

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

Date: Thursday, October 31, 2013

Source: House Veterans Affairs Subcommittee on Oversight and Investigations

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

The House Veterans Affairs Subcommittee on Oversight and Investigations is currently examining the roles and responsibilities of VA's Office of Information and 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		

OMB Memorandum:

Recommendations for Identity Theft Related Data Breach Notification

Issued on September 20, 2006

Overview of Recommendations:

II. Data Breach Planning:

(1) Agencies should immediately **identify a core response group** that can be convened in the event of a breach;

In addition, the memorandum provides a menu of steps for an agency to consider, so that it may pursue a risk-based, tailored response.

1. Since January 2010, how many incidents or breaches have occurred to the VA network? [Click here to enter text.](#)
 - a. How many of these incidents were the result of criminal activity? [Click here to enter text.](#)
 - b. How many of these incidents were by foreign entities? [Click here to enter text.](#)
 - c. Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
 - d. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

2. Since January 2010, for each incident, please describe the type of information that was potentially compromised (i.e. SSNs, bank account numbers, passwords, DOB etc.): [Click here to enter text.](#)
 - a. How many of these incidents were the result of criminal activity? [Click here to enter text.](#)
 - b. How many of these incidents were by foreign entities? [Click here to enter text.](#)
 - c. Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
 - d. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

3. Since January 2010, has VA utilized a core response group after every breach? Yes No Other:
 - a. If yes, please provide additional detail on how this is being accomplished. If no, please explain why not:
 - b. Documentation available (i.e. policy, guidelines, core response group members, actual evidentiary documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

4. Did VA identify a core response group after each of the nine foreign entity breaches? Yes No Other:
 - a. If yes, please provide additional detail on how this is being accomplished. If no, please explain why not:
 - b. Documentation available (i.e. policy, guidelines, description of roles and responsibilities, core response group members, actual evidentiary documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

5. Does VA's core response group include the following members:
 - a. Chief Information Officer? Yes No Other:
 - b. Chief Legal Officer? Yes No Other:
 - c. Chief Privacy Officer? Yes No Other:
 - d. Senior management official from VA? Yes No Other:
 - e. Inspector General? Yes No Other:
 - f. Communications? Yes No Other:
 - g. Legislative affairs? Yes No Other:
 - h. Budget and procurement official? Yes No Other:

- i. Documentation available (i.e. policy, guidelines, list of members, actual evidentiary documents)? Yes No Other:
 - j. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
6. How often does this group convene and what issues are discussed? [Click here to enter text.](#)
- a. Documentation available (i.e. policy, guidelines, charter, meeting notes, actual evidentiary documents)? Yes No Other:
 - b. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

Overview of Recommendations:

III. Identifying an Incident That Presents Identity Theft Risk and the Level of Risk Involved:

(2) If an incident occurs, the core response group should engage in a **risk analysis** to determine whether the incident poses problems related to identity theft;

- **how easy or difficult it would be for an unauthorized person to access the covered information** in light of the manner in which the covered information was protected;
- **the means by which the loss occurred**, including whether the incident might be the result of a criminal act or is likely to result in criminal activity;
- the **ability of the agency to mitigate** the identity theft; and
- evidence that the compromised information is actually being used to commit identity theft.

7. After an incident occurs, did VA's core response group engage in a risk analysis to determine whether the incident poses problems related to identity theft? Yes No Other:
- a. If yes, please provide additional detail on how this is being accomplished. If no, please explain why not:
 - b. If yes, how many times did VA perform a risk analysis? [Click here to enter text.](#)
 - c. If yes, how many incidents posed a problem related to identity theft? [Click here to enter text.](#)
 - d. Documentation available for 'a', 'b', and 'c' (i.e. policy, guidelines, risk analysis, criteria for a risk analysis, process to determine threat to identity theft, actual evidentiary documents)? Yes No Other:
 - e. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
8. How does VA assess the risk of identity theft from a data compromise? [Click here to enter text.](#)
- a. Documentation available (i.e. policy, guidelines, risk assessment, actual evidentiary documents)? Yes No Other:
 - b. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
9. In determining the level of risk of identity theft, an agency should consider not simply the data that was compromised, but all of the circumstances of the data loss. Does VA consider the following, including:
- a. How easy or difficult it would be for an unauthorized person to access the covered information (information posing a risk of identity theft) in light of the manner in which the covered information was protected (i.e. information on a computer laptop that is adequately protected by encryption is less likely to be accessed, while "hard copies" of printed-out data are essentially unprotected)? Yes No Other:
 - b. The means by which the loss occurred, including whether the incident might be the result of a criminal act or is likely to result in criminal activity? Yes No Other:
 - c. The ability of the VA to mitigate the identity theft (i.e. if the compromised information relates to disability beneficiaries, the agency can monitor its beneficiary database for requests for change of address, which may signal attempts to misuse the information, and take steps to prevent the fraud)? Yes No Other:
 - d. Evidence that the compromised information is actually being used to commit identity theft? Yes No Other:

- e. For each, if yes, please provide additional detail on how this is being accomplished. For each, if no, please explain why not:
- f. Documentation available for 'a' - '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:

Overview of Recommendations:

III. Identifying an Incident That Presents Identity Theft Risk and the Level of Risk Involved:

(3) If it is determined that an identity theft risk is present, the **agency should tailor its response** (which may include **advice** to those potentially affected, **services the agency may provide** to those affected, and **public notice**) to the **nature and scope** of the risk presented.

- 10. If it is determined that a risk of identity theft is present, does VA perform the following (see also question 24):
 - a. Describe the nature and scope of the risk? Yes No Other:
 - b. Provide advice to those potentially affected? Yes No Other:
 - c. List of services to those affected? Yes No Other:
 - d. Issue a public notice? Yes No Other:
 - e. For each, if yes, please provide additional detail on how this is being accomplished. For each, if no, please explain why not:
 - f. Documentation available for 'a' - '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:

Overview of Recommendations:

IV. Reducing Risk After Disclosure

While assessing the level of risk in a given situation, the **agency should simultaneously consider options for attenuating that risk**. It is important in this regard for the agency to understand certain standard options available to agencies and individuals to help protect potential victims.

A. Actions that Individuals Can Routinely Take

B. Actions that Agencies Can Take

- 11. Does VA utilize technologies to analyze whether a particular data loss appears to be resulting in identity theft (this data breach analysis may be a useful intermediate protective action, especially where the agency is uncertain about whether the identity-theft risk warrants implementing more costly additional steps such as credit monitoring)? Yes No Other:
 - a. If yes, please provide additional detail on how this is being accomplished. If no, please explain why not and whether you plan on doing so in the future:
 - b. Documentation available (i.e. policy, guidelines, screenshots, actual evidentiary documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
- 12. What type of data breach analysis does VA perform? [Click here to enter text.](#)
 - a. If yes, please provide additional detail on how this is being accomplished. If no, please explain why not and whether you plan on doing so in the future:
 - b. Documentation available (i.e. policy, guidelines, data breach analysis, actual evidentiary documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

13. Does VA determine whether the particular incident it has suffered is truly a source of identity theft, or whether, instead, any such reports are the normal by-product of the routine incidence of identity theft? Yes No Other:
- a. If yes, please provide additional detail on how this is being accomplished. If no, please explain why not and whether you plan on doing so in the future:
 - b. Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
14. For how many individuals has VA provided credit monitoring services? [Click here to enter text.](#)
- a. If yes, please provide additional detail on how this is being accomplished. If no, please explain why not:
 - b. Documentation available (i.e. policy, guidelines, criteria for offering credit monitoring, credit offering features, actual evidentiary documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
15. Does VA have criteria in place for deciding whether to offer credit monitoring services? Yes No Other:
- a. If yes, please describe the criteria. If no, please explain why not and whether you plan on doing so in the future:
 - b. Documentation available (i.e. policy, guidelines, criteria for offering credit monitoring, credit offering features, cost, length of time, actual evidentiary documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
16. How long does it take VA to offer credit monitoring services after an incident is reported and PII is deemed at risk? [Click here to enter text.](#)
- a. If yes, please provide additional detail on how this is being done.
 - b. Documentation available (i.e. policy, guidelines, criteria for offering credit monitoring, length of time, actual evidentiary documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
17. Does VA notify law enforcement to mitigate the risks faced by the potentially affected individuals? Yes No Other:
- a. If yes, please describe how this is done. If no, please explain why not and whether you plan on doing so in the future:
 - b. Documentation available (i.e. policy, guidelines, notifications, actual evidentiary documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

Overview of Recommendations:

V. Implementing a Response Plan: Notice to Those Affected

Assuming that an agency has made the decision to **provide notice to those put at risk**, agencies should **incorporate the following elements** into that notification process:

- Timing
- Source
- Contents
- Method of Notification
- Preparing for follow-on inquiries
- Prepare counterpart entities that may receive a surge in inquiries

18. **Timing:** Does VA ensure that their notices to those put at risk are provided in a timely manner? Yes No
 Other:
- a. If yes, please describe how this is done. If no, please explain why not and whether you plan on doing so in the future:
- b. Documentation available (i.e. policy, guidelines, notifications, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
19. **Timing:** Do VA officials consult with law enforcement officials investigating the incident (which could include the VA's Inspector General) regarding the timing and content of any announcement, before making any public disclosures about the incident? Yes No Other:
- a. If yes, please describe how this is done. If no, please explain why not and whether you plan on doing so in the future:
- b. Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
20. **Timing:** If a VA data breach resulted from a failure in a security or information system, was that system repaired and tested before disclosing details related to the incident? Yes No Other:
- a. If yes, please describe how this is done. If no, please explain why not and whether you plan on doing so in the future:
- b. Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
21. **Source:** Who within VA provides the notification to the affected individuals? [Click here to enter text.](#)
- a. If yes, please describe how this is done.
- b. Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
22. **Source:** Who within VA provides the notification to the affected individuals? [Click here to enter text.](#)
- a. If yes, please describe how this is done and the criteria used to determine the sender (i.e. contractor, responsible official, responsible team etc.).
- b. Documentation available (i.e. policy, guidelines, notification procedures, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
23. **Source:** Does VA ensure that its contractor or partner promptly notifies them of any data loss it suffers? Yes No Other:

- a. If yes, please describe how this is done. If no, please explain why not and whether you plan on doing so in the future:
- b. Documentation available (i.e. policy, guidelines, contractor notification procedures, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

24. **Contents:** Does VA's notice include the following elements:

- a. Capable of individual distribution and/or posting on the agency's website and other information sites? Yes No Other:
- b. A brief description of what happened? Yes No Other:
- c. A description of the types of personal information that were involved in the data security breach (i.e., full name, SSN, date of birth, home address, account number, disability code, etc.)? Yes No Other:
- d. A brief description of what the agency is doing to investigate the breach? Yes No Other:
- e. A brief description of what the agency is doing to mitigate losses? Yes No Other:
- f. A brief description of what the agency is doing to protect against any further breaches? Yes No Other:
- g. Contact procedures for those wishing to ask questions or learn additional information? Yes No Other:
 - a. Including a toll-free telephone number? Yes No Other:
 - b. Including a website? Yes No Other:
 - c. Including a postal address? Yes No Other:
- h. Steps individuals should take to protect themselves from the risk of identity theft? Yes No Other:
- i. Steps to take advantage of any credit monitoring or other service the agency intends to offer? Yes No Other:
- j. Contact information for the FTC website, including specific publications? Yes No Other:
- k. For each, if yes, please describe how this is done. If no, please explain why not and whether you plan on doing so in the future:
- l. Documentation available (i.e. policy, guidelines, notices to individuals affected, actual evidentiary documents)? Yes No Other:
- m. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

25. **Contents:** If VA has knowledge that the affected individuals are not English speaking, are the notices provided in the appropriate language? Yes No Other:

- a. If yes, please describe how this is done. If no, please explain why not and whether you plan on doing so in the future:
- b. Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

26. **Method of Notification:** Does VA use first-class mail notification to the last known mailing address of the individual as the primary means of notification? Yes No Other:

- a. If yes, please describe how this is done. If no, please explain why not and whether you plan on doing so in the future:
- b. Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

27. **Method of Notification:** Does VA use any other substitute means of notice? Yes No Other:
- If yes, broad public announcement through the media? Yes No Other:
 - If yes, website announcements? Yes No Other:
 - If yes, distribution to public service and other membership organizations likely to have access to the affected individual class? Yes No Other:
 - If yes, email notification? Yes No Other:
 - If yes, please describe how this is done and how many of each have been sent. If no, please explain why not and whether you plan on doing so in the future:
 - Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
28. **Method of Notification:** Does VA give special consideration in providing notice to individuals who are visually or hearing impaired consistent with Section 504 of the Rehabilitation Act of 1973? Yes No Other:
- If yes, please describe how this is done (Telecommunications Device for the Deaf (TDD) or posting a large-type notice on the agency's web site). If no, please explain why not and whether you plan on doing so in the future:
 - Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
29. **Preparing for follow-on inquiries:** How does VA prepare for follow-on inquiries? [Click here to enter text.](#)
- If no, please explain why not and whether you plan on doing so in the future:
 - Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
30. **Preparing for follow-on inquiries:** Does VA use GSA's stand-by capability through its "USA Services" operation? Yes No Other:
- If yes, please describe how this is done. If no, please explain why not and whether you plan on doing so in the future:
 - Documentation available (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
31. **Prepare counterpart entities that may receive a surge in inquiries:** For large incidents, including the nine foreign entity breaches, does VA inform the credit bureaus and the FTC of the timing and distribution of any notices, as well as the number of affected individuals, in order to prepare? Yes No Other:
- If yes, please describe how this is done. If no, please explain why not and whether you plan on doing so in the future:
 - Documentation available (i.e. policy, guidelines, notices to credit bureaus, actual evidentiary documents)? Yes No Other:
 - 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 **Thursday, November 14, 2013**. We do not expect VA to generate any new documentation for this response. **Attachment F** 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
