2014) requires each agency to "ensure security for information and systems maintained by or on behalf of the agency, including systems used or operated by a contractor or other organization on behalf of the agency."[16] It is OPM's responsibility to ensure that all contractors have in place the appropriate security controls to protect its information and information systems.

As set forth in House Rule X, the Committee on Science, Space, and Technology has jurisdiction over NIST which develops cybersecurity standards and guidelines to support the implementation of and compliance with FISMA 2014. As such, I would appreciate your response to the following questions and document requests by August 5, 2016:

1. What guidance does OPM provide its staff relative to oversight of information and information systems owned and operated by contractors? Is this guidance different from that provided for systems owned and operated by OPM staff? If so, how?

[11] NIST Special Publication 800-53, Revision 4, "Security and Privacy Controls for Federal Information Systems and Organizations," April 2013 (includes updates as of January 22, 2015), available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[12] Ibid.

[13] OMB Memorandum M-16-03, "Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements," October 30, 2015, available at: https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-03.pdf.

[14] OPM sample notification letter after cyber breach, available at: https://www.opm.gov/cybersecurity/final-verification.pdf.

[15] See *supra*, note 1, GAO Report.

[16] Ibid.

2. What guidance does OPM provide its staff relative to access to information and information systems by foreign nationals?

3. How does OPM comply with the NIST standard and guideline relative to personnel security identified above?

4. Does OMB provide OPM with any guidance relating specifically to foreign nationals and OPM's information security? If so, how does OPM comply with any such guidance?

5. Has OPM or any OPM contractor ever allowed foreign nationals access to systems or data bases that would provide them access to sensitive information or PII? If so, please provide all information and documents relating to all such incidents.

6. How many foreign nationals work for OPM directly or through contractors, and what is the extent of their access to OPM information and information systems? Please provide all relevant information and documents in response to this question.

7. The GAO report referenced in this letter indicates that OPM does not implement to GAO's satisfaction certain responsibilities under FISMA 2014, as indicated by OPM's comment about the security of systems owned and operated by contractors. How does OPM conduct oversight of information and information systems owned and operated by contractors?

8. Has OMB conducted CyberStat Review Sessions (CyberStats) with OPM either prior to or after OPM announced its data breach last year? If so, what were the results of the CyberStats and what conclusions did OPM and OMB reach relative to OPM's cybersecurity posture? If no CyberStats were conducted, please explain why not?

9. Did OMB staff meet with OPM staff as part of the Cybersecurity Sprint? If so, what was the result of the meetings and what conclusions did OPM and OMB reach relative to OPM's cybersecurity posture? If no such meetings occurred, please explain why not?

10. To further support answers to the above questions, please provide the following information:

    - All personnel security guidance that OPM provides its employees, including such guidance for OPM contractors and foreign nationals; and
    - All documents and communications not covered by the above questions and document requests regarding foreign nationals or foreign governments having unauthorized access to OPM information or information systems as a result of a data breach or cyber-attack.

When producing documents to the Committee, please deliver production sets to the Majority Staff in Room 2321 of the Rayburn House Office Building and the Minority Staff in Room 394 of the Ford House Office Building. The Committee prefers, if possible, to receive all documents in electronic format.

If you have any questions about this request, please contact Raj Bharwani or Sarah Jorgenson of the Committee Staff at 202-225-6371. Thank you for your attention to this matter.

Sincerely,

Lamar Smith
Chairman

cc: The Honorable Eddie Bernice Johnson, Ranking Member
Dr. Willie E. May, Director, National Institute of Standards and Technology