

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

Date: Friday, October 25, 2013

Source: House Veterans Affairs Subcommittee on Oversight and Investigations

Scope: The Privacy Act of 1974 and OMB Memo: Safeguarding Personally Identifiable Information, M-06-15, May 22, 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:	Date Sent: Wednesday, October 23, 2013	Date Due: Wednesday, November 6, 2013
The Veterans Benefits, Health Care, and Information Technology Act of 2006		

Attachment B:	Date Sent: Friday, October 25, 2013	Date Due: Friday, November 8, 2013
Privacy Act of 1974		

Attachment C:	Date Sent: Monday, October 28, 2013	Date Due: Monday, November 11, 2013
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:	Date Sent: Friday, October 25, 2013	Date Due: Friday, November 8, 2013
OMB Memo: Safeguarding Personally Identifiable Information, M-06-15, May 22, 2006		

Attachment D:	Date Sent: Tuesday, October 29, 2013	Date Due: Tuesday, November 12, 2013
OMB Memo: Protection of Sensitive Agency Information, M-06-16, June 23, 2006		

Attachment E:	Date Sent: Wednesday, October 30, 2013	Date Due: Wednesday, November 13, 2013
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:	Date Sent: Thursday, October 31, 2013	Date Due: Thursday, November 14, 2013
OMB Memo: Recommendations for Identity Theft Related Data Breach Notification, September 20, 2006		

Attachment G:	Date Sent: Friday, November 1, 2013	Date Due: Friday, November 15, 2013
President's Identity Theft Task Force: Combating Identity Theft - A Strategic Plan, April 11, 2007		

Attachment H:	Date Sent: Tuesday, November 5, 2013	Date Due: Tuesday, November 19, 2013
OMB Memo: Safeguarding Against and Responding to the Breach of Personally Identifiable Information, M-07-16, May 22, 2007		

Attachment I:	Date Sent: Wednesday, November 6, 2013	Date Due: Wednesday, November 20, 2013
Critical Security Controls for Effective Information Security		

Federal Legislation:

Privacy Act of 1974

5 U.S.C. 552a

Privacy Act Legislative Requirement:

The Act guarantees three primary rights:

- The right to see records about yourself.
- The right to amend that record if it is inaccurate, irrelevant, untimely, or incomplete.
- **The right to sue the federal government if it violates the statute, for example, allowing unauthorized individuals' access to your records**

1. Since January 2010, has VA notified all individuals who had their data breached? Yes No Other:
 - a. If yes, please describe the formal process for doing so. 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:
2. Has the VA ever been sued for allowing unauthorized individuals' access to Veterans' records? Yes No Other:
 - a. If yes, please provide additional information (i.e. dates, type of breach, persons involved, outcome etc.).
 - b. Documentation available (i.e. policy, guidelines, actual documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

Privacy Act Legislative Requirement:

Establish Rules of Conduct:

Agencies are required to establish "rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of [the Privacy Act], including any other rules and procedures adopted pursuant to [the Privacy Act] and the penalties for noncompliance." (5 U.S.C. § 552a(e)(9))

3. Has the VA established rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records? Yes No Other:
 - a. If yes, please describe these rules. If no, please explain why not:
 - b. Documentation available (i.e. policy, guidelines, actual rules of conduct)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

Privacy Act Legislative Requirement:

Establish Safeguards:

To determine whether notification of a breach is required, the agency should first **assess the likely risk of harm caused by the breach** and then **assess the level of risk**. Agencies should **consider a wide range of harms, such as harm to reputation and the potential for harassment or prejudice**, particularly when health or financial benefits information is involved in the breach. Agencies are also required to **"establish appropriate administrative, technical, and physical safeguards** to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained."

4. To determine whether a notification of a breach is required, does VA first assess the likely risk of harm caused by the breach? Yes No Other:
 - a. If yes, please describe the criteria and various types of harm. If no, please explain why not:

- b. Does VA's assessment consider harm to reputation? Yes No Other:
 - c. Does VA's assessment consider potential for harassment or prejudice? Yes No Other:
 - d. Documentation available (i.e. policy, guidelines, actual risk of harm assessment)? Yes No Other:
 - e. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
5. After assessing the likely risk of harm, does VA assess the level of risk for each breach? Yes No Other:
- a. If yes, please describe the criteria and levels of risk. If no, please explain why not:
 - b. Documentation available (i.e. policy, guidelines, actual level of risk assessment)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
6. Has VA established appropriate administrative, technical and physical safeguards to insure the security and confidentiality of their records? Yes No Other:
- a. If yes, please describe each of the safeguards and how they are used. If no, please explain why not:
 - b. Documentation available (i.e. policy, guidelines, descriptions of all safeguards)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

Privacy Act Legislative Requirement:

Maintain accurate, relevant, timely and complete information:

The Privacy Act also requires **personally identifiable information within a system of records to be maintained in a manner that is accurate, relevant, timely, and complete** including through the **use of notices to the public**. It is important for agencies to fulfill their responsibilities with respect to identifying systems of records and developing and publishing notices as required by the Privacy Act and OMB's implementing policies. By collecting only the information necessary and managing it properly, agencies can often reduce the volume of information they possess, the risk to the information, and the burden of safeguarding it.

7. Does VA maintain PII within a system of records in an accurate, relevant, timely and complete manner? Yes No Other:
- a. If yes, please describe how this was accomplished. If no, please explain why not:
 - b. If yes, did VA provide notices to the public? Yes No Other:
 - c. Documentation available (i.e. policy, guidelines, actual rules of conduct, notice to the public)? Yes No Other:
 - d. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

Privacy Act Legislative Requirement:

In order to ensure an agency is in the best position to respond in a timely and effective manner, in accordance with 5 U.S.C. § 552a(b)(3) of the Privacy Act, agencies should **publish a routine use for appropriate systems specifically applying to the disclosure of information** in connection with response and remedial efforts in the event of a data breach as follows:

To appropriate agencies, entities, and persons when

- (1) [the agency] suspects or has **confirmed** that the security or confidentiality of information in the system of **records has been compromised**;
- (2) the Department has determined that as a result of the suspected or confirmed compromise **there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system** or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and
- (3) the disclosure made to such agencies, entities, and persons **is reasonably necessary to assist in connection with the Department’s efforts to respond to the suspected or confirmed compromise** and prevent, minimize, or remedy such harm.

- 8. In the event of a data breach, does VA publish a routine use in connection with their response and remedial efforts? Yes No Other:
 - a. If yes, please describe the criteria used for publishing a routine use. If no, please explain why not:
 - b. Specifically, does VA publish a routine use for the disclosure of information when:
 - a. [the agency] suspects or has confirmed that the security of information in the system of records has been compromised? Yes No Other:
 - b. the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic interests, identity theft, or harm to the security of this system or other systems that rely upon the compromised information? Yes No Other:
 - c. it is reasonably necessary to assist in connection with the Department’s efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm? Yes No Other:
 - c. Documentation available (i.e. policy, guidelines, actual routine of use)? Yes No Other:
 - d. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

OMB Memorandum:
Safeguarding Personally Identifiable Information, M-06-15
May 22, 2006

Overview of OMB’s Memorandum:

Please have your agency’s Senior Official for **Privacy conduct a review of your policies and processes, and take corrective action as appropriate** to ensure your agency has adequate safeguards to prevent the intentional or negligent misuse of, or unauthorized access to, personally identifiable information. This **review shall address all administrative, technical, and physical means used by your agency to control such information**, including but not limited to procedures and restrictions on the use or removal of personally identifiable information beyond agency premises or control.

- 9. Has VA conducted a review of its policies and processes, and taken appropriate corrective action to ensure it has adequate safeguards to prevent the intentional or negligent misuse of personally identifiable information? Yes No Other:
 - a. If yes, please describe the review and the corrective actions taken. If no, please explain why not:
 - b. Does the review address the following means to control such information:
 - a. Administrative means? Yes No Other:
 - b. Technical means? Yes No Other:
 - c. Physical means? Yes No Other:

- c. Does VA have policy or mechanisms in place to encrypt VA records? Yes No Other:
- d. If yes, please describe the scope and how VA encrypts their records. If no, please explain why not:
- e. Documentation available for 'a', 'b', and 'c' (i.e. policy, guidelines, actual administrative, technical, and physical review, corrective actions, encryption procedures)? Yes No Other:
- f. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

10. Has VA implemented the following information security controls:

- a. Identified and deployed solutions to encrypt sensitive data? Yes No Other:
- b. Resolved clear text protocol vulnerabilities? Yes No Other:
- c. Deployed laptop and thumb drive encryption? Yes No Other:
- d. Encrypted VA databases? Yes No Other:
- e. For each, if yes, please provide additional information. For each, if no, please explain why not:
- f. Documentation available for 'a', 'b', 'c', and 'd' (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
- g. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

11. Does VA provide oversight to prevent privacy violations of VA records? Yes No Other:

- a. If yes, please describe how this oversight is accomplished. If no, please explain why not:
- b. Documentation available (i.e. policy, guidelines, case studies or examples, actual privacy evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

12. Does VA monitor employees for possible privacy violations of VA records? Yes No Other:

- a. If yes, please describe how this is being accomplished. If no, please explain why not:
- b. In cases where VA found privacy violations, what were the consequences for the perpetrator(s)? [Click here to enter text.](#)
- c. Documentation available for 'a' and 'b' (i.e. policy, guidelines, case studies or examples, actual privacy evidentiary documents)? Yes No Other:
- d. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

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 **Friday, November 8, 2013**. We do not expect VA to generate any new documentation for this response. **Attachment B** 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
