

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

Date: Monday, November 18, 2013

Source: House Veterans Affairs Subcommittee on Oversight and Investigations

Scope: OMB Memo: Safeguarding Against and Responding to the Breach of Personally Identifiable Information, M-07-16, May 22, 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: Monday, November 18, 2013	Date Due: Thursday, December 5, 2013
OMB Memo: Safeguarding Against and Responding to the Breach of Personally Identifiable Information, M-07-16, May 22, 2007		
Attachment I:	Date Sent: TBD	Date Due: TBD
Critical Security Controls for Effective Information Security		

OMB Memorandum: Safeguarding Against and Responding to the Breach of Personally Identifiable Information, M-07-16 May 22, 2007

Overview of OMB's Memorandum:

As part of the work of the Identity Theft Task Force, this memorandum **requires agencies to develop and implement a breach notification policy** within 120 days.

The attachments to this memorandum **outline the framework within which agencies must develop this breach notification policy** while ensuring proper safeguards are in place to protect the information.

While this framework identifies a number of steps to greatly reduce the risks related to a data breach of personally identifiable information, it is important to emphasize that a **few simple and cost-effective steps** may well deliver the greatest benefit, such as:

- reducing the volume of collected and retained information to the minimum necessary;
- limiting access to only those individuals who must have such access; and
- using **encryption, strong authentication** procedures, and **other security controls** to make information unusable by unauthorized individuals.

Materials created in response to this Memorandum and attachments **should be made available to the public** through means determined by the agency, e.g., posted on the agency web site, by request, etc.

Outline of OMB's Memorandum:

Attachment 1: Safeguarding Against the Breach of Personally Identifiable Information (agencies must review their existing requirements with respect to Privacy and Security)

Attachment 2: Incident Reporting and Handling Requirements (The policy must include existing and new requirements for Incident Reporting and Handling)

Attachment 3: External Breach Notification

Attachment 4: Rules and Consequences (requires agencies to develop policies concerning the responsibilities of individuals authorized to access personally identifiable information)

1. Since the issuance of OMB M-07-16, has VA developed and implemented a breach notification policy within the required 120 days? Yes No Other:
 - a. If yes, please provide additional detail on how and when this was done. If no, please explain why not:
 - b. If yes, does the policy address breaches for both electronic systems as well as paper documents? Yes No Other:
 - c. Documentation available (i.e. policy, guidelines, breach notification policy, 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. Overall, when developing and implementing their breach notification policy, did VA address or include the following (detailed questions regarding each attachment will be asked later):
 - a. Review their existing requirements with respect to privacy and security (see Attachment 1)? Yes No Other:
 - b. Include existing and new requirements for incident reporting and handling (see Attachment 2)? Yes No Other:
 - c. Include existing and new requirements for external breach notification (see Attachment 3)? Yes No Other:
 - d. Develop policies concerning the responsibilities of individuals authorized to access personally identifiable information (see Attachment 4)? 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 (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:
3. OMB's memo provides a few simple and cost-effective steps to reduce the risks related to a data breach of personally identifiable information. Has the VA implemented the following steps:
- a. Reducing the volume of collected and retained information to the minimum necessary? Yes No Other:
- b. Limiting access to only those individuals who must have such access? Yes No Other:
- c. Using encryption and other security controls to make information unusable by unauthorized individuals? Yes No Other:
- d. Using strong authentication procedures and other security controls to make information unusable by unauthorized individuals? 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 (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:
4. Have all the materials created in response to OMB M-07-16 and attachments (1-4), been made available to the public (e.g., posted on the agency web site, by request, etc.)? Yes No Other:
- a. If yes, please provide additional detail on how this was done and where they are located. 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:

Overview of Attachment 1 - Safeguarding Against the Breach of Personally Identifiable Information:

1. Current Privacy Act Requirements:

- Establish Rules of Conduct
- Establish Safeguards
- Maintain accurate, relevant, timely and complete information

2. Current Security Requirements:

- a. Assign an **impact level** to all information and information systems.
- b. Implement **minimum security requirements** and controls.
- c. **Certify and accredit** information systems.
- d. **Train** employees.

5. **2a:** Does VA assign an impact level to all information and information systems? 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:
6. **2a:** Does VA follow the processes outlined in Federal Information Processing Standard (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*, to categorize all information and information systems according to the standard's three levels of impact (i.e., low, moderate, or high)? 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. **2a:** Does VA categorize sensitive personally identifiable information (and information systems within which such information resides) as moderate or high impact? 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, 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:
8. **2b:** For each of the impact levels (i.e., low, moderate, or high), does VA implement the minimum security requirements and minimum (baseline) security controls set forth in FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, and NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, respectively? 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:
9. **2c:** Does VA certify and accredit (i.e., A&A) all information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source? 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, authorization and accreditations, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
10. **2c:** Does VA follow the specific procedures for conducting C&A's that are set out in NIST's Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*? 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:
11. **2c:** Does VA issue guidance for the continuous monitoring of certain security controls? 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, does VA's continuous monitoring assess a subset of the following controls used to safeguard such information (e.g., Privacy Impact Assessments):
- a. Management controls used to safeguard such information? Yes No Other:
- b. Operational controls used to safeguard such information? Yes No Other:
- c. Technical controls used to safeguard such information? Yes No Other:
- 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:
12. **2d:** Does VA initially train employees (including managers) on their privacy and security responsibilities before permitting access to agency information and information systems? 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:
13. **2d:** Does VA provide an annual refresher training to ensure employees continue to understand their responsibilities? 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:
14. **2d:** Does VA provide additional or advanced training to commensurate with increased responsibilities or change in duties? 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:
15. **2d:** Does VA's initial training include the following:
- a. Acceptable rules of behavior? Yes No Other:
- b. Consequences when the rules are not followed? Yes No Other:
- c. If yes, please provide additional detail on how they are being accomplished. 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:
16. **2d:** Does VA's refresher training include the following:
- a. Acceptable rules of behavior? Yes No Other:
- b. Consequences when the rules are not followed? Yes No Other:
- c. If yes, please provide additional detail on how they are being accomplished. 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:
17. **2d:** For VA's telework and other authorized remote access programs, does the training include the following:
- a. Acceptable rules of behavior? Yes No Other:
- b. Consequences when the rules are not followed? Yes No Other:
- c. If yes, please provide additional detail on how they are being accomplished. 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:

Overview of Attachment 1 - Safeguarding Against the Breach of Personally Identifiable Information:

B. Additional Privacy Requirements:

1. Review and Reduce the Volume of Personally Identifiable Information.

a. Review Current Holdings.

2. Reduce the Use of Social Security Numbers.

b. Eliminate Unnecessary Use.

c. Explore Alternatives.

18. **Review Current Holdings:** Does VA review their current holdings of all 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, reviews, 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. **Review Current Holdings:** Does VA ensure, to the maximum extent practicable, such holdings of PII are accurate, relevant, timely, and complete? 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:
20. **Review Current Holdings:** Does VA reduce their holdings of PII to the minimum necessary for the proper performance of a documented agency function? 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:
21. **Review Current Holdings:** Are VA's implementation plans and progress updates regarding this review incorporated as requirements in their annual report under FISMA? 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, implementation plan, progress updates, 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. **Review Current Holdings:** Since VA's initial review, have they developed and made public a schedule by which they will periodically update the review of their holdings? 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 Act's SORN, 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. **Review Current Holdings:** To help safeguard PII, agencies are reminded they must meet the requirements of FISMA and associated policies and guidance from the OMB and NIST. Does VA perform the following:
- a. Implement a comprehensive security program to protect the agency's information and information systems? Yes No Other:
- b. VA's Inspectors General independently evaluates the agency's program? Yes No Other:
- c. Report annually to OMB and Congress on the effectiveness of their program? Yes No Other:
- a. If yes, for each of the above, please provide additional detail on how this is being accomplished. If no, for each of the above, please explain why not:
- b. Documentation available (i.e. policy, guidelines, implementation plan, progress updates, 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 Attachment 1 - Safeguarding Against the Breach of Personally Identifiable Information:

B. Additional Privacy Requirements:

1. Review and Reduce the Volume of Personally Identifiable Information.
 - a. Review Current Holdings.
2. Reduce the Use of Social Security Numbers.
 - b. Eliminate Unnecessary Use.
 - c. Explore Alternatives.

24. **Eliminate Unnecessary Use:** Does VA review their use of social security numbers within their systems and programs to identify instances in which collection or use of the social security number is superfluous? 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, reviews, actual evidentiary documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
25. **Eliminate Unnecessary Use:** Within 120 days from the date of this memo, did VA establish a plan in which the agency will eliminate the unnecessary collection and use of social security numbers within eighteen months? 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, plan with date, 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. **Explore Alternatives:** Does VA participate in government-wide efforts to explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs (e.g., surveys, data calls, etc.)? 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:

Overview of Attachment 1 - Safeguarding Against the Breach of Personally Identifiable Information:

C. Additional Security Requirements:

- Encryption
- Control Remote Access.
- Time-Out Function.
- Log and Verify.
- Ensure Understanding of Responsibilities

Agencies should also contemplate and **incorporate best practices to prevent data breaches**. Examples of such practices might include using privacy screens when working outside the office or requiring employees to include laptop computers in carry-on luggage rather than checked baggage

27. **Encryption:** Does VA encrypt, using NIST certified cryptographic modules, all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive, in writing, by your Deputy Secretary? 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:
28. **Encryption:** Since January 2010, has VA lost any data on mobile computers/devices carrying agency data? Yes No Other:
- a. If yes, were these mobile computers/devices encrypted? Yes No Other: If no, please explain why not:
- a. If yes, was the encryption turned on? Yes No Other: If no, please explain why not:
- b. If yes, for each, please provide additional detail on how this is being accomplished. If no, for each, please explain why not:
- 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:
29. **Control Remote Access:** Does VA allow remote access only with 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:
30. **Time-Out Function:** Does VA use a “time-out” function for remote access and mobile devices requiring user re-authentication after thirty 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:
31. **Log and Verify:** 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, logs, 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:
32. **Log and Verify:** Does VA verify each extract, including whether sensitive data has been erased within 90 days or 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:
33. **Ensure Understanding of Responsibilities:** Does VA ensure all individuals with authorized access to personally identifiable information and their supervisors sign at least annually a document clearly describing their responsibilities? 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, signature documents, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

34. **Best Practices to Prevent Data Breaches:** Does VA contemplate and incorporate best practices to prevent data breaches (Examples of such practices might include using privacy screens when working outside the office or requiring employees to include laptop computers in carry-on luggage rather than checked baggage)?
 Yes No Other:
- If yes, please provide additional detail on how this is being accomplished. If no, please explain why not:
 - Documentation available (i.e. policy, guidelines, best practices, signature documents, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

Overview of Attachment 2 - Incident Reporting and Handling Requirements:

Current FISMA Requirements:

- implement procedures for detecting, reporting and responding to security incidents, including mitigating risks associated with such incidents before substantial damage is done
- notify and consult with:
 - the Federal information security incident center
 - law enforcement agencies and Inspectors General
 - an office designated by the President for any incident involving a national security system
 - any other agency or office in accordance with law or as directed by the President.
- implement NIST guidance and standards
- **Incident Handling and Response Mechanisms:**
 - agencies must establish formal incident response mechanisms
 - sharing information concerning common vulnerabilities and threats with those operating other systems and in other agencies
 - training employees on how to prevent incidents

Federal Information Processing Standards Publication 200 (FIPS 200) and NIST Special Publication 800-53 provide a framework for categorizing information and information systems, and provide minimum security requirements and minimum (baseline) security controls for incident handling and reporting. The procedures agencies must already use to implement the above FISMA requirements are found in two primary guidance documents: NIST Special Publication 800-61, Computer Security Incident Handling Guide; and the concept of operations for the Federal security incident handling center located within the Department of Homeland Security, i.e., United States Computer Emergency Readiness Team (US-CERT).

35. **Incident Handling and Response Mechanisms:** Has VA established formal incident response mechanisms?
 Yes No Other:
- If yes, please provide additional detail on how this is being accomplished. If no, please explain why not:
 - 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:
36. **Incident Handling and Response Mechanisms:** Does VA's incident handling and response include sharing information concerning common vulnerabilities and threats with those operating other systems and in other agencies? Yes No Other:
- If yes, please provide additional detail and examples on how this is being accomplished. If no, please explain why not:
 - Documentation available (i.e. policy, guidelines, information shared and with whom, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
37. **Incident Handling and Response Mechanisms:** Does VA train all its employees on how to prevent security incidents? Yes No Other:

- a. If yes, please provide additional detail and examples on how this is being accomplished. If no, please explain why not:
- b. Documentation available (i.e. policy, guidelines, employee training manual, actual evidentiary documents)?
 Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

38. **Incident Handling and Response Mechanisms:** Are VA employees instructed in their roles and responsibilities regarding responding to incidents should they occur? Yes No Other:
- a. If yes, please provide additional detail and examples on how this is being accomplished. If no, please explain why not:
 - b. Documentation available (i.e. policy, guidelines, employee training manual, actual evidentiary documents)?
 Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

(continued) Overview of Attachment 2 - Incident Reporting and Handling Requirements

B. Modified Agency Reporting Requirements:

1. US-CERT Modification - Agencies must report all incidents involving personally identifiable information to US-CERT.:

- **Category 1 Reporting.** Unauthorized Access or Any Incident Involving Personally Identifiable Information
 - 1) an **individual gains logical or physical access without permission** to a federal agency network, system, application, data, or other resource
 - 2) there is a suspected or **confirmed breach of personally identifiable information** regardless of the manner in which it might have occurred
- **Reporting to US-CERT is required within one hour** of discovery/detection - <http://www.us-cert.gov/government-users/reporting-requirements>.
 - For incidents involving personally identifiable information, agencies must:
 - Continue to follow internal agency procedures for **notifying agency officials** including your agency privacy official and Inspector General;
 - **Notify the issuing bank** if the breach involves government-authorized credit cards; and
 - **Notify US-CERT within one hour.** Although only limited information about the breach may be available, US-CERT must be advised so it can assist in coordinating communications with the other agencies. Updates should be provided as further information is obtained.
 - Under specific procedures established for these purposes, after notification by an agency, **US-CERT will notify the appropriate officials.**
 - **Monthly, US-CERT will distribute to designated officials in the agencies** and elsewhere, a report identifying the number of confirmed breaches of personally identifiable information and will also make available a **public version of the report.**

39. **US-CERT Modification:** Since January 2010, has VA reported all incidents, including foreign entity breaches, involving personally identifiable information to US-CERT? 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, reports, actual evidentiary documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

40. **US-CERT Modification:** Does VA's incident reporting include both potential and confirmed 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, reports, actual evidentiary documents)? Yes No Other:

- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
41. **Category 1. Unauthorized Access or Any Incident Involving Personally Identifiable Information:** Does VA provide a report to US-CERT when an individual gains logical or physical access without permission to their network, system, application, data, or other resource? 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, reports, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
42. **Category 1. Unauthorized Access or Any Incident Involving Personally Identifiable Information:** Does VA provide a report to US-CERT when there is a suspected or confirmed breach of personally identifiable information regardless of the manner in which it might have occurred? 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, reports, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
43. **Category 1. Unauthorized Access or Any Incident Involving Personally Identifiable Information:** Since January 2010, has VA reported to US-CERT within one hour of discovery/detection of foreign and domestic 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, reports, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
44. **Category 1. Unauthorized Access or Any Incident Involving Personally Identifiable Information:** For each incident did VA notify agency officials including VA's privacy official and Inspector General? 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, 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:
45. **Category 1. Unauthorized Access or Any Incident Involving Personally Identifiable Information:** Monthly, for each incident, did the US-CERT distribute to designated officials in the VA, a report identifying the number of confirmed breaches 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, report distributed to VA officials, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
46. **Category 1. Unauthorized Access or Any Incident Involving Personally Identifiable Information:** Monthly, for each incident, did the US-CERT make available a public version of the report? 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, public version of the report, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

(continued) Overview of Attachment 2 - Incident Reporting and Handling Requirements

B. Modified Agency Reporting Requirements (Questions regarding this section were addressed in previous attachments):

2. Develop and Publish a Routine Use:

- Effective Response
 - An effective response necessitates disclosure of information regarding the breach to those individuals affected by it, as well as to persons and entities in a position to cooperate, either by assisting in notification to affected individuals or playing a role in preventing or minimizing harms from the breach.
- Disclosure of Information.
 - 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

Overview of Attachment 3 - External Breach Notification (this Attachment identifies the questions and factors each agency should consider in determining when notification outside the agency should be given and the nature of the notification)

Background

- Harm - Agencies are referred to the ID Theft Task Force’s Strategic Plan for guidance
- Requirement - Agencies must develop a breach notification policy and plan
- Threshold questions - The likely risk of harm and the level of impact will determine when, what, how and to whom notification should be given
- Chilling Effects of Notices - Agencies should exercise care to evaluate the benefit of notifying the public of low impact incidents.

B. New Requirements

Six elements should be addressed in the policy and plan and when considering external notification:

1. whether breach notification is required
 2. timeliness of the notification
 3. source of the notification
 4. contents of the notification
 5. means of providing the notification
 6. who receives notification: public outreach in response to a breach
- Each agency should develop a breach notification policy and plan
 - Each agency should **establish an agency response team** including the Program Manager of the program experiencing the breach, Chief Information Officer, Chief Privacy Officer or Senior Official for Privacy, Communications Office, Legislative Affairs Office, General Counsel and the Management Office which includes Budget and Procurement functions.

47. Agency Response Team: Has VA established an agency response team that includes the following officials:

- a. Program Manager of the program experiencing the breach? Yes No Other:
- b. Chief Information Officer? Yes No Other:
- c. Chief Privacy Officer or Senior Official for Privacy? Yes No Other:
- d. Communications Office? Yes No Other:
- e. Legislative Affairs Office? Yes No Other:
- f. General Counsel? Yes No Other:
- g. Management Office which includes Budget and Procurement functions? Yes No Other:
- h. If yes, please provide additional detail on how this is being accomplished. If no, please explain why not:

- i. Documentation available (i.e. policy, guidelines, response team 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:

(continued) - Overview of Attachment 3 - External Breach Notification (this Attachment identifies the questions and factors each agency should consider in determining when notification outside the agency should be given and the nature of the notification)

B. New Requirements

Six elements should be addressed in the policy and plan and when considering external notification:

1. **whether breach notification is required**
2. timeliness of the notification
3. source of the notification
4. contents of the notification
5. means of providing the notification
6. who receives notification: public outreach in response to a breach

1. Whether Breach Notification is Required

- 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.
- **Five factors should be considered to assess the likely risk of harm**
 - a. **Nature of the Data Elements Breached.**
 - b. **Number of Individuals Affected.**
 - c. **Likelihood the Information is Accessible and Usable.**
 1. Agencies will first need to assess whether the personally identifiable information is at a low, moderate, or high risk of being compromised using NIST standards and guidance
 - d. **Likelihood the Breach May Lead to Harm** - In considering whether the loss of information could result in identity theft or fraud, agencies should consult guidance from the Identity Theft Task Force
 1. **Broad Reach of Potential Harm** - agencies should consider a number of possible harms associated with the loss or compromise of information. Such harms may include the effect of a breach of confidentiality or fiduciary responsibility, the potential for blackmail, the disclosure of private facts, mental pain
 2. **Likelihood Harm Will Occur** - Social Security numbers and account information are useful to committing identity theft, as are date of birth, passwords, and mother's maiden name.
 - e. **Ability of the Agency to Mitigate the Risk of Harm**
 1. In addition to containing the breach, appropriate countermeasures, such as monitoring system(s) for misuse of the personal information and patterns of suspicious behavior, should be taken

- 48. **Nature of the Data Elements Breached:** In assessing the levels of risk and harm, does VA consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals? 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, assessments, actual evidentiary documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
- 49. **Number of Individuals Affected:** Does the magnitude of the number of affected individuals dictate the method(s) VA chooses for providing notification? 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:

50. **Number of Individuals Affected:** Does the magnitude of the number of affected individuals affect the method(s) VA chooses for providing notification? Yes No Other:
- If yes, please provide additional detail on how this is being accomplished. If no, please explain why not:
 - 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:
51. **Likelihood the Information is Accessible and Usable:** Upon learning of a breach, does VA assess the likelihood personally identifiable information will be or has been used by unauthorized individuals? Yes No Other:
- If yes, is this assessment guided by NIST security standards and guidance? Yes No Other:
 - If yes, for the above, please provide additional detail on how this is being accomplished and other assessment considerations (i.e., the likelihood any unauthorized individual will know the value of the information and either use the information or sell it to others), if any. If no, for the above, please explain why not:
 - Documentation available (i.e. policy, guidelines, assessments, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
52. **Broad Reach of Potential Harm:** Does VA consider the possible harms associated with the loss or compromise of information? Yes No Other:
- If yes, do they consider the following harms:
 - The effect of a breach of confidentiality or fiduciary responsibility? Yes No Other:
 - The potential for blackmail? Yes No Other:
 - The disclosure of private facts? Yes No Other:
 - Mental pain and emotional distress? Yes No Other:
 - The disclosure of address information for victims of abuse? Yes No Other:
 - The potential for secondary uses of the information which could result in fear or uncertainty? Yes No Other:
 - The unwarranted exposure leading to humiliation or loss of self-esteem? Yes No Other:
 - If yes, for each, please provide additional detail on how this is being accomplished. If no, for each, please explain why not:
 - 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:
53. **Likelihood Harm Will Occur:** How does VA determine the likelihood a breach may result in harm? [Click here to enter text.](#)
- 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:
54. **Ability of the Agency to Mitigate the Risk of Harm:** For each of the nine foreign data breaches, was VA able to mitigate further compromise of the system(s) affected by the breach? Yes No Other:
- If yes, please provide additional detail on how this was accomplished. If no, please explain why not:
 - 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:
55. **Ability of the Agency to Mitigate the Risk of Harm:** Does VA take countermeasures to prevent or limit the associated harm, such as monitoring system(s) for misuse of the personal information and patterns of

suspicious behavior (i.e. if the information relates to disability beneficiaries, monitoring a beneficiary database for requests for change of address may signal fraudulent activity)? 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:

(continued) - Overview of Attachment 3 - External Breach Notification (this Attachment identifies the questions and factors each agency should consider in determining when notification outside the agency should be given and the nature of the notification)

B. New Requirements

Six elements should be addressed in the policy and plan and when considering external notification:

1. whether breach notification is required
2. **timeliness of the notification**
3. source of the notification
4. contents of the notification
5. means of providing the notification
6. who receives notification: public outreach in response to a breach

2. Timeliness of the Notification

Agencies should **provide notification without unreasonable delay following the discovery of a breach**, consistent with the needs of law enforcement and national security and any measures necessary for your agency to determine the scope of the breach and, if applicable, to restore the reasonable integrity of the computerized data system compromised.

Decisions to delay notification should be made by the Agency Head or a senior-level individual he/she may designate in writing

56. Since January 2010, for each of the nine foreign entity data breaches, how long did VA wait to provide notification following the discovery of each breach? [Click here to enter text.](#)
- a. Please provide additional detail on how this was accomplished. If no, please explain why not:
 - 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:
57. Since January 2010, for each of the nine foreign data breaches, how long did it take VA to restore the reasonable integrity of the computerized data system that was compromised? [Click here to enter text.](#)
- a. Please provide additional detail on how this was 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:
58. Who within VA has the power to delay a possible notification? [Click here to enter text.](#)
- a. Documentation available (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:

(continued) - Overview of Attachment 3 - External Breach Notification (this Attachment identifies the questions and factors each agency should consider in determining when notification outside the agency should be given and the nature of the notification)

B. New Requirements

Six elements should be addressed in the policy and plan and when considering external notification:

1. whether breach notification is required
2. timeliness of the notification
3. **source of the notification**
4. contents of the notification
5. means of providing the notification
6. who receives notification: public outreach in response to a breach

3. Source of the Notification

Notification to individuals affected by the breach should **be issued by the Agency Head, or senior-level individual**

Notification involving only a limited number of individuals (**e.g., under 50**) may also be issued jointly under the auspices of the **Chief Information Officer and the Chief Privacy Officer**

If breach involves a **Federal contractor** or a public-private partnership operating a system of records on behalf of the agency, the **agency is responsible for ensuring any notification and corrective actions** are taken.

59. **Source of the Notification:** Are VA's notifications to individuals affected by the breach issued by the Secretary, or a senior-level individual he may designate in writing? 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, notifications to individuals, notifications sent out after the foreign data 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:
60. **Source of the Notification:** Are VA's notifications involving a limited number of individuals (e.g., under 50) issued jointly under the auspices of the Chief Information Officer and the Chief Privacy Officer or Senior Agency Official for Privacy? 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, notifications to individuals, notifications sent out after the foreign data 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:
61. **Source of the Notification:** If a breach at the VA involves a Federal contractor or a public-private partnership operating a system of records on behalf of the agency, is VA held responsible for ensuring any notification and corrective actions are taken? 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, notifications to individuals, notifications sent out after the foreign data 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:
62. **Source of the Notification:** Are the roles, responsibilities, and relationships with contractors or partners reflected in the following:
- a. VA's breach notification policy and plan? Yes No Other:
 - b. VA's system certification and accreditation documentation? Yes No Other:
 - c. VA's contracts? Yes No Other:
 - d. If yes, for each, please provide additional detail on how this is being accomplished. If no, for each, please explain why not:

- e. Documentation available (i.e. policy, guidelines, notification policy and plan, contracts, actual evidentiary documents)? Yes No Other:
- f. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

(continued) - Overview of Attachment 3 - External Breach Notification (this Attachment identifies the questions and factors each agency should consider in determining when notification outside the agency should be given and the nature of the notification)

B. New Requirements

Six elements should be addressed in the policy and plan and when considering external notification:

1. whether breach notification is required
2. timeliness of the notification
3. source of the notification
- 4. contents of the notification**
5. means of providing the notification
6. who receives notification: public outreach in response to a breach

4. Contents of the Notification – Majority of contents addressed in Attachment C

The notification should be provided in writing and should be concise, conspicuous, plain language. A standard notice should be part of your approved breach plan. The notice should include the following elements:

- A brief description of what happened, including the date(s) of the breach and of its discovery;
- To the extent possible, a description of the types of personal information involved in the breach (e.g., full name, Social Security number, date of birth, home address, account number, disability code, etc.);
- A statement whether the information was encrypted or protected by other means, when determined such information would be beneficial and would not compromise the security of the system;
- What steps individuals should take to protect themselves from potential harm, if any;
- What the agency is doing, if anything, to investigate the breach, to mitigate losses, and to protect against any further breaches; and
- Who affected individuals should contact at the agency for more information, including a toll-free telephone number, e-mail address, and postal address.

If you have knowledge the affected individuals are not English speaking, **notice should also be provided in the appropriate language(s)**. A **standard notice** should be part of your approved breach plan

63. **Contents of the Notification:** Are VA's notifications to individuals provided in writing and are they required to be concise, conspicuous, plain language? 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, notifications to individuals, notifications sent out after the foreign data 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:
64. **Contents of the Notification:** If the affected individuals are not English speaking, does VA send the notice in the appropriate language(s)? 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, notifications to individuals, notifications sent out after the foreign data 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:
65. **Contents of the Notification:** If the affected individuals are not English speaking, does VA send the notice in the appropriate language(s)? 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, notifications to individuals, notifications sent out after the foreign data 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:

66. **Contents of the Notification:** Is a standard notice should part of VA's approved breach plan? 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:

(continued) - Overview of Attachment 3 - External Breach Notification (this Attachment identifies the questions and factors each agency should consider in determining when notification outside the agency should be given and the nature of the notification)

B. New Requirements

Six elements should be addressed in the policy and plan and when considering external notification:

- 1. whether breach notification is required
- 2. timeliness of the notification
- 3. source of the notification
- 4. contents of the notification
- 5. means of providing the notification**
- 6. who receives notification: public outreach in response to a breach

5. Means of Providing Notification

The **best means for providing notification will depend on the number of individuals affected** and what contact information is available about the affected individuals. The following examples are types of notice which may be considered.

- a. Telephone.
- b. First-Class Mail
- c. E-Mail
- d. Existing Government Wide Services
- e. Newspapers or other Public Media Outlets
- f. Substitute Notice
- g. Accommodations

67. **Means of Providing Notification:** Does VA's notice to individuals affected by a breach commensurate with the number of people affected and the urgency with which they need to receive notice? 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, notifications to individuals, notifications sent out after the foreign data 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:

68. Since January 2010, in instances where VA has found a data breach, how many times did VA notify individuals using the following methods:

- a. Telephone? [Click here to enter text.](#)
- b. First-Class Mail? [Click here to enter text.](#)
- c. E-Mail? [Click here to enter text.](#)
- d. Existing Government Wide Services? [Click here to enter text.](#)
- e. Newspapers or other Public Media Outlets? [Click here to enter text.](#)
- f. Substitute Notice? [Click here to enter text.](#)
- g. Accommodations? [Click here to enter text.](#)

- h. Documentation available (i.e. policy, guidelines, other evidentiary documents)? Yes No Other:
- i. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
69. **Telephone:** For telephone notifications made by VA, are they contemporaneous with written notification by first-class mail? 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, telephone notifications to individuals, telephone notifications sent out after the foreign data 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:
70. **First-Class Mail:** For first-class mail notifications, is the front of the envelope labeled to alert the recipient to the importance of its contents, e.g., “Data Breach Information Enclosed” and marked with the VA as the sender to reduce the likelihood the recipient thinks it is advertising mail? 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, first-class mail notifications to individuals, first-class mail notifications sent out after the foreign data 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:
71. **E-Mail:** When does VA employ e-mail notifications? [Click here to enter text.](#)
- a. Documentation available (i.e. policy, guidelines, e-mail notifications to individuals, e-mail notifications sent out after the foreign data breaches, actual evidentiary documents)? Yes No Other:
- b. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
72. **Existing Government Wide Services:** Does VA use Government wide services already in place to provide support services needed, such as USA Services, including toll free number of 1-800-FedInfo and www.USA.gov? 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:
73. **Newspapers or other Public Media Outlets:** Has VA set up toll-free call centers staffed by trained personnel to handle inquiries from the affected individuals and the public? 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:
74. **Substitute Notice:** If applicable, does VA’s substitute notice consist of a conspicuous posting of the notice on the VA home page and notification to major print and broadcast media, including major media in areas where the affected individuals reside? 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:

75. **Substitute Notice:** If applicable, does VA's notice to media include a toll-free phone number where an individual can learn whether or not his or her personal information is included in the breach? Yes No Other:
- If yes, please provide additional detail on how this is being accomplished. If no, please explain why not:
 - Documentation available (i.e. policy, guidelines, toll-free number used, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
76. **Accommodations:** If applicable, does VA provide special consideration to providing notice to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973? Yes No Other:
- If yes, please provide additional detail on how this is being accomplished. If no, please explain why not:
 - Documentation available (i.e. policy, guidelines, toll-free number used, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
77. **Accommodations:** If applicable, do VA's accommodations include establishing a Telecommunications Device for the Deaf (TDD) or posting a large type notice on the agency web site? Yes No Other:
- If yes, please provide additional detail on how this is being accomplished. If no, please explain why not:
 - 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:

(continued) - Overview of Attachment 3 - External Breach Notification (this Attachment identifies the questions and factors each agency should consider in determining when notification outside the agency should be given and the nature of the notification)

B. New Requirements

Six elements should be addressed in the policy and plan and when considering external notification:

- whether breach notification is required
- timeliness of the notification
- source of the notification
- contents of the notification
- means of providing the notification
- who receives notification: public outreach in response to a breach**

6. Who Receives Notification: Public Outreach in Response to a Breach

- **Notification of Individuals.**
- **Notification of Third Parties including the Media**
 - Careful Planning.
 - Web Posting - The information should also appear on the www.USA.gov web site.
 - Notification of other Public and Private Sector Agencies
 - Congressional Inquiries
- **Reassess the Level of Impact Assigned to the Information** - After evaluating each of these factors, you should review and reassess the level of impact you have already assigned to the information using the impact levels defined by the NIST (See FIPS 199 and Attachment 1 of this memorandum). The determination of the potential impact of loss of information is made by the agency during an information system's certification and accreditation process.
- The impact levels – low, moderate, and high, describe the (worst case) potential impact on an organization or individual if a breach of security occurs

78. **Notification of Individuals:** Once VA has determined to provide a notice regarding the breach, how long does it take the affected individuals to receive the notification? Yes No Other:
- If yes, please provide additional detail on how this is being accomplished. If no, please explain why not:
 - Documentation available (i.e. policy, guidelines, notifications to individuals, notifications sent out after the foreign data breaches, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
79. **Notification of Third Parties including the Media – Careful Planning:** How does VA notify the public media without unnecessarily alarming the public? [Click here to enter text.](#)
- 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:
80. **Notification of Third Parties including the Media – Careful Planning:** After the nine foreign data breaches, did VA notify the public media? Yes No Other:
- If yes, please provide additional detail on how this is being accomplished, the type of information within the notifications, and how long it took for VA to contact the public media. If no, please explain why not:
 - Documentation available (i.e. policy, guidelines, notifications to the public media, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
81. **Notification of Third Parties including the Media – Web Posting:** For the nine foreign data breaches did VA post information about the breach and notification in a clearly identifiable location on the home page of VA's web site? Yes No Other:
- If yes, please provide additional detail on how this was accomplished and how long it took for each breach. If no, please explain why not:
 - Documentation available (i.e. policy, guidelines, screenshots, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
82. **Notification of Third Parties including the Media – Web Posting:** Did each web posting include the following: The posting should include a link to Frequently Asked Questions (FAQ) and other talking points to assist the public's understanding of the breach and the notification process. The information should also appear on the www.USA.gov web site? Yes No Other:
- Link to Frequently Asked Questions (FAQ)? Yes No Other:
 - Other talking points to assist the public's understanding of the breach and the notification process? Yes No Other:
 - Does the information should also appear on the www.USA.gov web site? Yes No Other:
 - If yes, for each, please provide additional detail on how this was accomplished. If no, for each, please explain why not:
 - Documentation available (i.e. policy, guidelines, screenshots, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

83. **Notification of Third Parties including the Media – Notification of other Public and Private Sector Agencies:** Did VA notify other public and private sector agencies that may be affected by the breach or may play a role in mitigating the potential harms stemming from the breach? Yes No Other:
- If yes, please provide additional detail on how this was accomplished. If no, please explain why not:
 - Documentation available (i.e. policy, guidelines, screenshots, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
84. **Notification of Third Parties including the Media – Congressional Inquiries:** For the nine foreign data breaches did VA have to respond to any inquires from other governmental agencies such as the Government Accountability Office and Congress? Yes No Other:
- If yes, please provide additional detail on how this was accomplished. If no, please explain why not:
 - 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:
85. **Reassess the Level of Impact Assigned to the Information:** After evaluating each of the above factors, does VA review and reassess the level of impact it already assigned to the information using the impact levels defined by the NIST? Yes No Other:
- If yes, please provide additional detail on how this was accomplished. If no, please explain why not:
 - Documentation available (i.e. policy, guidelines, evaluations, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
86. **Reassess the Level of Impact Assigned to the Information:** Please describe in detail the risk levels (i.e. low, moderate, and high) used at the VA to describe the (worst case) potential impact on the organization or individual if a breach of security occurs: [Click here to enter text.](#)
- Documentation available (i.e. policy, guidelines, FIPS 199, five risk factors discussed in section 1 of M-07-16, actual evidentiary documents)? Yes No Other:
 - Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
87. **Reassess the Level of Impact Assigned to the Information:** Please describe how the impact levels help VA determine when and how a notification should be provided: [Click here to enter text.](#)
- 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:

Overview of Attachment 4 - Rules and Consequences

A. New Requirement: Rules and Consequences Policy

Responsibility of each agency head to develop and implement an **appropriate policy outlining the rules of behavior and identifying consequences and corrective actions available** for failure to follow these rules to safeguarding personally identifiable information.

- **Affected Individuals** - At a minimum, **each agency should have a documented policy** in place which applies to employees of the agency (including managers), and its contractors, licensees, certificate holders, and grantees.
- **Affected Actions** - The agency's policy should **describe the terms and conditions affected individuals shall be subject to and identify available corrective actions**. Rules of behavior and corrective actions should address the following:
 - **Failure to implement and maintain security controls**, for which an employee is responsible and aware, for personally identifiable information regardless of whether such action results in the loss of control or unauthorized disclosure of personally identifiable information
 - **Exceeding authorized access to, or disclosure to unauthorized persons of, personally identifiable information;**
 - **Failure to report any known or suspected loss of control** or unauthorized disclosure of personally identifiable information; and
 - For managers, **failure to adequately instruct, train, or supervise employees** in their responsibilities.
- **Consequences** - Applicable **consequences may include reprimand, suspension, removal, or other actions in accordance with applicable law and agency policy**. The minimum consequence agencies should consider is prompt removal of authority to access information or systems from individuals who demonstrates egregious disregard or a pattern of error in safeguarding personally identifiable information

88. Has the Secretary developed and implemented an appropriate policy outlining the rules of behavior and identify the consequences and corrective actions available for failure to safeguard personally identifiable information? 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, actual evidentiary documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
89. Do the consequences commensurate with the level of responsibility and type of personally identifiable information involved? 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, actual evidentiary documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
90. Does the VA remind supervisors of their responsibility to instruct, train and supervise employees on safeguarding personally identifiable information? 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, actual evidentiary documents)? Yes No Other:
 - c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:
91. **Affected Individuals:** Does VA have a documented policy in place which applies to the following employees:
- a. Managers? Yes No Other:
 - b. Contractors? Yes No Other:
 - c. Licensees? Yes No Other:
 - d. Certificate holders? Yes No Other:
 - e. Grantees? Yes No Other:

- f. Documentation available (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:

92. **Affected Actions:** Does VA's rules of behavior and corrective actions address failure to implement and maintain security controls, for which an employee is responsible and aware, for personally identifiable information regardless of whether such action results in the loss of control or unauthorized disclosure of personally identifiable information? 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, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

93. **Affected Actions:** Does VA's rules of behavior and corrective actions address exceeding authorized access to, or disclosure to unauthorized persons of, personally identifiable information? 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, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

94. **Affected Actions:** Does VA's rules of behavior and corrective actions address failure to report any known or suspected loss of control or unauthorized disclosure of personally identifiable information? 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, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

95. **Affected Actions:** Does VA's rules of behavior and corrective actions address for managers, failure to adequately instruct, train, or supervise employees in their responsibilities? 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, actual evidentiary documents)? Yes No Other:
- c. Please provide source of documentation (if necessary, point to specific pages): VA will provide VA website Other:

96. **Consequences:** Please describe the minimal and applicable consequences for VA employees etc. demonstrating egregious disregard or a pattern of error in safeguarding personally identifiable information:

[Click here to enter text.](#)

- 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:

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, December 5, 2013**. We do not expect VA to generate any new documentation for this response, as the above are practices and deliverables that VA should already be addressing. **Attachment H** 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
