Attachment A:
Information Security Questions for Veterans Affairs (VA)

Date: Wednesday, October 23, 2013
Source: House Veterans Affairs Subcommittee on Oversight and Investigations
Scope: The Veterans Benefits, Health Care, and Information Technology Act of 2006

The House Veterans Affairs Subcommittee on Oversight and Investigations is currently examining the roles and responsibilities of VA's Office of Information & Technology (OI&T) in managing its information security initiatives. The Subcommittee is asking that VA answer the questions below designed to gather information regarding their efforts to address applicable federal legislation, standards, and guidance. This work reflects the continuing interest of the Subcommittee in preventing exploitation of Veterans' personally identifiable information (PII) and to improve VA's internal and external cyber security of Veterans' records.

We identified the following as either statutory requirements or as critical to effective information security management of PII and data breaches:

Legislation

- **Attachment A:**
- **The Veterans Benefits, Health Care, and Information Technology Act of 2006**

Attachment B:
Privacy Act of 1974

Attachment C:
The Health Information Technology for Economic and Clinical Health Act (HITECH Act), issued in 2009

OMB Guidance (includes NIST standards and audit controls)

Attachment B:
OMB Memo: Safeguarding Personally Identifiable Information, M-06-15, May 22, 2006

Attachment D:
OMB Memo: Protection of Sensitive Agency Information, M-06-16, June 23, 2006

Attachment E:
OMB Memo: Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, M-06-19, July 12, 2006

Attachment F:
OMB Memo: Recommendations for Identity Theft Related Data Breach Notification, September 20, 2006

Attachment G:
President's Identity Theft Task Force: Combating Identity Theft - A Strategic Plan, April 11, 2007

Attachment H:
OMB Memo: Safeguarding Against and Responding to the Breach of Personally Identifiable Information, M-07-16, May 22, 2007

Attachment I:
Critical Security Controls for Effective Information Security

Federal Legislation:

The Veterans Benefits, Health Care, and Information Technology Act of 2006 – (VBHCIT)
P.L. 109-461; 38 U.S.C. §§5722 et
December 26, 2006

VBHCIT Legislative Requirement:
Title IX of P.L. 109-461, the Veterans Affairs Information Security Act, requires the Department of Veterans Affairs (VA) to implement agency-wide information security procedures to protect the VA's "sensitive personal information" (SPI) and VA information systems. In the event of a "**data breach**" of sensitive personal information processed or maintained by the VA Secretary, the **Secretary** must ensure that, as soon as possible after discovery, either a non-VA entity or the VA's Inspector General conduct an **independent risk analysis of the data breach** to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information.

Based upon the risk analysis, if the **Secretary** determines that a reasonable risk exists of the potential misuse of sensitive personal information, the Secretary must provide **credit protection services**.

1. Since January 2010, the Committee has learned of at least nine foreign breaches to the VA network. For these breaches, did the Secretary ensure that a non-VA entity or the VAOIG conducted an independent risk analysis of each data breach? ☐ Yes ☐ No ☐ Other:
   a. If yes, please describe how this was accomplished. If no, please explain why not:
   b. Documentation available (i.e. policy, guidelines, actual document)? ☐ Yes ☐ No ☐ Other:
   c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

2. Based on the risk analysis, did the Secretary provide credit protection services for the misuse of any personal information? ☐ Yes ☐ No ☐ Other:
   a. If yes, please describe how this was accomplished. If no, please explain why not:
   b. Documentation available (i.e. policy, guidelines, actual document)? ☐ Yes ☐ No ☐ Other:
   c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

VBHCIT Legislative Requirement:
"(b) REGULATIONS.—Not later than 180 days after the date of the enactment of the Veterans Benefits, Health Care, and Information Technology Act of 2006, the **Secretary** shall prescribe interim regulations for the provision of the following in accordance with subsection (a)(2):
"(1) Notification.
"(2) Data mining.
"(3) Fraud alerts.
"(4) Data breach analysis.
"(5) Credit monitoring.
"(6) Identity theft insurance.
"(7) Credit protection services.

3. Has the Secretary issued regulations concerning data breach analysis? ☐ Yes ☐ No ☐ Other:
   a. If yes, please describe how this was accomplished. If no, please explain why not:
   b. Documentation available (i.e. policy, guidelines, actual document)? ☐ Yes ☐ No ☐ Other:
   c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

VBHCIT Legislative Requirement:
"(c) REPORT.—(1) For each data breach with respect to sensitive personal information processed or maintained by the Secretary, **the Secretary** shall promptly submit to the **Committees on Veterans' Affairs** of the Senate and

House of Representatives a **report containing the findings of any independent risk analysis** conducted under subsection (a)(1), any determination of the Secretary under subsection (a)(2), and a description of any services provided pursuant to subsection (b)

4. Has the Secretary promptly submit a report to HVAC containing the findings of each independent risk analysis? ☐ Yes ☐ No ☐ Other:
   a. If yes, please describe how this was accomplished. If no, please explain why not:
   b. Documentation available (i.e. policy, guidelines, actual document)? ☐ Yes ☐ No ☐ Other:
   c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

VBHCIT Legislative Requirement:
"(a) CONTRACT REQUIREMENTS.—If the Secretary enters into a contract for the performance of any Department function that requires access to sensitive personal information, the Secretary shall require as a condition of the contract that—
"(2) the **contractor,** or any subcontractor for a subcontract of the contract, shall promptly **notify the Secretary of any data breach** that occurs with respect to such information.

5. Since January 2010, were VA's IT contractors responsible in any way for any data breaches? ☐ Yes ☐ No ☐ Other:
   a. If yes, please provide additional details. If no, please explain who was, especially for the nine foreign breaches:
   b. Documentation available (i.e. policy, guidelines, actual notification)? ☐ Yes ☐ No ☐ Other:
   c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

6. Did VA's contractors promptly notify the Secretary of any data breaches? ☐ Yes ☐ No ☐ Other:
   a. If yes, please describe how this was accomplished. If no, please explain why not:
   b. Documentation available (i.e. policy, guidelines, actual notification)? ☐ Yes ☐ No ☐ Other:
   c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

7. Of the nine foreign data breaches, who had access to these systems and what type of access was given to the contractors? Click here to enter text.
   a. Documentation available (i.e. policy, guidelines, actual notification)? ☐ Yes ☐ No ☐ Other:
   b. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

VBHCIT Legislative Requirement:
"(b) LIQUIDATED DAMAGES.—Each contract subject to the requirements of subsection (a) shall **provide for liquidated damages to be paid by the contractor to the Secretary** in the event of a data breach with respect to any sensitive personal information processed or maintained by the contractor or any subcontractor under that contract.

8. If VA's contractors were held liable for data breaches, did they end up paying for any liquidated damages? ☐ Yes ☐ No ☐ Other:
   a. If yes, please describe how this was accomplished. If no, please explain why not:
   b. Documentation available (i.e. contractual requirement, policy, guidelines, actual document)? ☐ Yes ☐ No ☐ Other:
   c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

VBHCIT Legislative Requirement:
"(b) ASSISTANT SECRETARY FOR INFORMATION AND TECHNOLOGY.—
The Assistant Secretary for Information and Technology, as the **Chief Information Officer** of the Department, is responsible for the following:
(16) Providing **immediate notice to the Secretary** of any presumptive data breach.

9. Does VA ensure that the CIO provides immediate notice to the VA Secretary of any data breach? ☐ Yes ☐ No ☐ Other:
   a. If yes, please describe how this was accomplished. If no, please explain why not:
   b. Documentation available (i.e. policy, guidelines, actual notice(s) to the Secretary)? ☐ Yes ☐ No ☐ Other:
   c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

10. Since, January 2010, did VA's CIO provide immediate notice to the VA Secretary on any of the nine foreign data breaches? ☐ Yes ☐ No ☐ Other:
   a. If yes, please describe how this was accomplished. If no, please explain why not:
   b. Documentation available (i.e. policy, guidelines, actual notice(s) to the Secretary)? ☐ Yes ☐ No ☐ Other:
   c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

VBHCIT Legislative Requirement:
"§ 5726. Reports and notice to Congress on data breaches
"(a) **QUARTERLY REPORTS.—(**1) Not later than 30 days after the last day of a fiscal quarter, the **Secretary** shall submit to the **Committees on Veterans' Affairs** of the Senate and **House of Representatives** a report on any data breach with respect to sensitive personal information processed or maintained by the Department that occurred during that quarter.

"(2) Each **report** submitted under paragraph (1) shall identify, for each data breach covered by the report—
"(A) the **Administration and facility** of the Department responsible for processing or maintaining the sensitive personal information involved in the data breach; and
"(B) the **status of any remedial or corrective action** with respect to the data breach.

11. Since January 2010, has VA sent quarterly reports to HVAC, including information regarding the nine foreign entity data breaches? ☐ Yes ☐ No ☐ Other:
   a. If yes, please describe how this was accomplished. If no, please explain why not:
   b. Documentation available (i.e. policy, guidelines, quarterly reports since January 2010)? ☐ Yes ☐ No ☐ Other:
   c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

12. Do the quarterly reports include the administration and facility of the Department responsible for processing or maintaining the sensitive personal information involved in the data breach? ☐ Yes ☐ No ☐ Other:
   a. If yes, please provide additional details. If no, please explain why not:
   b. Documentation available (i.e. policy, guidelines, actual quarterly reports)? ☐ Yes ☐ No ☐ Other:
   c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

13. Do the quarterly reports include the status of any remedial or corrective action(s)? ☐ Yes ☐ No ☐ Other:

a. If yes, please provide additional details. If no, please explain why not:
b. Documentation available (i.e. policy, guidelines, actual quarterly reports)? ☐ Yes ☐ No ☐ Other:
c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

VBHCIT Legislative Requirement:
"(b) NOTIFICATION OF **SIGNIFICANT DATA BREACHES**.—(1) In the event of a **data breach with respect to sensitive personal information** processed or maintained by the Secretary that the Secretary determines is significant, the **Secretary shall provide notice** of such breach to the **Committees on Veterans' Affairs** of the Senate and House of Representatives.

"(3) Notice under paragraphs (1) and (2) shall be provided promptly following the discovery of such a data breach and the implementation of any measures necessary to determine the **scope of the breach**, **prevent any further breach** or unauthorized disclosures, and reasonably **restore the integrity of the data system**.

14. Please define and provide the criteria for a "significant data breach". Click here to enter text.
    a. Documentation available (i.e. policy, guidelines, actual notifications)? ☐ Yes ☐ No ☐ Other:
    b. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

15. Has the Secretary sent a notification of these significant data breaches to HVAC? ☐ Yes ☐ No ☐ Other:
    a. If yes, please provide additional details. If no, please explain why not:
    b. Documentation available (i.e. policy, guidelines, actual notifications)? ☐ Yes ☐ No ☐ Other:
    c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

16. Since January 2010, did the Secretary send a notification to HVAC after the nine foreign entity data breaches? ☐ Yes ☐ No ☐ Other:
    a. If yes, please provide additional details. If no, please explain why not:
    b. Documentation available (i.e. policy, guidelines, actual notifications)? ☐ Yes ☐ No ☐ Other:
    c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

17. Do these notifications include the following attributes:
    a. Scope of the breach? ☐ Yes ☐ No ☐ Other:
    b. Has VA implemented any measures to prevent any further breach or unauthorized disclosures? ☐ Yes ☐ No ☐ Other:
    c. Has VA implemented measures to reasonably restore the integrity of the data system? ☐ Yes ☐ No ☐ Other:
    d. If yes, please provide additional details for all the above (a-c). If no, please explain why not:
    e. Documentation available (i.e. policy, guidelines, actual notifications)? ☐ Yes ☐ No ☐ Other:
    f. Please provide source of documentation (if necessary, po0int to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

18. How quickly are these notifications sent to HVAC after a data breach has been discovered? Click here to enter text.
    a. Documentation available (i.e. policy, guidelines, actual notifications)? ☐ Yes ☐ No ☐ Other:
    b. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

VBHCIT Legislative Requirement:
"(10) Submitting to the **Committees on Veterans' Affairs** of the Senate and **House of Representatives**, the Committee on Government Reform of the House of Representatives, and the Committee on Homeland Security and Governmental Affairs of the Senate, not later than **March 1** each year, a report on the compliance of the Department with **subchapter III of chapter 35 of title 44**, with the information in such report **displayed in the aggregate and separately for each Administration, office, and facility of the Department.**

19. Since January 2010, has VA submitted their FISMA reports to HVAC, displayed in the aggregate and separately for each Administration, office, and facility of the Department? ☐ Yes ☐ No ☐ Other:
    a. If yes, please describe how this was accomplished. If no, please explain why not:
    b. Documentation available (i.e. policy, guidelines, FISMA reports)? ☐ Yes ☐ No ☐ Other:
    c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

VBHCIT Legislative Requirement:
"(a) **SECRETARY** OF VETERANS AFFAIRS.—In accordance with the provisions of subchapter III of chapter 35 of title 44, the Secretary is responsible for the following:"
'(12) Providing **notice** to the **Director of the Office of Management and Budget**, the **Inspector General of the Department,** and such other Federal agencies as the Secretary considers appropriate of a presumptive data breach of which notice is provided the **Secretary under subsection (b)(16)** if, in the opinion of the Assistant Secretary for Information and Technology, the **breach involves the information of twenty or more individuals**

20. Since January 2010, has the Secretary provided OMB with a notice of a presumptive data breach involving the information of twenty or more individuals? ☐ Yes ☐ No ☐ Other:
    a. If yes, please describe how this was accomplished. If no, please explain why not:
    b. Documentation available (i.e. evidence of CIO's opinion, policy, guidelines, actual notices)? ☐ Yes ☐ No ☐ Other:
    c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

21. Since January 2010, has the Secretary provided VA's OIG with a notice of a presumptive data breach involving the information of twenty or more individuals? ☐ Yes ☐ No ☐ Other:
    a. If yes, please describe how this was accomplished. If no, please explain why not:
    b. Documentation available (i.e. evidence of CIO's opinion, policy, guidelines, actual notices)? ☐ Yes ☐ No ☐ Other:
    c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

22. Since January 2010, has the Secretary provided other federal agencies with a notice of a presumptive data breach involving the information of twenty or more individuals? ☐ Yes ☐ No ☐ Other:
    a. If yes, please list the other agencies and why they received the notice. If no, please explain why not:
    b. Documentation available (i.e. evidence of CIO's opinion, policy, guidelines, actual notices)? ☐ Yes ☐ No ☐ Other:
    c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

VBHCIT Legislative Requirement:
"(e**) OTHER KEY OFFICIALS**.—In accordance with the provisions of subchapter III of chapter 35 of title 44, the **Under Secretaries, Assistant Secretaries, and other key officials** of the Department are responsible for the following:
"(3) Providing a **plan of action and milestones** to the **Assistant Secretary for Information and Technology** on at least a **quarterly basis** detailing the **status of actions being taken to correct any security compliance failure** or policy violation.

"(16) **PLAN OF ACTION AND MILESTONES**.—The term 'plan of action and milestones', means a plan used as a **basis for the quarterly reporting requirements of the Office of Management and Budget** that includes the following information:
"(A) A description of the security weakness.'
'(B) The identity of the office or organization responsible for resolving the weakness.
"(C) An estimate of resources required to resolve the weakness by fiscal year.
"(D) The scheduled completion date.
"(E) Key milestones with estimated completion dates.
"(F) Any changes to the original key milestone date.
"(G) The source that identified the weakness.
"(H) The status of efforts to correct the weakness.

23. Have other key VA officials provided the CIO with a plan of action and milestones on at least a quarterly basis detailing the status of actions being taken to correct any security compliance failure or policy violation? ☐ Yes ☐ No ☐ Other:
    a. If yes, please describe how this was accomplished. If no, please explain why not:
    b. Documentation available (i.e. policy, guidelines, actual plan of action and milestones)? ☐ Yes ☐ No ☐ Other:
    c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

24. Have other key VA officials provided the CIO with a plan of action and milestones for each of the nine foreign entity breaches? ☐ Yes ☐ No ☐ Other:
    a. If yes, please describe how this was accomplished. If no, please explain why not:
    b. Documentation available (i.e. policy, guidelines, actual plan of action and milestones)? ☐ Yes ☐ No ☐ Other:
    c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

25. How often does VA provide OMB with their plan of action and milestones? Click here to enter text.
    a. Does OMB review and provide comments to VA regarding this document? ☐ Yes ☐ No ☐ Other:
    b. Documentation available (i.e. policy, guidelines, actual plan of action and milestones)? ☐ Yes ☐ No ☐ Other:
    c. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

26. Does VA's plan of action and milestones include the following attributes:
    a. A description of the security weakness? ☐ Yes ☐ No ☐ Other:
    b. The identity of the office or organization responsible for resolving the weakness? ☐ Yes ☐ No ☐ Other:
    c. An estimate of resources required to resolve the weakness by fiscal year? ☐ Yes ☐ No ☐ Other:
    d. The scheduled completion date? ☐ Yes ☐ No ☐ Other:
    e. Key milestones with estimated completion dates? ☐ Yes ☐ No ☐ Other:
    f. Any changes to the original key milestone date? ☐ Yes ☐ No ☐ Other:
    g. The source that identified the weakness? ☐ Yes ☐ No ☐ Other:
    h. The status of efforts to correct the weakness? ☐ Yes ☐ No ☐ Other:

i. Documentation available (i.e. policy, guidelines, actual plan of action and milestones)? ☐ Yes ☐ No ☐ Other:
j. Please provide source of documentation (if necessary, point to specific pages): ☐ VA will provide ☐ VA website ☐ Other:

Additional Document Request:
Taken from FCW's May 30, 2013 article:
"What's wrong with Veterans Affairs?"

27. According to the article, in December 2012, Deloitte provided VA's OIT with an in-depth formal report of their operations, management, and organizational structure.
    a. What was the impetus for the report being commissioned? Click here to enter text.
    b. Please provide the Subcommittee with a copy of the report.

The Subcommittee would like to thank VA for taking the time to answer our questions. In case we have additional questions, for each attachment, provide a point of contact(s) or person(s) responsible for filling out the above. If you have any questions, please contact Ashfaq Huda, 202.225.6624, ashfaq.huda@mail.house.gov. Please return your responses along with all supporting documentation required to verify the satisfaction of our questions by **Wednesday, November 6, 2013**. We do not expect VA to generate any new documentation for this response. **Attachment A** and associated documents can be submitted via email to Ashfaq, or you may send it via cd to the following address:

Ashfaq Huda
Senior Professional Staff Member
Subcommittee on Oversight and Investigations
House Committee on Veterans' Affairs
335 Cannon House Office Building
Washington, D.C. 20515