

## Attachment D: Information Security Questions for Veterans Affairs (VA)

**Date:** Tuesday, October 29, 2013

**Source:** House Veterans Affairs Subcommittee on Oversight and Investigations

**Scope:** OMB Memo: Protection of Sensitive Agency Information, M-06-16, June 23, 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

<b>Attachment A:</b>	<b>Date Sent:</b> Wednesday, October 23, 2013	<b>Date Due:</b> Wednesday, November 6, 2013
The Veterans Benefits, Health Care, and Information Technology Act of 2006		
<b>Attachment B:</b>	<b>Date Sent:</b> Friday, October 25, 2013	<b>Date Due:</b> Friday, November 8, 2013
Privacy Act of 1974		
<b>Attachment C:</b>	<b>Date Sent:</b> Monday, October 28, 2013	<b>Date Due:</b> 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)

<b>Attachment B:</b>	<b>Date Sent:</b> Friday, October 25, 2013	<b>Date Due:</b> Friday, November 8, 2013
OMB Memo: Safeguarding Personally Identifiable Information, M-06-15, May 22, 2006		
<b>Attachment D:</b>	<b>Date Sent:</b> Tuesday, October 29, 2013	<b>Date Due:</b> Tuesday, November 12, 2013
<b>OMB Memo: Protection of Sensitive Agency Information, M-06-16, June 23, 2006</b>		
<b>Attachment E:</b>	<b>Date Sent:</b> Wednesday, October 30, 2013	<b>Date Due:</b> 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		
<b>Attachment F:</b>	<b>Date Sent:</b> Thursday, October 31, 2013	<b>Date Due:</b> Thursday, November 14, 2013
OMB Memo: Recommendations for Identity Theft Related Data Breach Notification, September 20, 2006		
<b>Attachment G:</b>	<b>Date Sent:</b> Friday, November 1, 2013	<b>Date Due:</b> Friday, November 15, 2013
President's Identity Theft Task Force: Combating Identity Theft - A Strategic Plan, April 11, 2007		
<b>Attachment H:</b>	<b>Date Sent:</b> Tuesday, November 5, 2013	<b>Date Due:</b> Tuesday, November 19, 2013
OMB Memo: Safeguarding Against and Responding to the Breach of Personally Identifiable Information, M-07-16, May 22, 2007		
<b>Attachment I:</b>	<b>Date Sent:</b> Wednesday, November 6, 2013	<b>Date Due:</b> Wednesday, November 20, 2013
Critical Security Controls for Effective Information Security		

# OMB Memorandum:

## Protection of Sensitive Agency Information, M-06-16

Issued on June 23, 2006

### Recommendations within OMB's Memorandum (M-06-16):

In addition to using the NIST checklist, I am **recommending** all departments and agencies take the following actions:

- **Encrypt all data on mobile computers/devices** which carry agency data unless the data is determined to be non-sensitive, in writing, by your Deputy Secretary or an individual he/she may designate in writing;
- **Allow remote access only with two-factor authentication** where one of the factors is provided by a device separate from the computer gaining access;
- **Use a "time-out" function for remote access** and mobile devices requiring user re-authentication after 30 minutes inactivity; and
- **Log all computer-readable data extracts from databases holding sensitive information** and verify each extract including sensitive data has been erased within 90 days or its use is still required.

1. Does VA encrypt all data on mobile computers/devices which carry agency data?  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, actual evidentiary documents)?  Yes  No  Other:
  - c. Please provide source of documentation (if necessary, point to specific pages):  VA will provide  VA website  Other:
2. Does VA allow remote access with only two-factor authentication, where one of the factors is provided by a device separate from the computer gaining access?  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, actual evidentiary documents)?  Yes  No  Other:
  - c. Please provide source of documentation (if necessary, point to specific pages):  VA will provide  VA website  Other:
3. Does VA use a "time-out" function for remote access and mobile devices when requiring user re-authentication after 30 minutes of inactivity?  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, 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 log all computer-readable data extracts from databases holding sensitive information?  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, logs, 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 verify each data extract, ensuring sensitive data had been erased within 90 days or if its use is still required?  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, verifications, 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 OMB's Memorandum:

### Security Checklist:

- This checklist provides specific actions to be taken by federal agencies for the protection of **Personally Identifiable Information (PII)** categorized in accordance with **FIPS 199** as moderate or high impact that is either:
  - **Accessed remotely;** or
  - **Physically transported outside of the agency's secured, physical perimeter** (this includes information transported on removable media and on portable/mobile devices such as laptop computers and/or personal digital assistants).
- The security controls and associated control assessment methods/procedures in this checklist were taken from **NIST Special Publication 800-53**, Recommended Security Controls for Federal Information Systems and **NIST Special Publication 800-53A**, Guide for Assessing the Security Controls in Federal Information Systems (Second Public Draft), April 2006

6. Does VA take actions to protect Veterans' PII, in accordance with FIPS 199, designated as either moderate or high impact, which is accessed remotely?  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, actual evidentiary documents)?  Yes  No  Other:
- c. Please provide source of documentation (if necessary, point to specific pages):  VA will provide  VA website  Other:
7. Does VA take actions to protect Veterans' PII, in accordance with FIPS 199, designated as either moderate or high impact that is physically transported outside of the agency's secured, physical perimeter?  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, actual evidentiary documents)?  Yes  No  Other:
- c. Please provide source of documentation (if necessary, point to specific pages):  VA will provide  VA website  Other:

### STEP 1: Detailed Procedures as described within the Memorandum:

The controls and assessment methods/procedures in the checklist are a subset of what is currently required for moderate and high impact information systems.

### Security Checklist for Personally Identifiable Information that is to Be Transported and/or Stored Offsite, or that is to be Accessed Remotely:

- **STEP 1:** Confirm identification of personally identifiable information protection needs.
    - **Action Item 1.1:** Verify information categorization to ensure identification of personally identifiable information requiring protection when accessed remotely or physically removed.
    - **Action Item 1.2:** Verify existing risk assessment.
8. Does VA ensure all PII through which a moderate or high impact might result have been explicitly identified?  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, privacy impact assessments, security categorizations, actual evidentiary documents)?  Yes  No  Other:
- c. Please provide source of documentation (if necessary, point to specific pages):  VA will provide  VA website  Other:
9. Does VA confirm or modify as needed their existing risk assessment associated with remote access and physical removal of PII?  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, risk assessment update, actual evidentiary documents)?  Yes  No  Other:

- c. Please provide source of documentation (if necessary, point to specific pages):  VA will provide  VA website  Other:

**STEP 2: Detailed Procedures as described within the Memorandum:**

**Security Checklist for Personally Identifiable Information that is to Be Transported and/or Stored Offsite, or that is to be Accessed Remotely:**

- **STEP 2:** Verify adequacy of organizational policy.
  - **Action Item 2.1:** Identify **existing organizational policy** that addresses the information protection needs associated with personally identifiable information that is accessed remotely or physically removed.
  - **Action Item 2.2:** Verify that the **existing organizational policy** adequately addresses the information protection needs associated with personally identifiable information that is accessed remotely or physically removed.
    - For PII **physically removed**:
    - For PII **accessed remotely**:
  - **Action Item 2.3:** **Revise/develop organizational policy** as needed, including steps 3 and 4.

10. **Action Item 2.1:** Does VA *have* existing organizational policy that addresses the information protection needs associated with PII that is accessed:
- a. Remotely?  Yes  No  Other:
  - b. Physically removed?  Yes  No  Other:
  - c. For each, if yes, please provide additional detail on how this is being accomplished. For each, if no, explain why this policy does not exist. **If 'no' for both 'a' and 'b', skip to the next set (Step 3) of questions and explain why this policy does not exist:**
  - d. Documentation available (i.e. policy, guidelines, actual evidentiary documents)?  Yes  No  Other:
  - e. Please provide source of documentation (if necessary, point to specific pages):  VA will provide  VA website  Other:
11. **Action Item 2.2:** Does VA *verify* that their existing organizational policy adequately addresses the information protection needs associated with PII that is accessed:
- a. Remotely?  Yes  No  Other:
  - b. Physically removed?  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:
  - d. Documentation available (i.e. policy, guidelines, actual evidentiary documents)?  Yes  No  Other:
  - e. Please provide source of documentation (if necessary, point to specific pages):  VA will provide  VA website  Other:
12. **Action Item 2.2: For PII removed:** Does the policy explicitly identify the rules for determining whether physical removal is allowed?  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, rules, 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. **Action Item 2.2: For PII removed:** Does VA's policy require the following:
- a. Information to be encrypted?  Yes  No  Other:
  - b. Appropriate procedures are in place to ensure that remote use of this encrypted information does not result in bypassing the protections provided by the encryption?  Yes  No  Other:

- c. Appropriate training is in place to ensure that remote use of this encrypted information does not result in bypassing the protections provided by the encryption?  Yes  No  Other:
  - d. Appropriate accountability measures are in place to ensure that remote use of this encrypted information does not result in bypassing the protections provided by the encryption?  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 13a – 13d (i.e. policy, guidelines, procedures, training manuals, measures, other actual evidentiary documents)?  Yes  No  Other:
  - g. Please provide source of documentation (if necessary, point to specific pages):  VA will provide  VA website  Other:
14. **Action Item 2.2: For PII accessed remotely:** Does VA's policy explicitly identify the rules for determining whether remote access is allowed?  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, rules, 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. **Action Item 2.2: For PII accessed remotely:** When remote access is allowed, does VA's policy require that this access be accomplished via a virtual private network (VPN) connection established using agency-issued authentication certificate(s) or hardware token?  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, 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. **Action Item 2.2: For PII accessed remotely:** When remote access is allowed, does the policy identify the rules for determining whether download and remote storage of the information is allowed? (For example, the policy could permit remote access to a database, but prohibit downloading and local storage of that database.)?  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, rules, 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. **Action Item 2.3:** Is VA's organizational policy revised or developed to fully address the questions posed in the previous action items?  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, access control policy and procedures, security awareness and training policy and procedures, revisions, changes made, actual evidentiary documents etc.)?  Yes  No  Other:
  - c. Please provide source of documentation (if necessary, point to specific pages):  VA will provide  VA website  Other:

**STEP 3: Detailed Procedures as described within the Memorandum:**

**Security Checklist for Personally Identifiable Information that is to Be Transported and/or Stored Offsite, or that is to be Accessed Remotely:**

- **STEP 3:** Implement protections for personally identifiable information **being transported and/or stored offsite.**
  - **Action Item 3.1:** Identify **existing organizational policy** that addresses the information protection needs associated with personally identifiable information that is accessed remotely or physically removed.
  - **Action Item 3.2:** **Verify that the existing organizational policy** adequately addresses the information protection needs associated with personally identifiable information that is accessed remotely or physically removed.

18. **Action Item 3.1:** In those instances where PII is *transported* to a remote site, does VA implement NIST Special Publication 800-53 security controls ensuring that information is transported only in encrypted form?  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, media transport, use of validated cryptography, 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. **Action Item 3.2:** In those instances where PII is being *stored* at a remote site, does VA implement NIST Special Publication 800-53 security controls ensuring that information is stored only in encrypted form?  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, rules of behavior, use of validated cryptography, 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. **Action Item 3.2:** In those instances where PII is being *stored* at a remote site, does VA establish and train users on the rules of behavior and information use that will help prevent unencrypted forms of VA information from being stored on remote components of the information system?  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, rules of behavior, use of validated cryptography, actual evidentiary documents)?  Yes  No  Other:
  - c. Please provide source of documentation (if necessary, point to specific pages):  VA will provide  VA website  Other:

**STEP 4: Detailed Procedures as described within the Memorandum:**

**Security Checklist for Personally Identifiable Information that is to Be Transported and/or Stored Offsite, or that is to be Accessed Remotely:**

- **STEP 4: Implement protections** for remote access to personally identifiable information. **This step is executed when the policy allows remote access to personally identifiable information.** If VA's policy does not allow remote access to PII, skip the questions within this section and explain why this does not exist.
  - **Action Item 4.1:** Implement NIST Special Publication 800-53 security controls requiring **authenticated, virtual private network (VPN) connection.**
  - **Action Item 4.2:** Implement NIST Special Publication 800-53 security controls **enforcing allowed downloading of personally identifiable information.**
  - **Action Item 4.3:** Implement NIST Special Publication 800-53 security controls **enforcing encrypted remote storage of personally identifiable information.**

If remote storage of **personally identifiable information is to be permitted answer Action Item 4.3**, otherwise answer Action Item 4.4.

- **Action Item 4.4:** Implement NIST Special Publication 800-53 security controls **enforcing no remote storage of personally identifiable information.**

21. **Action Item 4.1:** Does VA implement NIST Special Publication 800-53 security controls requiring an authenticated, virtual private network (VPN) connection when allowing remote access to PII?  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, security controls, VPN connection data, 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. **Action Item 4.2:** Does VA implement NIST Special Publication 800-53 security controls enforcing allowed downloading of personally identifiable information to a remote location, for ensuring appropriate downloading?  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, access enforcement, access control, audit monitoring, analysis, and reporting, 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. **Action Item 4.2:** Does VA implement NIST Special Publication 800-53 security controls enforcing allowed downloading of personally identifiable information to a remote location, for ensuring appropriate downloading?  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, access enforcement, access control, audit monitoring, analysis, and reporting, 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. Does VA permit the remote storage of personally identifiable information?  Yes  No  Other:
- a. If yes, (**Action Item 4.3**) does VA Implement NIST Special Publication 800-53 security controls enforcing encrypted remote storage of personally identifiable information?  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, security controls, rules of behavior, information remnants, use of validated cryptography, actual evidentiary documents)?  Yes  No  Other:
- c. Please provide source of documentation (if necessary, point to specific pages):  VA will provide  VA website  Other:
- b. If no, **(Action Item 4.4)** does VA implement NIST Special Publication 800-53 security controls enforcing no remote storage of personally identifiable information?  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, access enforcement, security awareness, 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](mailto:ashfaq.huda@mail.house.gov). Please return your responses along with all supporting documentation required to verify the satisfaction of our questions by **Tuesday, November 12, 2013**. We do not expect VA to generate any new documentation for this response. **Attachment D** 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

---