

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

Date: Friday, November 1, 2013

Source: House Veterans Affairs Subcommittee on Oversight and Investigations

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

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		

President's Identity Theft Task Force:

Combating Identity Theft - A Strategic Plan

April 11, 2007

Overview of Recommendations:

Establishing a Data Breach Policy for the Public Sector

The Task Force has developed and formally **approved a set of guidelines**

Improving Data Security in the Public Sector

Task Force recommends that the ISS LOB (OMB and DHS) should

(a) outline best practices in the area of automated tools, training, processes, and standards that would enable agencies to improve their security and privacy programs, and

(b) develop a list of the top 10 or 20 "mistakes" to avoid in order to protect information held by the government.

Decreasing the Use of Social Security Numbers by the Public Sector

OMB should require all federal agencies to review their use of SSNs to determine the circumstances under which such use can be eliminated, restricted, or concealed in agency business processes, systems, and paper and electronic forms, other than those authorized or approved by OPM.

Publication of a "Routine Use" for Disclosure of Information Following a Breach

Task Force recommends that all federal agencies, to the extent consistent with applicable law, publish a new "routine use" for their systems of records under the Privacy Act. Publish a "Routine Use" Allowing Disclosure of Information Following a Breach.

Developing Alternate Means of Authenticating Identities

Restitution for Identity Theft Victims

Development of a Universal Police Report

1. Are VA's network security controls able to monitor and prevent the following cyber security threats:
 - a. Keyloggers (programs that record every keystroke as an Internet user logs onto his computer or a banking website)? Yes No Other:
 - b. Spyware (software that covertly gathers user information through the user's Internet connection, without the user's knowledge)? Yes No Other:
 - c. Botnets (networks of computers that criminals have compromised and taken control of for some other purpose, ranging from distribution of spam and malicious computer code to attacks on other computers)? Yes No Other:
 - d. Remote code execution? Yes No Other:
 - e. Malicious code programs? Yes No Other:
 - f. Phishing? Yes No Other:
 - g. For each, if yes, please provide additional detail on how this is being accomplished. For each, if no, please explain why not:
 - h. Documentation available (i.e. policy, guidelines, screenshots, actual evidentiary documents)? Yes No Other:
 - i. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
2. Are VA's application security controls able to monitor and prevent the following cyber security threats:
 - a. Keyloggers (programs that record every keystroke as an Internet user logs onto his computer or a banking website)? Yes No Other:
 - b. Spyware (software that covertly gathers user information through the user's Internet connection, without the user's knowledge)? Yes No Other:

- c. Botnets (networks of computers that criminals have compromised and taken control of for some other purpose, ranging from distribution of spam and malicious computer code to attacks on other computers)? Yes No Other:
- d. Remote code execution? Yes No Other:
- e. Malicious code programs? Yes No Other:
- f. Phishing? Yes No Other:
- g. For each, if yes, please provide additional detail on how this is being accomplished. For each, if no, please explain why not:
- h. Documentation available (i.e. policy, guidelines, screenshots, actual evidentiary documents)? Yes No Other:
- i. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

Overview of Recommendations:

A. Prevention: Keeping Consumer Data Out of the Hands of Criminals

1. Decreasing the Unnecessary Use of Social Security Numbers

a. Safeguarding of Information in the Public Sector

- 3. Since January 2010, has VA taken any steps, internally or with OPM, to proactively decrease the unnecessary use of Veterans' social security numbers? Yes No Other:
 - a. If yes, please provide additional detail on how this was done and the exact decrease in numbers. If no, please explain why not:
 - 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:
- 4. Does VA, internally or with assistance from OPM, perform or utilize the following:
 - a. Issue guidance on the appropriate use of SSNs? Yes No Other:
 - b. Review the use of SSNs? Yes No Other:
 - c. Agency best practices that minimize use of SSNs? Yes No Other:
 - d. Documentation available (i.e. policy, guidelines, best practices, actual evidentiary documents)? Yes No Other:
 - e. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

Overview of Recommendations:

A. Prevention: Keeping Consumer Data Out of the Hands of Criminals

2. Data Security in the Public Sector

a. Safeguarding of Information in the Public Sector

- 5. Please describe the types of training VA has provided to employees for improving the effectiveness of their security programs: [Click here to enter text.](#)
 - a. Documentation available (i.e. policy, guidelines, training plans, information security plan, actual evidentiary documents)? Yes No Other:
 - b. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
- 6. Does VA, review and update existing training programs to reflect the most recent changes, issues, and trends? 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, employee training requirements, changes in training from year to year, 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:

A. Prevention: Keeping Consumer Data Out of the Hands of Criminals

2. Data Security in the Public Sector

b. Responding to Data Breaches in the Public Sector

- **Develop Concrete Guidance and Best Practices**
- **Issue Data Breach Guidance to Agencies**

- 7. Has VA utilized the following:
 - a. In the past, OMB and DHS, through the interagency Information Systems Security Line of Business (ISS LOB) task force, outlined best practices in the area of automated tools, training, processes, and standards that would enable agencies to improve their security and privacy programs. Yes No Other:
 - b. In addition, OMB and DHS developed a list of the most common 10 or 20 “mistakes” to avoid in protecting information held by the government. Yes No Other:
 - c. If yes, please provide additional detail on how this was being accomplished. If no, please explain why not:
 - d. Documentation available (i.e. policy, guidelines, lessons learned, best practices, case studies, 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. Has VA developed and formally approved a data breach policy? Yes No Other:
 - a. If yes, please provide additional detail on how this was done. If no, please explain why not:
 - b. Documentation available (i.e. policy, guidelines, data breach policy, 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:

C. Victim Recovery: Helping Consumers Repair Their Lives

1. Victim Assistance: Outreach and Education

- 9. Has VA developed and issued guidance advising Veterans’ of steps to take if they have become victims of identity theft, or if their personal information has been breached? Yes No Other:
 - a. If yes, please provide additional detail on how this was accomplished. If no, please explain why not:
 - b. Documentation available (i.e. policy, guidelines, data breach policy, 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:

D. Law Enforcement: Prosecuting and Punishing Identity Thieves

2. Coordination with Foreign Law Enforcement

- 10. Because of the international nature of VA’s data breaches, has VA provided assistance to, and received assistance from foreign law enforcement for each of the nine breaches? Yes No Other:
 - a. If yes, please describe the collaboration that occurred during the investigation. If no, please explain why not:

- b. Documentation available (i.e. policy, guidelines, communication, actual evidentiary documents)? Yes
 No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
11. Has VA provided assistance to, and received assistance from federal law enforcement agencies, led by DOJ, FBI, and ICE etc. during the investigation of any of the foreign entity data breaches? Yes No Other:
- a. If yes, please describe the collaboration that occurred during the investigation. If no, please explain why not:
- b. Documentation available (i.e. policy, guidelines, communication, 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 **Friday, November 15, 2013**. We do not expect VA to generate any new documentation for this response. **Attachment G** 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
