

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

Date: Wednesday October 30, 2013

Source: House Veterans Affairs Subcommittee on Oversight and Investigations

Scope: 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

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:

Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments, M-06-19 Issued on July 12, 2006

Overview of OMB's Memorandum:

- ❖ Federal Information Security Management Act of 2002 requires all agencies to **report security incidents to a Federal incident response center**. The center (US-CERT) is located within the Department of Homeland Security. The specific reporting procedures are found in the concept of operations for US-CERT.
- ❖ This memorandum revises those reporting procedures to now require agencies to **report all incidents** involving personally identifiable information to US-CERT **within one hour of discovering the incident**.
- ❖ Agencies should report all incidents involving personally identifiable information **in electronic or physical form** and **should not distinguish between suspected and confirmed breaches**.

1. Does VA report **all** incidents involving personally identifiable information to US-CERT within one hour of discovering the incident? 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 does VA ensure that that the incidents are sent within one hour to US-CERT? [Click here to enter text.](#)
 - c. Documentation available for 'a' and 'b' (i.e. policy, guidelines, reports to US-CERT, timestamps, 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. Does VA report all incidents involving PII in:
 - a. Electronic form? Yes No Other:
 - b. Physical form? Yes No Other:
 - c. For each, if yes, please provide additional detail on how this is being accomplished. For each, if no, please explain why not:
 - a. Documentation available for 'a' and 'b' (i.e. policy, guidelines, actual evidentiary documents)? Yes No Other:
 - b. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
3. Does VA distinguish between suspected and confirmed breaches? Yes No Other:
 - a. If yes, please explain why: [Click here to enter text.](#)
 - b. Documentation available (i.e. policy, guidelines, criteria for breaches, 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. Does VA's incident report include the following attributes:
 - a. Agency name? Yes No Other:
 - b. Point of contact information including:
 - a. Name? Yes No Other:
 - b. Telephone? Yes No Other:
 - c. Email address? Yes No Other:
 - c. Incident Category Type (e.g., CAT 1, CAT 2, etc.)? Yes No Other:
 - d. Incident date? Yes No Other:

- e. Incident time, including time zone? Yes No Other:
- f. Source IP? Yes No Other:
- g. Source port? Yes No Other:
- h. Source protocol? Yes No Other:
- i. Destination IP? Yes No Other:
- j. Destination port? Yes No Other:
- k. Destination protocol? Yes No Other:
- l. Operating System? Yes No Other:
- a. Including version? Yes No Other:
- b. Patches? Yes No Other:
- m. System Function (e.g., DNS/web server, workstation, etc.)? Yes No Other:
- n. Antivirus software installed? Yes No Other:
- a. Including version? Yes No Other:
- b. Latest updates? Yes No Other:
- o. Location of the system(s) involved in the incident (e.g., Washington DC, Los Angeles, CA)? Yes No Other:
- p. Method used to identify the incident (e.g., IDS, audit log analysis, system administrator)? Yes No Other:
- q. Impact to agency? Yes No Other:
- r. Resolution? Yes No Other:
- s. Documentation available (i.e. policy, guidelines, actual incident reports)? Yes No Other:
- t. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
5. Did VA provide an incident report to US-CERT for each of the nine foreign breaches to the VA network? Yes No Other:
- a. If yes, please provide additional detail on how this was accomplished. If no, please explain why not:
- b. If yes, were the incident reports sent to US-CERT within one hour? Yes No Other:
- a. If no, please explain why:
- c. Documentation available for 'a' and 'b' (i.e. policy, guidelines, reports to US-CERT, timestamps, actual evidentiary documents)? Yes No Other:
- d. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
6. Since January 2010, how many incidents did VA report as:
- a. Category 0 - Exercise/Network Defense Testing? [Click here to enter text.](#)
- b. Category 1 - Unauthorized Access? [Click here to enter text.](#)
- c. Category 2 - Denial of Service (DoS)? [Click here to enter text.](#)
- d. Category 3 - Malicious Code? [Click here to enter text.](#)
- e. Category 4 - Improper Usage? [Click here to enter text.](#)
- f. Category 5 - Scans/Probes/Attempted Access? [Click here to enter text.](#)
- g. Category 6 - Investigation? [Click here to enter text.](#)
- h. Documentation available (i.e. policy, guidelines, VA's incident and event categories, reporting criteria, actual evidentiary documents)? Yes No Other:
- i. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
7. Does VA utilize US-CERT's incident and event categories and reporting timeframe criteria for reporting all incidents? 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, VA's incident and event categories, reporting criteria, actual evidentiary documents)? Yes No Other:
- c. 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 **Wednesday, November 13, 2013**. We do not expect VA to generate any new documentation for this response. **Attachment E** 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
