U.S. House of Representatives
COMMITTEE ON VETERANS' AFFAIRS
ONE HUNDRED THIRTEENTH CONGRESS
335 CANNON HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
http://veterans.house.gov

October 22, 2013

The Honorable Eric K. Shinseki
Secretary
Department of Veterans Affairs
810 Vermont Ave., NW
Washington, DC 20420

Dear Secretary Shinseki:

We are writing to advise you that the House Committee on Veterans' Affairs, Subcommittee on Oversight and Investigations, under Rules X and XI of the Rules of the U.S. House of Representatives, is continuing a formal bipartisan investigation into Department of Veterans Affairs (VA) Information Technology (IT) security.

Please be advised that the Subcommittee is operating under a heightened sense of urgency regarding this investigation and the resulting requests for answers to questions and the production of documents will require the highest priority and accelerated responses from the VA.

We ask that you respond to the following questions by **Friday, November 8, 2013**:

1. Why was Congress not informed of VA's network security breaches, as required by the Federal Information Security Management Act (FISMA) and other statutes?

2. Why were VA's audit controls not active as required by federal law?

3. Provide details regarding VA's current IT security posture, **all** vulnerabilities (including all past and present compromises by any entity from January 2010 to present) and a plan to address these vulnerabilities, originally requested June 13, 2013;

4. Continuous monitoring is one of the six steps in the Risk Management Framework (RMF) described in NIST Special Publication 800-37, Revision 1, Applying the Risk Management Framework to Federal Information Systems (February, 2010).

    a. Please provide the Subcommittee with a detailed explanation of steps VA has undertaken since January 1, 2010 to present to implement continuous monitoring at the VA.

b. Is a continuous monitoring program in place currently at VA and if so, is this program in place organization-wide?

c. Of the number of information systems identified by the VA in Document Request 7, below, how many are part of the continuous monitoring program?

d. As part of the continuous monitoring program, please provide the Subcommittee with a detailed explanation of the types of monitoring undertaken by the VA's continuous monitoring program, as well as they types and locations of any diagnostic tools concomitant with the continuous monitoring program to include the types of reports or information generated by such tools and how these reports or information are made available to VA leadership.

5. The Subcommittee understands that VA is moving to an organization-wide deployment of Windows 7. Please provide the Subcommittee with the estimated completion date of this deployment, as well as the number of computers, at present, that are operating using an older operating system.

6. Please provide the Subcommittee with a detailed explanation of the VA's program and policy regarding ensuring that all updated software and security patches are made to all computers in the VA, including manner of performing updates, schedule of performing updates, and policies and procedures regarding computers and systems that operate software incompatible with software or security patches.

7. Please provide an update on VA's progress in addressing the recommendations made by VA OIG in its *Federal Information Security Management Act Audit for Fiscal Year 2012* (Report #: 12-01712-229, June 27, 2013,).

8. Please provide an update on progress in addressing the recommendations made by VA OIG in its *Review of Alleged Transmission of Sensitive VA Data Over Internet Connections* (Report #: 12-02802-111, March 6, 2013).

9. Please provide the Subcommittee with detailed information regarding the VA's policy and practice regarding addressing security vulnerabilities in web applications and programs.

10. The Subcommittee is aware that an encryption program was purchased in 2008, and again in 2010. Please provide the Subcommittee with details regarding whether or not these programs were installed and deployed and if not installed or deployed, the reasons why.

11. According to VA, since 2010 to July 11, 2013, there have been 71 incidents involving targeted malware and labeled by the VA as "Focused Operations (FO) Incidents, and 8 incidents categorized by US-CERT as Category 1 incidents at VA from January 1, 2010 to July 10, 2013.

a. From July 10, 2013 to present, have there been any additional FO incidents?

b. It is our understanding that eight of these 71 incidents were classified as US-CERT Category 1 incidents. Please provide the Subcommittee with the US-CERT categorization of the other 63, or more, incidents.

12. Please provide the Subcommittee with the number of incidents referred to VA's Data Breach Core Team, from January 2010 to present, including the number of referred cybersecurity incidents. In addition, please provide the determinations of VA's DBCT in regards to each of these incidents.

13. According to VA, the number of incidents reported by the VA to US-CERT declined from 7,289 in 2012 to 3,708 in 2013. Please provide the Subcommittee with a detailed explanation of the reasons behind this drop in the number of reported incidents to US-CERT.

14. According to testimony at the June 4, 2013 Oversight and Investigations Subcommittee hearing, a recommendation was made to "designate the VA network as a compromised environment" and that VA should "establish controls that are effective and support the reclamation of control back to VA from nation state sponsored organizations."

a. Has the VA made such a designation, and if not, is the VA planning to make such a designation?

b. What are the practical effects of such a designation if such a designation were to be made?

c. As of now, is the VA network a "compromised environment"? Provide reasoning for any determination.

d. If the VA network is not considered a "compromised environment," explain in detail how VA came to its conclusion, specifically identifying how the domain controller was recaptured from a non-VA entity and control was regained by VA.

Please provide the Subcommittee with the following records by **Friday, November 8, 2013**:

1. All records related to the Authority to Operate (ATO), including waivers of automated information systems from January 2010 to present, originally requested May 14, 2013.

2. Weekly Key Investigations Reports from January 1, 2010 to present;

3. Quarterly reports, from January 1, 2010 to present, provided by the Deputy Assistant Secretary for Information Security to the Secretary, as referenced in VA Handbook 6500.4(b)(9)(s) (dated September 12, 2012) ("[s]ubmitting to the Secretary, at least once every quarter, a report on the deficiencies of the Department or any Administration, office, or facility of the Department in compliance with 44 U.S.C. 3541-3549");

4. Any records referencing matters reported in accordance with the reporting requirement contained in 6500.4(b)(9)(t) ("[r]eporting immediately to the Secretary on any significant deficiency in accordance with paragraph (t) [*sic.*, (s)?] above");

5. Any records referencing matters reported in accordance with the reporting requirement contained in 6500.4(b)(9)(p) ("[r]eporting any compliance failure or policy violation directly to the appropriate Under secretary, Assistant Secretary, or Other Key Officials of the Department for appropriate administrative or disciplinary action");

6. Position descriptions, as well as any changes to position descriptions, effective from January 1, 2010 to present, for positions referenced in VA Handbook 6500.4(b)(1)-(10);

   a. According to the Federal Vacancies Reform Act of 1998, agencies are required to report to Congress and GAO information about the temporary filling of a vacant executive agency position if an acting officer is determined to be serving longer than 210 days. Does the Secretary have a timeline in place for appointing a permanent Chief Information Officer and Chief Information Security Officer? If so, please provide appropriate documentation.

7. A detailed list of the individual information systems, as defined in 44 U.S.C. 3502(8) ("the term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information") or as defined in OMB Circular A-130 or in a publication of the National Institute of Standards and Technology, currently in place at VA as of present (as categorized in accordance with a FIPS 199 impact analysis). Please indicate whether this system is currently authorized to operate, when such authorization was approved, and, if applicable, when such authorization will expire. In addition, please provide a copy of the system security plan for each system, to include:

a. The unique system name and identifier for each system (as required by OMB Circular A-11);

b. The system categorization, in accordance with FIPS 199;

c. The system owner;

d. The authorizing official for that system;

e. The system operational status;

f. A description of the determination of whether the system is a major application or general support system, as well as any other additional categories of information systems types required by VA;

g. A brief description of the function and purpose of the system;

h. A general description of the operational environment of the system;

i. A description the systems interconnected with that system;

j. A description of any particular any laws or regulations that establish specific requirements for that system;

k. A description of the security control baseline selected for that system and a thorough description of how all selected minimum security controls are being implemented or planned to be implemented;

l. The date the security plan was completed and the date the security plan was approved.

8. In regards to the detailed list provided pursuant to request (7), please provide in respect to each identified information system whether that system has been [compromised] at any time between January 1, 2010 to present, and if compromised, whether the VA believes, as of now, that the system remains compromised (as defined by NIST SP 800-32, FIPS 140-2 (and related updates or versions) and CNSSI-4009 (April 2010);

a. For any system identified as compromised, please provide a description of the steps taken to address the effects of such compromise, when such steps have been taken (or are being taken);

b. Whether that system continues to be compromised or is at greater risk of future compromise because of the initial compromise.

Furthermore, the Subcommittee will provide VA with additional letters consisting of questions addressing relevant IT security legislation and guidance. Please deliver one set of responses to the current and future questions as well as one set of copies of all requested records to both the Majority and Minority Oversight & Investigations Subcommittee offices (335 Cannon House Office Building and 333 Cannon House Office Building) by the date specified above.

If there are any questions regarding this investigation, please have your staff contact Eric Hannel, Majority Staff Director at (202) 225-3569 and Juan Lara, Minority Staff Director at 202-225-9756.

Mike Coffman
Chairman,
Subcommittee on Oversight and Investigations

Ann Kirkpatrick
Ranking Minority Member
Subcommittee on Oversight and Investigations