OFFICE OF THE SECRETARY OF DEFENSE
1950 DEFENSE PENTAGON
WASHINGTON, DC 20301-1950

ADMINISTRATION AND
MANAGEMENT

06 AUG 2007

MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS
CHAIRMAN OF THE JOINT CHIEFS OF STAFF
UNDER SECRETARIES OF DEFENSE
ASSISTANT SECRETARIES OF DEFENSE
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE
DIRECTOR, OPERATIONAL TEST AND EVALUATION
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE
ASSISTANTS TO THE SECRETARY OF DEFENSE
DIRECTOR, ADMINISTRATION AND MANAGEMENT
DIRECTOR, NET ASSESSMENT
DIRECTOR, FORCE TRANSFORMATION
DIRECTORS OF THE DEFENSE AGENCIES
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Department of Defense (DoD) Reporting Guidance for Agency Privacy Management for Fiscal Year 2007 (FY2007) / OMB Memo M-07-19

On July 25, 2007, the Office of Management and Budget (OMB) issued instructions for agency reporting under the Federal Information Security Management Act of 2002 (FISMA) (Attachment 1).

The privacy section asks a series of questions relating to (1) system of records notices and privacy training for your respective privacy programs, (2) agency privacy procedures and practices, and finally, (3) internal oversight mechanisms for privacy . The questions also relate, in part, to agency implementation of the privacy provisions of the E-Government Act of 2002.

The 2007 reporting requirements are similar to the 2006 requirements except in four areas. In particular, the plans required by OMB memorandum (M-07-16) of May 22, 2007, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information" should be provided if available in an appendix to your annual report and including the four following items (1) Breach notification policy; (2) implementation plan to eliminate unnecessary use of Social Security Numbers; (3) implementation plan and progress update on review and reduction of holdings of personally identifiable information; and (4) policy outlining rules of behavior and identifying consequences and corrective actions available for failure to follow these rules (Attachment 2).

In order to prepare the report, each DoD Component shall review its privacy program and provide information responsive to the OMB questions. To assist in this review, DoD

OSD 12732-07
8/7/2007 12:28:20 PM

supplementary guidance (4) have been prepared that can be used by Component Privacy Officials incident to obtaining and reporting the necessary information.

To this end, OMB requires that DoD Components complete the Section D, Reporting Template for Senior Agency Official for Privacy (SAOP) (Attachment 3) and Section D, Senior Agency Official for Privacy (SAOP) of the hard copy of the OMB Memo, M-07-19 (Attachment 1).

To meet the OMB suspense of October 1, 2007, the senior Component official having responsibility for privacy shall complete the review and submit their Component report no later than August 28, 2007.

My point of contact for this report is Mr. Samuel P. Jenkins, Director of the Defense Privacy Office. Should you have any questions, he can be contacted at (703) 607-2943 or via email at samuel.jenkins@osd.mil.

Michael B. Donley
DoD Senior Privacy Official

1. OMB Memo M-07-19
2. OMB Memo M-07-16
3. DoD Supplementary FY07 FISMA (Narrative Statement) Privacy Guidance
4. OMB's Template

TAB A

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

DEPUTY DIRECTOR
FOR MANAGEMENT

July 25, 2007

M-07-19

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Clay Johnson III
Deputy Director for Management

SUBJECT: FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

This memorandum provides instructions for meeting your agency's FY 2007 reporting requirements under the Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347). It also includes reporting instructions on your agency's privacy management program.

Because the Office of Management and Budget (OMB) and Congress use this report to evaluate agency-specific and Government-wide security performance, it is especially important your agency's report clearly and accurately reflect the overall status of your program and not include conflicting views of, or unresolved differences among, the various parties contributing to the report including the Chief Information Officer (CIO), the Inspector General (IG), and the Senior Agency Official for Privacy (SAOP). Although the reporting categories and questions are generally the same as last year, there are some updates based on security and privacy policies issued within the last year. In particular, the plans required by OMB memorandum (M-07-16) of May 22, 2007, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information"[1] should be provided in an appendix to your annual report and include the following items:

- Breach notification policy (Attachment 3);
- Implementation plan to eliminate unnecessary use of Social Security Numbers (SSN) (Attachment 1);
- Implementation plan and progress update on review and reduction of holdings of personally identifiable information (PII) (Attachment 1); and
- Policy outlining rules of behavior and identifying consequences and corrective actions available for failure to follow these rules (Attachment 4).

Please send one formal copy of your report addressed to the Director of OMB and an electronic copy to fisma@omb.eop.gov by October 1, 2007. Each report must include a transmittal letter from the agency head reconciling any differences between the findings of the agency CIO, IG, and SAOP. The report must reflect the agency head's

[1] http://www.whitehouse.gov/omb/memoranda/fy2007/m07-16.pdf

determination of the adequacy and effectiveness of information security and privacy policies, procedures, and practices. More details on reporting are found in the attachments to this memorandum. Your staff may contact Kristy LaLonde Daphnis, klalonde@omb.eop.gov, regarding security questions or Hillary Fielden, hfielden@omb.eop.gov, regarding privacy questions.

Attachments

- Instructions for Preparing the FISMA Report and Agency Privacy Management Report
- Reporting Template for Micro Agencies (Excel, 77 kb)
- Reporting Template for CIOs (Excel, 117 kb)
- Reporting Template for IGs (Excel, 112 kb)
- Reporting Template for SAOPs (Excel, 202 kb)
- Quarterly Reporting Template (Excel, 132 kb)

FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

Table of Contents

Section A - **Instructions for Completing the Annual Federal Information Security Management Act (FISMA) and Agency Privacy Management Report**..... Page 1

This section contains instructions, frequently asked questions, and definitions to aid Chief Information Officers (CIO), Inspectors General (IG), and Senior Agency Officials for Privacy (SAOP) in preparing and submitting the annual FISMA and Privacy Management Report.

Section B– **Reporting Template for CIOs**..... Page 24

This section contains instructions for CIOs to complete the annual FISMA reporting template (attached).

Section C– **Reporting Template for IGs** ..... Page 29

This section contains instructions for IGs to complete the annual FISMA reporting template (attached).

Section D – **Reporting Template for SAOPs**..... Page 36

This section contains instructions for SAOPs to complete the annual privacy reporting template (attached). The template in this attachment shall be completed by all agencies.

FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

Table of Contents

Section A - **Instructions for Completing the Annual Federal Information Security Management Act (FISMA) and Agency Privacy Management Report**..... Page 1

This section contains instructions, frequently asked questions, and definitions to aid Chief Information Officers (CIO), Inspectors General (IG), and Senior Agency Officials for Privacy (SAOP) in preparing and submitting the annual FISMA and Privacy Management Report.

Section B– **Reporting Template for CIOs**..... Page 24

This section contains instructions for CIOs to complete the annual FISMA reporting template (attached).

Section C– **Reporting Template for IGs** ..... Page 29

This section contains instructions for IGs to complete the annual FISMA reporting template (attached).

Section D – **Reporting Template for SAOPs**..... Page 36

This section contains instructions for SAOPs to complete the annual privacy reporting template (attached). The template in this attachment shall be completed by all agencies.

Frequently Asked Questions

Sending to Congress and GAO

1. When should my agency send our annual report to Congress and the Government Accountability Office (GAO)?

After review by and notification from OMB, agencies shall forward their transmittal letter with report sections B, C, and D to the appropriate Congressional Committees and GAO. Transmittal of agency reports to Congress shall be made by, or be consistent with guidance from, the agency's Congressional or Legislative Affairs office to the following: Committees on Oversight and Government Reform and Science and Technology of the House, the Committees on Government Affairs and Commerce, Science, and Transportation of the Senate, and the Congressional authorization and appropriations committees for each individual agency. In prior years, the Committees have provided to OMB specific points of contact for receiving the reports. As in the past, if such are provided to OMB, we will notify the agencies.

Submission Instructions and Templates

2. Which template should my agency use to fill out the annual and quarterly reports?

All Chief Financial Officer (CFO) Act agencies and agencies participating in the President's Management Agenda scorecard process (i.e., agencies with E-Government scorecards) should complete the annual report and submit quarterly updates to OMB. Quarterly updates are due to OMB by September 1, December 1, March 1, and June 1. All materials should be submitted to the OMB FISMA mailbox at fisma@omb.eop.gov

All other agencies should provide OMB only the annual report. Agencies should be prepared to provide information or submit quarterly reports to OMB upon request, however. Microagencies (i.e., agencies employing 100 or fewer FTEs) should use the abbreviated Excel spreadsheet (see Reporting Template for Microagencies attached) for their annual report.

3. When should program officials, SAOPs, CIOs, and IGs share the results of their reviews?

While the goal of FISMA is stronger agency- and Government-wide security, information regarding an agency's information security program should be shared as it becomes available. This helps promote timely correction of weaknesses in the agency's information systems and resolution of issues. Waiting until the completion of a report or the year's end does not promote stronger information system security.

4. Should agencies set an internal FISMA reporting cut-off date?

Yes. OMB suggests agencies set an internal cut-off date for data collection and report preparation. A cut-off date should permit adequate time for meaningful internal review and comment and resolution of any disputes before finalizing the agency's report to OMB. However, with respect to an IG's review of the CIO's or SAOP's work product, such review does not in itself fulfill FISMA's requirement for IGs to independently evaluate an agency's program including testing the effectiveness of a representative subset of the agency's information systems.

Security Reporting

5. Does the FISMA quarterly report represent cumulative totals of security and privacy information or show just a snapshot of the agency's inventory?

Agencies should report the cumulative total on each of their quarterly reports. For example, in Q1, an agency may report 497 systems containing Federal information in identifiable form. If the agency adds five systems during the following quarter, then the Q2 report would include 502 systems containing Federal information in identifiable form.

6. Must agencies report at both an agency wide level and by individual component?

Yes. Agencies must provide an overall agency view of their security and privacy program but most of the topic areas also require specific responses for each of the major components (e.g., bureaus or operating divisions). Thus, the agencies' and OMB's report can distinguish good performing components from poor performers and more accurately reflect the overall agency performance.

For agencies with extensive field and regional offices, it is not necessary to report to OMB on the security performance of each of the field offices. Rather, agencies shall confirm the security program of the major component which operates the field offices is: 1) effectively overseeing and measuring field performance; 2) including any weaknesses in the agency-wide POA&M; and 3) developing, implementing, and maintaining system-level POA&Ms.

7. Should all of my agency's information systems be included as part of our FISMA report?

Yes. Section 3544(a)(1)(A) states: "The head of each agency shall be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of (i) information collected or maintained by or on behalf of the agency; and (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." Your agency's annual FISMA report therefore summarizes the performance of your agency's program to secure all of your agency's information and information systems, in any form or format, whether automated

or manual. NIST Special Publication 800-37 provides guidance on establishing information system boundaries which can help you identify your systems.

8. Must the Department of Defense and the Director of National Intelligence (DNI) follow OMB policy and NIST guidance?

Provided DoD and DNI internal security standards and policies are as stringent as OMB's policies and NIST's standards, they must only follow OMB's reporting policies.

9. What reporting is required for national security systems?

FISMA requires annual reviews and reporting of all systems, including national security systems. Agencies can choose to provide responses to the questions in the template either in aggregate with or separate from their non-national security systems.

Agencies shall describe how they are implementing the requirements of FISMA for national security systems. When management and internal control oversight of an agency's national security programs and systems are handled differently than non-national security programs, a description of and explanation for the differences is required. DoD and the Director of National Intelligence (DNI) shall report on compliance with their policies and guidance.

The CIO for the (DNI) reports on systems processing or storing sensitive compartmentalized information (SCI) across the intelligence community and those other systems for which the DNI is the principal accrediting authority. Agencies shall follow the intelligence community reporting guidance for these systems. SCI systems shall only be reported via the intelligence community report. However, this separate reporting does not alter an agency head's responsibility for overseeing the security of all operations and assets of the agency or component. Therefore, copies of separate reporting must also be provided to the agency head for their use.

To assist oversight by appropriate national security authorities, it is important to specify where practicable which portion of the agency report pertains to national security systems.

NIST Guidance and Standards

10. Is use of National Institute of Standards and Technology (NIST) publications required?

Yes. For non-national security programs and information systems, agencies must follow NIST standards and guidance.

11. Is NIST guidance flexible?

Yes. While agencies are required to follow NIST standards and guidance in accordance with OMB policy, there is flexibility within NIST's guidance documents (specifically in the 800-series) in how agencies apply the guidance. However, NIST standards, or Federal Information Processing Standards (FIPS) are mandatory. Unless specified by additional implementing policy by OMB, guidance documents published by NIST generally allow agencies latitude in their application. Consequently, the application of NIST guidance by agencies can result in different security solutions that are equally acceptable and compliant with the guidance.

General

12. Are the security requirements outlined in the Act limited to information in electronic form?

No. Section 3541 of FISMA provides the Act's security requirements apply to "information and information systems" without distinguishing by form or format; therefore, the security requirements outlined in FISMA apply to Federal information in all forms and formats (including electronic, paper, audio, etc.).

13. Does OMB give equal weight to the assessments by the agency and the IG? What if the two parties disagree?

Yes, OMB gives equal weight to both assessments. In asking different questions of each party, OMB seeks complementary and not conflicting reporting. Inasmuch as OMB guidance requires a single report from each agency, OMB expects the report to represent the consolidated views of the agency and not separate views of various reviewers. All disagreements should be resolved prior to reporting to OMB.

14. FISMA, OMB policy, and NIST guidance require agency security programs to be risk-based. Who is responsible for deciding the acceptable level of risk (e.g., the CIO, program officials and system owners, or the IG)? Are the IGs' independent evaluations also to be risk-based? What if they disagree?

The agency head ultimately is responsible for deciding the acceptable level of risk for their agency. System owners, program officials, and CIOs provide input for this decision. Such decisions must reflect policies from OMB and standards and guidance from NIST (particularly FIPS 199 and FIPS 200). An information system's designated approving authority takes responsibility for accepting any residual risk, thus they are held accountable for managing the security for that system.

IG evaluations are intended to independently assess if the agency is applying a risk-based approach to their information security programs and the information systems that support the conduct of agency missions and business functions. When reviewing the Certification and Accreditation (C&A) of an individual system, for example, the IG would generally

assess whether: 1) the C&A was performed in the manner prescribed in NIST guidance and agency policy; 2) controls are being implemented as stated in any planning documentation; and 3) continuous monitoring is adequate given the system impact level of the system and information. Any disagreements among various program officials, the CIO, and/or the IG would be an internal agency matter and resolved consistent with guidance from the agency head.

15. Could you provide examples of high impact systems?

In some respects, the answer to this question is unique to each agency depending on their mission requirements. At the same time, some examples are relatively obvious and common to all agencies. As a rebuttable presumption, all cyber critical infrastructure and key resources identified in an agency's Homeland Security Policy Directive – 7 (HSPD-7) plans are high impact, as are all systems identified as necessary to support agency continuity of operations. Systems necessary for continuity of operations purposes include, for example, telecommunications systems identified in agency reviews under OMB's June 30, 2005, memorandum M-05-16, "Regulation on Maintaining Telecommunications Service During Crisis or Emergency in Federally-owned Buildings," implementing Section 414 the Transportation, Treasury, Independent Agencies, and General Government Appropriations Act, 2005 (Division H of Public Law 108-447).

Additionally, information systems used by agencies to provide services to other agencies such as under e-Government initiatives and lines of business, could also be high impact, but are at least moderate impact. The decision as to information system impact level in this circumstance must be agreed to by the provider and all of its customers.

16. My IG says the agency's inventory of major information systems is less than 96% complete. How do I reconcile the differing lists?

OMB expects agency IGs to provide to the agency CIO and OMB the list of systems they've identified as not being part of the agency's inventory.

17. When OMB asks if an agency has a process, are you also asking if the process is implemented and is effective?

Yes. OMB wants to know whether processes are working effectively to safeguard information and information systems. An ineffective process cannot be relied upon to achieve its information security and privacy objectives. To gauge the effectiveness of a particular IT security program process, we rely on responses to questions asked of the agency IG.

18. We often find security weaknesses requiring additional and significant resources to correct such discoveries seldom coincide with the budget process; can we delay correction until the next budget cycle?

No. Agencies must plan for security needs as they develop new and operate existing systems and as security weaknesses are identified.

OMB's policies regarding information security funding were articulated in OMB Memorandum M-00-07 dated February 28, 2000. They remain in effect, were repeated in OMB Memorandum M-06-19, and are included in OMB's budget preparation guidance, i.e., Circular A-11. In brief, agencies must do two specific things. First, they must integrate security into and fund it over the lifecycle of each system as it is developed. This requirement was codified in section 3544(b)(2)(C) of FISMA. Second, the operations of legacy (steady-state) systems must meet security requirements before funds are spent on new systems (development, modernization or enhancement).

As an example of this policy in practice, if an agency has a legacy system not currently certified and accredited, or for which a contingency plan has not been tested, these actions must be completed before spending funds on a new system. A simple way to accomplish this is to redirect the relatively modest costs of C&A or contingency plan testing from the funds intended for development, modernization or enhancement.

OMB recognizes other unanticipated security needs may arise from time-to-time. In such cases, agencies should prioritize available resources to correct the most significant weaknesses. Correcting such weaknesses would still be required prior to spending funds on development on an interim basis, and NIST's Special Publication 800-53 "Recommended Security Controls for Federal Information Systems" provides guidance for using these compensating controls.

19. You are no longer asking agencies to report significant deficiencies in the annual FISMA report. Don't we have to report them?

Not in your annual FISMA report to OMB. However, agencies must maintain all documentation supporting a finding of a significant deficiency or material weakness and make it available in a timely manner upon request by OMB or other oversight authorities.

FISMA requires agencies to report a significant deficiency as: 1) a material weakness under FMFIA, and 2) an instance of a lack of substantial compliance under FFMIA, if related to financial management systems. (See OMB Circular A-123 for further information on reporting significant deficiencies.) As you know, all security weaknesses (including those identified as a significant deficiency or material weakness) must be included in and tracked on your plan of action and milestones.

A significant deficiency is defined as a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken.

20. Should my agency's regulatory and information collection activities apply FISMA and privacy requirements?

Yes and Federal regulatory and information collection activities depend upon quality information protected from unauthorized access, use, disclosure, disruption, modification, or destruction.

Federal regulatory and information collection activities often require Federal agencies, and entities (e.g., contractors, private companies, non-profit organizations) which operate on behalf of Federal agencies, to collect, create, process, or maintain Federal government information. When developing regulations, agencies must ensure information security and privacy law and policy are applied where appropriate. Your agency's information collection activities (subject to the Paperwork Reduction Act and OMB's rule providing implementing guidance found at 5 CFR 1320), including those activities conducted or sponsored by other entities on behalf of your agency, must also ensure procedures for adequately securing and safeguarding Federal information are consistent with existing law and policy.

If your agency promulgates regulations requiring entities which operate on behalf of your agency to collect, create, process, or maintain Federal information, then procedures established by the regulation for adequately securing and safeguarding this information must be consistent with existing law and policy (e.g., FISMA, the Privacy Act, the E-Gov Act, OMB security and privacy policy, and NIST standards and guidance), regardless of whether the information is being held at the Agency or with the entity collecting, processing, or maintaining the information on behalf of the agency.

21. Are agencies allowed to utilize data services in the private sector, including "software as a service" and "software subscription" type solutions?

Yes. Agencies are permitted to utilize these types of agreements and arrangements, provided appropriate security controls are implemented, tested, and reviewed as part of your agency's information security program. We encourage agencies to seek out and utilize private sector, market-driven solutions resulting in cost savings and performance improvements – provided agency information is protected to the degree required by FISMA, FISMA implementing standards, and associated guidance. As with other contractor services and relationships, agencies should include these software solutions and subscriptions as they complete their annual security reviews.

22. How do agencies ensure FISMA compliance for connections to non-agency systems? Do Statement of Auditing Standards No. 70 (SAS 70) audits meet the requirements of FISMA and implementing policies and guidance?

NIST Special Publication 800-47 "Security Guide for Interconnecting Information Technology Systems" (August 2002) provides a management approach for interconnecting IT systems, with an emphasis on security. The document recommends development of an Interconnection Security Agreement (ISA) and a Memorandum of

Understanding (MOU). The ISA specifies the technical and security requirements of the interconnection, and the MOU defines the responsibilities of the participating organizations. The security guide recommends regular communications between the organizations throughout the life cycle of the interconnection. One or both organizations shall review the security controls for the interconnection at least annually or whenever a significant change occurs to ensure the controls are operating properly and are providing appropriate levels of protection.

Security reviews may be conducted by designated audit authorities of one or both organizations, or by an independent third party. Both organizations shall agree on the rigor and frequency of reviews as well as a reporting process.

SAS 70 audits may or may not meet the requirements of FISMA. The private sector relies on Statement on Auditing Standards (SAS) No. 70, to ensure among other purposes compliance with Section 404 of the Sarbanes-Oxley Act of 2002, requiring management assessment of internal controls. While SAS 70 reports may be sufficient to determine contractor compliance with OMB Circular A-123 and financial statement audit requirements, it is not a pre-determined set of control objectives or control activities, and therefore is not in itself sufficient to meet FISMA requirements. In addition, it is not always clear the extent to which specific systems supporting the Government activity or contract are actually reviewed as part of a particular audit. In determining whether SAS 70 reports provide sufficient evidence of contractor system FISMA compliance, it is the agency's responsibility to ensure:

- The scope of the SAS 70 audit was sufficient, and fully addressed the specific contractor system requiring FISMA review.
- The audit encompassed all controls and requirements of law, OMB policy and NIST guidance.

To reduce burden on agencies and service providers and increase efficiency, agencies and IGs should share with their counterparts at other agencies any assessment described above.

C&A

23. Why place such an emphasis on the C&A of agency information systems?

The C&A process when applied to agency information systems, provides a systematic approach for assessing security controls to determine their overall effectiveness; that is, the extent to which operational, technical, and managerial security controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Understanding the overall effectiveness of the security controls implemented in the information system is essential in determining the risk to the organization's operations and assets, to individuals, to other organizations, and to the nation resulting from the use of the system.

Agencies are reminded the C&A process is more than just planning. The continuous monitoring phase of the C&A process (discussed in NIST Special Publications 800-37 and 800-53) must include an appropriate set of management, operational, and technical controls including controls over physical access to systems and information. Agency officials and IGs should be advised of the results of this monitoring as appropriate. OMB asks CIOs to present a quantitative assessment and the IGs a qualitative assessment of the C&A process.

24. Is C&A required for all information systems? OMB Circular A-130 requires authorization to process only for general support systems and major applications.

Yes, C&A is required for all Federal information systems. Section 3544(b)(3) of FISMA refers to "subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems" and does not distinguish between major or other applications. Smaller "systems" and "applications" may be included as part of the assessment of a larger system-as allowable in NIST guidance and provided an appropriate risk assessment is completed and security controls are implemented.

25. Does OMB recognize interim authority to operate for C&A?

No. The C&A process has been required for many years, and it is important to measure the implementation of this process to improve consistency and quality Government-wide. Introducing additional inconsistency to the Government's security program would be counter to FISMA's goals.

Testing

26. Must all agency information systems be tested and evaluated annually?

Yes, all information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency must be tested at least annually. FISMA (section 3544(b)(5)) requires each agency to perform for all systems "periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually." This review shall include the testing of management, operational, and technical controls.

27. How can agencies meet the annual testing and evaluation (review) requirement?

To satisfy the annual FISMA assessment requirement, organizations can draw upon the security control assessment results from any of the following sources, including but not limited to:

- security certifications conducted as part of an information system accreditation or re-accreditation process;

- continuous monitoring activities; or
- testing and evaluation of the information system as part of the ongoing system development life cycle process (provided that the testing and evaluation results are current and relevant to the determination of security control effectiveness).

Existing security assessment results can be reused to the extent that they are still valid and are supplemented with additional assessments as needed. Reuse of assessment information is critical in achieving a broad-based, cost-effective, and fully integrated security program capable of producing the needed evidence to determine the actual security status of the information system.

FISMA does not require an annual assessment of all security controls employed in an organizational information system. In accordance with OMB policy, organizations must determine the necessary depth and breadth of an annual review and assess a subset of the security controls based on several factors, including: (i) the FIPS 199 security categorization of the information system; (ii) the specific security controls selected and employed by the organization to protect the information system; (iii) the relative comprehensiveness of the most recent past review, (iv) the adequacy and successful implementation of the plan of action and milestone (POA&M) for weaknesses in the system, (v) advice from IGs or US-CERT on threats and vulnerabilities at your agency, and (vi) the level of assurance (or confidence) that the organization must have in determining the effectiveness of the security controls in the information system, among others.

It is expected agencies will assess all of the security controls in the information system during the three-year accreditation cycle, and agencies can use the current year's assessment results obtained during security certification to meet the annual FISMA assessment requirement.

28. What NIST guidance must agencies use for their annual testing and evaluations?

For FY 2007 and beyond, agencies are required to use FIPS 200/NIST Special Publication 800-53 for the specification of security controls and NIST Special Publications 800-37 and 800-53A for the assessment of security control effectiveness. DoD and DNI may use their internal policies, directives and guidance provided that they are as stringent as the NIST security standards.

29. Why should agencies conduct continuous monitoring of their security controls?

Continuous monitoring of security controls is a cost-effective and important part of managing enterprise risk and maintaining an accurate understanding of the security risks confronting your agency's information systems. Continuous monitoring of security controls is required as part of the security C&A process to ensure controls remain effective over time (e.g., after the initial authorization or reauthorization of an

information system) in the face of changing threats, missions, environments of operation, and technologies.

Agencies should develop an enterprise-wide strategy for selecting subsets of their security controls to be monitored on an ongoing basis to ensure all controls are assessed during the three-year accreditation cycle. A robust and effective continuous monitoring program will ensure important procedures included in an agency's accreditation package (e.g., as described in system security plans, security assessment reports, and POAMs) are updated as appropriate and contain the necessary information for authorizing officials to make credible risk-based decisions regarding the security state of the information system on an ongoing basis. This will help make the C&A process more dynamic and responsive to today's federal missions and rapidly changing conditions. NIST Special Publications 800-37, 800-53, and 800-53A provide guidance on continuous monitoring programs.

30. Do agencies need to test and evaluate (review) security controls on low impact information systems?

Yes. While the depth and breadth of security controls testing and evaluation (review) will vary based on information system risk and system impact level, agencies are required to do annual testing and evaluation (review) of ALL systems. NIST Special Publications 800-37 and 800-53A provide guidance on assessment of security controls in low-impact information systems.

Configuration Management

31. What are minimally acceptable system configuration requirements?

FISMA (section 3544(b)(2)(D)(iii)) requires each agency to develop minimally acceptable system configuration requirements and ensure compliance with them. Common security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. This allows agencies to improve system performance, decrease operating costs, and ensure public confidence in the confidentiality, integrity, and availability of Government information.

Agencies are to cite the frequency by which they implement system configuration requirements. Security configuration checklists are now available for computer software widely used within the Federal Government, and they can be found on the NIST Computer Security Division web site (see: http://checklists.nist.gov) as well as the NSA System and Network Attack Center web site. Agencies must document and provide NIST with any deviations from the common security configurations (send documentation to checklists@nist.gov) and be prepared to justify why they are not using them. IGs should review such use.

OMB recently issued policy for agencies to adopt security configurations for Windows XP and VISTA, as well as policy for ensuring new acquisitions include common security

configurations. For more information, see OMB Memorandum M-07-11 "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," at: http://www.whitehouse.gov/omb/memoranda/fy2007/m07-11.pdf, and OMB Memorandum M-07-18 "Ensuring New Acquisitions Include Common Security Configurations," at: http://www.whitehouse.gov/omb/memoranda/fy2007/m07-18.pdf, respectively.

32. Why must agencies explain their performance metrics in terms of FIPS 199 categories?

FISMA directed NIST to develop a standard to categorize all information and information systems based upon the need to provide appropriate levels of information security according to a range of risk levels. "Federal Information Processing Standard 199: Standards for Security Categorization of Federal Information and Information Systems" (February 2004) defines three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). These impact levels are: low, moderate and high. Agencies must categorize their information and information systems using one of these three categories in order to comply with the minimum security requirements described in FIPS 200 and to determine which security controls in NIST Special Publication 800-53 are required. While NIST guidance does not apply to national security systems nor DoD nor DNI, OMB expects all agencies to implement a reasonably similar process.

POA&M

33. What is required of agency POA&Ms?

As outlined in previous guidance (OMB M-04-25, "FY 2004 Reporting Instructions for the Federal Information Security Management Act") agency POA&Ms must:

1) Be tied to the agency's budget submission through the unique project identifier of a system. This links the security costs for a system with the security performance of a system.

2) Include all security weaknesses found during any other review done by, for, or on behalf of the agency, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments. These plans should be the authoritative agency-wide management tool, inclusive of all evaluations.

3) Be shared with the agency IG to ensure independent verification and validation of identified weaknesses and completed corrective actions.

4) Be submitted to OMB upon request.

While agencies are no longer required to follow the exact format prescribed in the POA&M examples in M-04-25, they must still include all of the associated data elements in their POA&Ms. To facilitate compliance with POA&M reporting requirements,

agencies may choose to utilize the FISMA reporting services of a Shared Service Center as part of the Information Security Line of Business.

34. Can a POA&M process be effective even when correcting identified weaknesses is untimely?

Yes. The purpose of a POA&M is to identify and track security weaknesses in one location. A POA&M permits agency officials and oversight authorities to identify when documented corrective actions are both timely and untimely. In either circumstance, the POA&M has served its intended purpose. Agency managers can use the POA&M process to focus resources to resolve delays.

Contractor Monitoring and Controls

35. Must Government contractors abide by FISMA requirements?

Yes, and each agency must ensure their contractors are doing so. Section 3544(a)(1)(A)(ii) describes Federal agency security responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." Section 3544(b) requires each agency to provide information security for the information and "information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source." This includes services which are either fully or partially provided, including agency hosted, outsourced, and software-as-a-service (SaaS) solutions.

Because FISMA applies to both information and information systems used by the agency, contractors, and other organizations and sources, it has somewhat broader applicability than prior security law. That is, agency information security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems (whether automated or manual) – on behalf of a Federal agency. Such other organizations may include contractors, grantees, State and local Governments, industry partners, providers of software subscription services, etc. FISMA, therefore, underscores longstanding OMB policy concerning sharing Government information and interconnecting systems.

Therefore, Federal security requirements continue to apply and the agency is responsible for ensuring appropriate security controls (see OMB Circular A-130, Appendix III). Agencies must develop policies for information security oversight of contractors and other users with privileged access to Federal data. Agencies must also review the security of other users with privileged access to Federal data and systems.

Finally, because FISMA applies to Federal information and information systems, in certain limited circumstances its requirements also apply to a specific class of information technology to which Clinger-Cohen did not, i.e., "equipment that is acquired by a Federal contractor incidental to a Federal contract." Therefore, when Federal

information is used within incidentally acquired equipment, the agency continues to be responsible and accountable for ensuring FISMA requirements are met.

36. Could you provide examples of "incidental" contractor equipment which is not subject to FISMA?

In considering the answer to this question, it is essential to remember FISMA requires agencies to provide security protections "...commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or other organization on behalf of an agency." This includes services which are either fully or partially provided by another source, including agency hosted, outsourced, and SaaS solutions.

A corporate human resource or financial management system acquired solely to assist managing corporate resources assigned to a Government contract could be incidental, provided the system does not use agency information or interconnect with an agency system.

37. Could you provide examples of agency security responsibilities concerning contractors and other sources?

FISMA requires agencies to provide security protections "...commensurate with the risk and magnitude of harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; and information systems used or operated by an agency or other organization on behalf of an agency." This includes full or partial operations.

While we cannot anticipate all possible combinations and permutations, there are five primary categories of contractors as they relate to securing systems and information: 1) service providers, 2) contractor support, 3) Government Owned, Contractor Operated facilities (GOCO), 4) laboratories and research centers, and 5) management and operating contracts.

1) Service providers -- this encompasses typical outsourcing of system or network operations, telecommunications services, or other managed services (including those provided by another agency and subscribing to software services).

Agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed and such must be included in the terms of the contract. Agencies must ensure identical, not "equivalent," security procedures. For example, annual reviews, risk assessments, security plans, control testing, contingency planning, and C&A must, at a minimum, explicitly meet guidance from NIST. Additionally, IGs shall include some contractor systems in their "representative subset of agency systems," and not doing so presents an incomplete independent evaluation.

Agencies and IGs should to the maximum extent practicable, consult with other agencies using the same service provider, share security review results, and avoid the unnecessary burden on the service provider and the agencies resulting from duplicative reviews and re-reviews. Additionally, provided they meet FISMA and policy requirements, agencies and IGs should accept all or part of the results of industry-specific security reviews performed by an independent auditor on the commercial service provider.

In the case of agency service providers, they must work with their customer agencies to develop suitable arrangements for meeting all of FISMA's requirements, including any special requirements for one or more particular customer agencies. Any arrangements should also provide for an annual evaluation by the IG of one agency. Thereafter, the results of that IG evaluation would be shared with all customer agencies and their respective IGs.

2) Contractor support -- this encompasses on- or off-site contractor technical or other support staff.

Agencies are fully responsible and accountable for ensuring all FISMA and related policy requirements are implemented and reviewed and such must be included in the terms of the contract. Agencies must ensure identical, not "equivalent," security procedures. Specifically, the agency is responsible for ensuring the contractor personnel receive appropriate training (i.e., user awareness training and training on agency policy and procedures).

3) Government Owned, Contractor Operated (GOCO) -- For the purposes of FISMA, GOCO facilities are agency components and their security requirements are identical to those of the managing Federal agency in all respects. Security requirements must be included in the terms of the contract.

4) Laboratories and research facilities -- For the purposes of FISMA, laboratories and research facilities are agency components and their security requirements are identical to those of the managing Federal agency in all respects. Security requirements must be included in the terms of the contract or other similar agreement.

5) Management and Operating Contracts – For the purposes of FISMA, management and operating contracts include contracts for the operation, maintenance, or support of a Government-owned or -controlled research, development, special production, or testing establishment.

38. Should agencies include FISMA requirements in grants and contracts?

Yes, as with the Government Information Security Reform Act of 2000, agency contracts including but not limited to those for IT services must reflect FISMA requirements.

The Federal Acquisition Regulation, Subpart 7.1—Acquisition Plans, requires heads of agencies to ensure agency planners on information technology acquisitions comply with the information technology security requirements in the Federal Information Security Management Act (44 U.S.C. 3544), OMB's implementing policies including Appendix III of OMB Circular A-130, and guidance and standards from NIST.

When applicable, agencies must also include FISMA's security requirements in the terms and conditions of grants.

39. How deeply into contractor, state, or grantee systems must a FISMA review reach? To the application, to the interface between the application and their network, or into the corporate network/infrastructure?

This question has a two-part answer. First, FISMA's requirements follow agency information into any system which uses it or processes it on behalf of the agency. That is, when the ultimate responsibility and accountability for control of the information continues to reside with the agency, FISMA applies. Second, with respect to system interconnections, as a general rule, OMB assumes agency responsibility and accountability extends to the interface between Government systems (or contractor systems performing functions on behalf of the agency) and corporate systems and networks. For example, a corporate network, human resource, or financial management system would not be covered by FISMA requirements, provided the agency has confirmed appropriate security of the interface between them and any system using Government information or those operating on behalf of the agency. See also the discussions concerning interconnection agreements and C&A boundaries.

40. Are all information systems operated by a contractor on behalf of an agency subject to the same type of C&A process?

Yes, they must be addressed in the same way. As with agency-operated systems, the level of effort required for C&A depends on the impact level of the information contained on each system. C&A of a system with an impact level of low will be less rigorous and costly than a system with a higher impact level. More information on system security categorization is available in FIPS Pub 199 and NIST Special Publication 800-60 "Guide for Mapping Types of Information and Information Systems to Security Categories."

FISMA is unambiguous regarding the extent to which NIST C&A and annual IT security self-assessments apply. To the extent that contractor, state, or grantee systems process, store, or house Federal Government information (for which the agency continues to be responsible for maintaining control), their security controls must be assessed against the same NIST criteria and standards as if they were a Government-owned or -operated system. The accreditation boundary for these systems must be carefully mapped to ensure that Federal information: (a) is adequately protected, (b) is segregated from the contractor, state or grantee corporate infrastructure, and (c) there is an interconnection security agreement in place to address connections from the contractor, state or grantee

system containing the agency information to systems external to the accreditation boundary.

41. Who is responsible for the POA&M process for contractor systems owned by the contractor?

The agency is responsible for ensuring the contractor corrects weaknesses discovered through self-assessments and independent assessments. Any weaknesses are to be reflected in the agency's POA&M.

Training

42. Do employees who never access electronic information systems need annual security and privacy awareness training?

Yes, FISMA and OMB policy (Memorandum M-07-17, Attachment I.A.2.d.) require all employees to receive annual security and privacy awareness training, and they must be included as part of your agency's training totals. When administering your security and privacy awareness training programs, it is important to remember: (i) all employees collect, process, access and/or maintain government information, in some form or format, to successfully perform their duties and support the agency's mission; and (ii) information is processed in various forms and formats, including paper and electronic, and information systems are a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

43. OMB asks agencies whether they have provided information security training and awareness to all employees, including contractors. Is it the agency's responsibility to ensure contractors have security training if they are hired to perform IT security functions? Wouldn't they already be trained by their companies to perform this work?

The agency should include in its contract the requirements for level of skill and experience. However, contractors must be trained on agency-specific security policies and procedures, including rules of behavior. Agencies may explain the type of awareness training they provide to contractors as part of the response to section B.6.c.

Privacy Reporting

44. Which agency official should complete the privacy questions in this FISMA report?

These questions shall be completed or supervised by the SAOP. Since privacy management may fall into areas of responsibility likely held by several program officials, e.g., the CIO, the Privacy Act Officer, etc., the SAOP shall consult with these officials when responding to these questions, and note (Section D, part IV) those who contributed and/or reviewed the responses to the questions.

45. Why is OMB asking some of the same privacy questions posed by the annual E-Government Act Report?

OMB is using the FISMA reporting vehicle to aggregate privacy reporting requirements and reduce burden on the agencies. Privacy reporting in Section D will satisfy agencies' privacy reporting obligations under the E-Government Act. OMB will not include privacy reporting in the E-Government Act reporting template.

46. Why has OMB expanded the review of breaches of personally identifiable information, including Privacy Act violations, required by Circular A-130 to include incidents or instances of non-compliance with any of the requirements of the Act, even if they have not or will not result in civil or criminal action? Won't this result in "double counting?"

OMB is asking agencies to review all circumstances that might reveal weakness in the privacy program for which remedial action or additional training is required for an individual. Agencies should report incidents also reported elsewhere for security purposes. This reporting includes violations that are either physical or electronic, and regardless of whether the source was internal or external. While this reporting may result in double counting, it is important for agency managers and oversight authorities to understand the performance of agency privacy programs.

47. What does it mean for a system of records notice (SORN) to be "current"?
A SORN is "current" if that document satisfies the applicable requirements under the Privacy Act and there have been no subsequent substantive changes to the system which would necessitate republication of the notice in the Federal Register.

48. Must agencies publish a SORN for all systems?

No. As required by the Privacy Act (5 U.S.C. 552a), agencies must publish a SORN for systems with records about individuals maintained in a system of records covered by the Privacy Act.

49. Are agencies required to conduct a Privacy Impact Assessment (PIA) for information technology systems that contain or administer information in identifiable form strictly about Federal employees (including contractors)?

The legal and policy requirements addressing Federal agency computer security apply equally to Federal IT systems containing identifiable information about members of the public and to systems containing identifiable information solely about agency employees (or contractors). That is, as a practical matter, all systems containing information in identifiable form fall subject to the same technical, administrative and operational security controls. Although neither Section 208 of the E-Government Act, nor OMB's implementing guidance mandate agencies conduct PIAs on electronic systems containing information about Federal employees (including contractors), OMB encourages agencies to scrutinize their internal business processes and the handling of identifiable information

about employees to the same extent they scrutinize processes and information handling procedures involving information collected from or about members of the public (Memorandum M-03-22, Section II.B.3.a.).

50. If an agency chooses to conduct a PIA on systems which only contain information about Federal employees (including contractors), should these be included in the total number of systems reported in section D.II.5.c.?

No, when responding to section D.II.5.c., agencies should count only those systems which require a PIA under the E-Government Act. OMB recognizes some agencies choose to conduct a PIA on systems containing information about Federal employees (including contractors), or conduct a "threshold analysis" to determine whether a formal PIA is required for the system. While OMB applauds this level of dedication to privacy awareness and encourages agencies to continue pursuing these efforts, including these additional assessments inhibits meaningful evaluation of agency compliance with Section 208 of the E-Government Act of 2002.

51. What evidence are agencies required to provide to successfully demonstrate compliance with the privacy requirements on the quarterly report?

Agencies must provide the URL to a centrally located web page on the agency web site on which the agency lists working links to all of its PIAs and working links to all of its SORNs published in the Federal Register. Additionally, by submitting the template, the agency CIO certifies that, to the best of his or her knowledge, the annual and quarterly reports account for all of the agency and contractor systems to which the privacy requirements of the E-Government and Privacy Act are applicable.

Definitions

Adequate Security (defined in OMB Circular A-130, Appendix III, (A)(2)(a))
Security is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

Capital Planning and Investment Control Process (as defined in OMB Circular A-130, (6)(c))
A management process for ongoing identification, selection, control, and evaluation of investments in information resources. The process links budget formulation and execution, and is focused on agency missions and achieving specific program outcomes.

Certification
A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and

producing the desired outcome with respect to meeting the security requirements of the system.

General Support System or System (defined in OMB Circular A-130, Appendix III, (A)(2)(c))
An interconnected set of information resources under the same direct management control which shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people. A system can be, for example, a local area network (LAN) including smart terminals that supports a branch office, an agency-wide backbone, a communications network, a departmental data processing center including its operating system and utilities, a tactical radio network, or a shared information processing service organization (IPSO).

Information Security (defined by FISMA, section 3542(b)(1)(A-C))
Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide: (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information.

Information System (defined in OMB Circular A-130, (6)(q))
The term "information system" means a discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

Information Technology (defined by the Clinger-Cohen Act of 1996, sections 5002, 5141 and 5142)
Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For purposes of this definition, equipment is used by an agency whether the agency uses the equipment directly or it is used by a contractor under a contract with the agency which (1) requires the use of such equipment or (2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. Information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources. It does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

Major Acquisition/Investment (defined in OMB Circular A-11, section 300)
Major acquisition/investment means a system or project requiring special management attention because of its importance to the mission or function of the agency, a component of the agency or another organization; is for financial management and obligates more than $500,000 annually; has significant program or policy implications; has high

executive visibility; has high development, operating or maintenance costs or is defined as major by the agency's capital planning and investment control process.

Major Application (defined in OMB Circular A-130, (A)(2)(d))
An application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Note: All Federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by the security of the systems in which they operate.

Major Information System (defined in OMB Circular A-130)
An information system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

National Security System (defined in FISMA, section 3542 (b)(2)(A-B))
(A) The term "national security system" means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency--

(i) the function, operation, or use of which--

(I) involves intelligence activities;

(II) involves cryptologic activities related to national security;

(III) involves command and control of military forces;

(IV) involves equipment that is an integral part of a weapon or weapons system; or

(V) subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

(ii) is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

(B) Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

Plan of Action and Milestone (defined in OMB Memorandum 02-01)
A plan of action and milestones (POA&M), also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the task, and scheduled completion dates for the milestones. The purpose of the POA&M is to assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective efforts for security weaknesses found in programs and systems.

Privacy Impact Assessment (PIA) (See OMB Memorandum M-03-22)
A process for examining the risks and ramifications of using information technology to collect, maintain and disseminate information in identifiable form from or about members of the public, and for identifying and evaluating protections and alternative processes to mitigate the impact to privacy of collecting such information.

Security Controls (defined in FIPS 199)
The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Program (defined by FISMA, Section 3544(b)(1-8))
Each agency shall develop, document, and implement an agency wide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Significant Deficiency
A significant deficiency is a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken.

As required in FISMA (section 3544(c)(3)), agencies are to report any significant deficiency in policy, procedure, or practice as a material weakness in reporting under FMFIA and if relating to financial management systems, as an instance of a lack of substantial compliance under FFMIA.

System of Records Notice (SORN)
A statement providing to the public notice of the existence and character of a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.

Section B - Reporting Template for CIOs

A reporting template tool will be posted at http://www.omb.gov. Below are the questions to be included in the template, in a narrative format. This shall be completed by all agencies.

Questions in the Excel template require mostly numerical responses, and must follow the prescribed format provided. Please do not alter the questions or the reporting template. Comments and narrative to accompany quantitative answers should be provided in the comment area following each question, but, only if appropriate or necessary.

1. FISMA Systems Inventory

By component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized), identify the number of agency and contractor systems. Extend the worksheet onto subsequent pages if necessary to include all components/bureaus.

Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self-reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

FIPS 199, a Federal information processing standard, was published in February 2004. If there are systems which have not yet been categorized, or, if a system impact level was determined through another method, please explain below in item (d.).

a. Agency Systems
- By Component/Bureau: number
- By FIPS 199 system impact level (high, moderate, low, not categorized)

b. Contractor Systems
- By Component/Bureau: number
- By FIPS 199 system impact level (high, moderate, low, not categorized)

c. Total Number of Systems (Agency and Contractor Systems)
- By Component/Bureau: total number
- By FIPS 199 system impact level (high, moderate, low, not categorized)

d. If there are systems which have not yet been categorized by system impact level, or, if a system impact level was determined through another method, please explain.

2. Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

For the Total Number of Systems identified by Component/Bureau and FIPS system impact level in the Table for question 1, identify the number and percentage of systems which have: a current certification and accreditation[2], security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy.

Contingency planning is a requirement for certification and accreditation, with annual contingency plan testing required thereafter. If the number of systems with full certification and accreditation is higher than the number of systems with a tested contingency plan, please explain in 2.d. NIST does not require the testing of contingency plans of information systems at the low impact level, but consistent with previous OMB instructions, OMB does.

a. Number and percentage of systems certified and accredited
- By Component/Bureau
- By FIPS 199 system impact level (high, moderate, low, not categorized)

b. Number and percentage of systems for which security controls have been tested and reviewed in the last year
- By Component/Bureau
- By FIPS 199 system impact level (high, moderate, low, not categorized)

c. Number and percentage of systems for which contingency plans have been tested in accordance with policy
- By Component/Bureau
- By FIPS 199 system impact level (high, moderate, low, not categorized)

d. If the number of systems with full certification and accreditation is higher than the number of systems with a tested contingency plan, please explain.

e. For all systems reported as not having a C&A (Question 2.a. percentage is less than 100%), please identify the system by Component/Bureau, the system impact level, and the Unique Project Identifier (UPI) associated with the system as presented in your FY08 Exhibit 53. Extend the table as necessary to include all systems without a C&A.

[2] Certification and accreditation requires documentation of security planning, including: risk assessments, contingency plans, incident response plans, security awareness and training plans, information systems rules of behavior, configuration management plans, security configuration checklists, privacy impact assessments, and system interconnection agreements.

3. Implementation of Security Controls in NIST Special Publication 800-53

As OMB stated in last year's guidance, agencies must implement the appropriate security controls in NIST Special Publication 800-53.

a. Has the organization developed policies and corresponding procedures to cover all NIST SP 800-53 control families, and associated 800-53a controls? Yes or No.

b. Please describe your testing and continuous monitoring process.

4. Incident Detection Capabilities

a. What tools, techniques, technologies, etc., does the agency use for incident detection?

b. How many systems (or networks of systems) are protected using the tools, techniques and technologies described above?

5. Incidents

Information gathered in this question will be supplemented by your agency's reporting to United States Computer Emergency Readiness Team (US-CERT).

Identify the number of successful incidents reported to the US-CERT and the number of incidents reported to law enforcement. Explanatory comments can also be provided.

6. Security Awareness Training

a. Has the agency ensured information technology security awareness training of all employees, including contractors and those employees with significant information technology security responsibilities? Yes or No.

Report the following for your agency:

b.1. Total number of employees

b.2. Number of employees that received information technology security awareness training during the past year, as described in NIST Special Publication 800-50, "Building an Information Technology Security Awareness and Training Program" (October 2003)

b.3. Number of employees that received information technology security awareness training using an Information Systems Security Line of Business (ISSLOB) shared service. (breakout of total for 6.b.2. above)

b.4. Total number of employees with significant information technology security responsibilities

b.5. Number of employees with significant security responsibilities that received specialized training, as described in NIST Special Publication 800-16, "Information Technology Security Training Requirements: A Role- and Performance-Based Model" (April 1998).

b.6. Total costs for providing information technology security training in the past year

c. Briefly describe the training provided in 6.b.2. and 6.b.5.

7. Peer-to-Peer File Sharing

Does the agency explain policies regarding peer-to-peer file sharing in IT security awareness training, ethics training, or any other agency-wide training? Yes or No.

8. Configuration Management

a. Is there an agency-wide security configuration policy? Yes or No.

b. Approximate the extent to which applicable systems implement common security configurations established by NIST.

Response Categories:
- Rarely, for example, on approximately 0-50% of the time
- Sometimes, for example, approximately 51-70% of the time
- Frequently, for example, approximately 71-80% of the time
- Mostly, for example, approximately 81-95% of the time
- Almost Always, for example, approximately 96-100% of the time

9. Incident Reporting

Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided below.

a. The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.
b. The agency follows defined procedures for reporting to US-CERT. http://www.us-cert.gov. Yes or No.
c. The agency follows documented policies and procedures for reporting to law enforcement authorities. Yes or No.

10. New Technologies and Emerging Threats

a. Has the agency documented in its security policies special procedures for using emerging technologies (including but not limited to wireless and IPv6) and countering emerging threats (including but not limited to spyware, malware, etc.)?
Yes or No.

b. If the answer to 10 a. is "Yes," briefly describe the documented procedures. These special procedures could include more frequent control tests and evaluations, specific configuration requirements, additional monitoring, or specialized training.

11. Performance Metrics for Security Policies and Procedures

Please describe three (3) performance metrics used by your agency to measure the effectiveness or efficiency of security policies and procedures. The metrics must be different than the ones used in these FISMA reporting instructions and can be tailored from NIST's Special Publication 800-80 "Guide for Developing Performance Metrics for Information Security."

Section C – Reporting Template for IGs

A reporting template tool will be posted at http://www.omb.gov. Below are the questions to be included in the template, in a narrative format. This shall be completed by all agencies.

Questions in the Excel template require mostly numerical responses, and must follow the prescribed format provided. Please do not alter the questions or the reporting template. Comments and narrative to accompany quantitative answers should be provided in the comment area following each question, if appropriate or necessary. IGs may also submit additional narrative in an appendix to the report.

1. FISMA Systems Inventory

As required in FISMA, the IG shall evaluate a representative subset of systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.

By component/bureau and FIPS 199 system impact level (high, moderate, low, or not categorized), identify the number of agency and contractor systems, and the number of systems reviewed. Extend the worksheet onto subsequent pages if necessary to include all components/bureaus.

Agency systems shall include information systems used or operated by an agency. Contractor systems shall include information systems used or operated by a contractor of an agency or other organization on behalf of an agency. The total number of systems shall include both agency systems and contractor systems.

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self-reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider, may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

a. Agency Systems
- By Component/Bureau: total number, number reviewed
- By FIPS 199 system impact level (high, moderate, low, not categorized)

b. Contractor Systems
- By Component/Bureau: total number, number reviewed
- By FIPS 199 system impact level (high, moderate, low, not categorized)

c. Total Number of Systems (Agency and Contractor Systems)
- By Component/Bureau: total number, number reviewed
- By FIPS 199 system impact level (high, moderate, low, not categorized)

2. Certification and Accreditation, Security Controls Testing, and Contingency Plan Testing

For the Total Number of Systems reviewed by Component/Bureau and FIPS system impact level in the Table for question 1, identify the number and percentage of systems which have: a current certification and accreditation[3], security controls tested and reviewed within the past year, and a contingency plan tested in accordance with policy. NIST does not require the testing of contingency plans of information systems at the low impact level, but consistent with previous OMB instructions, OMB does.

a. Number and percentage of systems certified and accredited
   - By Component/Bureau
   - By FIPS 199 system impact level (high, moderate, low, not categorized)

b. Number and percentage of systems for which security controls have been tested and reviewed in the last year
   - By Component/Bureau
   - By FIPS 199 system impact level (high, moderate, low, not categorized)

c. Number and percentage of systems for which contingency plans have been tested in accordance with policy
   - By Component/Bureau
   - By FIPS 199 system impact level (high, moderate, low, not categorized)

3. Evaluation of Agency Oversight of Contractor Systems and Quality of Agency System Inventory

The agency performs oversight and evaluation to ensure information systems used or operated by a contractor of the agency or other organization on behalf of the agency meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy.

Agencies are responsible for ensuring the security of information systems used by a contractor of their agency or other organization on behalf of their agency; therefore, self-reporting by contractors does not meet the requirements of law. Self-reporting by another Federal agency, for example, a Federal service provider may be sufficient. Agencies and service providers have a shared responsibility for FISMA compliance.

Response Categories:
- Rarely, for example, approximately 0-50% of the time
- Sometimes, for example, approximately 51-70% of the time

[3] Certification and accreditation requires documentation of security planning, including: risk assessments, contingency plans, incident response plans, security awareness and training plans, information systems rules of behavior, configuration management plans, security configuration checklists, privacy impact assessments, and system interconnection agreements.

- Frequently, for example, approximately 71-80% of the time
- Mostly, for example, approximately 81-95% of the time
- Almost Always, for example, approximately 96-100% of the time

b. The agency has developed a complete inventory of major information systems (including major national security systems) operated by or under the control of such agency, including an identification of the interfaces between each such system and all other systems or networks, including those not operated by or under the control of the agency.

Response Categories:
- The inventory is approximately 0-50% complete
- The inventory is approximately 51-70% complete
- The inventory is approximately 71-80% complete
- The inventory is approximately 81-95% complete
- The inventory is approximately 96-100% complete

c. The IG **generally** agrees with the CIO on the number of agency-owned systems. Yes or No.

d. The IG **generally** agrees with the CIO on the number of information systems used or operated by a contractor of the agency or other organization on behalf of the agency. Yes or No.

e. The agency inventory is maintained and updated at least annually. Yes or No.

f. If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please identify the known missing systems by Component/Bureau, the Unique Project Identifier (UPI) associated with the system as presented in your FY2008 Exhibit 53 (if known), and indicate if the system is an agency or contractor system.

4. Evaluation of Agency Plan of Action and Milestones (POA&M) Process

Assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone (POA&M) process. Evaluate the degree to which each statement reflects the status in your agency by choosing from the responses provided. If appropriate or necessary, include comments in the area provided.

For each statement in items 4.a. through 4.f., select the response category that best reflects the agency's status.

Response Categories:
- Rarely, for example, approximately 0-50% of the time
- Sometimes, for example, approximately 51-70% of the time
- Frequently, for example, approximately 71-80% of the time

- Mostly, for example, approximately 81-95% of the time
- Almost Always, for example, approximately 96-100% of the time

a. The POA&M is an agency-wide process, incorporating all known information technology security weaknesses associated with information systems used or operated by the agency or by a contractor of the agency or other organization on behalf of the agency.

b. When an information technology security weakness is identified, program officials (including CIOs, if they own or operate a system) develop, implement, and manage POA&Ms for their system(s).

c. Program officials and contractors report their progress on security weakness remediation to the CIO on a regular basis (at least quarterly).

d. Agency CIO centrally tracks, maintains, and reviews POA&M activities on at least a quarterly basis.

e. IG/external audit findings are incorporated into the POA&M process.

f. POA&M process prioritizes information technology security weaknesses to help ensure significant information technology security weaknesses are addressed in a timely manner and receive appropriate resources.

5. IG Assessment of the Certification and Accreditation Process

Provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. Provide narrative comments as appropriate.

Agencies shall follow NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems" (May 2004) for certification and accreditation work initiated after May 2004. This includes use of the FIPS 199,"Standards for Security Categorization of Federal Information and Information Systems," (February 2004) to determine a system impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans.

a. The IG rates the overall quality of the Agency's certification and accreditation process as:

Response Categories:
- Excellent
- Good
- Satisfactory
- Poor
- Failing

b. The IG's quality rating included or considered the following aspects of the C&A process: (check all that apply)

-the security plan
-system impact level
-system test and evaluation
-security control testing
-incident handling
-security awareness training
-security configurations (including patch management)
-other:

6. IG Assessment of the Privacy Impact Assessment (PIA) Process

6.a. Provide a qualitative assessment of the agency's PIA process as discussed in Section D. II. 4. (SAOP reporting template), including adherence to existing policy, guidance, and standards.

Assess the overall quality of the Department's Privacy Impact Assessment policies

Response Categories:
- Excellent
- Good
- Satisfactory
- Poor
- Failing

Comments: Space for narrative comments.

6.b. Provide a qualitative assessment of the agency's progress to date in implementing the provisions of M-06-15 "Safeguarding Personally Identifiable Information" since the most recent self-review, including the agency's policies and processes, and the administrative, technical, and physical means used to control and protect personally identifiable information (PII).

Response Categories:
- Excellent
- Good
- Satisfactory

- Poor
- Failing

Comments: Space for narrative comments.

7. Configuration Management

a. Is there an agency-wide security configuration policy? Yes or No.
Space provided for narrative comments.

b. Approximate the extent to which applicable systems implement common security configurations established by NIST. Information systems using software and technology for which no common security configurations exist do not apply when answering this question.

Response Categories:
- Rarely, for example, on approximately 0-50% of the time
- Sometimes, for example, on approximately 51-70% of the time
- Frequently, for example, on approximately 71-80% of the time
- Mostly, for example, on approximately 81-95% of the time
- Almost Always, for example, on approximately 96-100% of the time

8. Incident Reporting

Indicate whether or not the agency follows documented policies and procedures for reporting incidents internally, to US-CERT, and to law enforcement. If appropriate or necessary, include comments in the area provided.

a. The agency follows documented policies and procedures for identifying and reporting incidents internally. Yes or No.
b. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). Yes or No. (http://www.us-cert.gov)
c. The agency follows documented policies and procedures for reporting to law enforcement authorities. Yes or No.

9. Security Awareness Training

Has the agency ensured security awareness training of all employees, including contractors and those employees with significant information technology security responsibilities?

Response Categories:
- Rarely, or, approximately 0-50% of employees
- Sometimes, or approximately 51-70% of employees
- Frequently, or approximately 71-80% of employees
- Mostly, or approximately 81-95% of employees

- Almost Always, or approximately 96-100% of employees

10. Peer-to-Peer File Sharing

Does the agency explain policies regarding peer-to-peer file sharing in information technology security awareness training, ethics training, or any other agency-wide training? Yes or No.

11. E-authentication Risk Assessments

The agency has completed system e-authentication risk assessments. Yes or No.

Section D - Reporting Template for SAOPs

A reporting template tool will be posted at http://www.omb.gov. Below are the questions to be included in the template, in a narrative format. This shall be completed by all agencies.

1. Inventory of Systems that Contain Federal Information in Identifiable Form which Require a PIA or SORN

In column (a) of the table below, identify by component/bureau the number of agency and contractor information systems that contain Federal information in identifiable form. In column (b), identify the number of agency and contractor systems in (a) for which a Privacy Impact Assessment (PIA) is required under the E-Gov Act. In column (c), identify the number of agency and contractor systems in (b) covered by an existing PIA. In column (d), identify the number of systems in (a) for which a system of records notice (SORN) is required under the Privacy Act. In column (e), identify the number of systems in (d) for which a current SORN has been published in the Federal Register.

Extend the table as necessary to include all Components/Bureaus.

For the purposes of this inventory, the number of systems covered by an existing PIA cannot exceed the number of systems for which a PIA is required under the E-Government Act, and the number of systems for which a current SORN has been published cannot exceed the number of systems for which a SORN is required under the Privacy Act.

a. By Component/Bureau: Number of systems that contain Federal information in identifiable form
- Agency Systems
- Contractor Systems
- Total number of systems

b. By Component/Bureau: Number of systems in (a.) for which a Privacy Impact Assessment (PIA) is required under the E-Gov Act
- Agency Systems
- Contractor Systems
- Total number of systems

c. By Component/Bureau: Number of systems in (b.) covered by an existing
- Agency Systems
- Contractor Systems
- Total number of systems
- Percentage of PIAs completed

d. By Component/Bureau: Number of systems in (a.) for which a SORN is required under the Privacy Act
- Agency Systems
- Contractor Systems

- Total number of systems

e. By Component/Bureau: Number of systems in (d.) for which a current SORN has been published in the Federal register
- Agency Systems
- Contractor Systems
- Total number of systems
- Percentage of SORNs completed

2. Links to PIAs and SORNs

a. Provide the URL (does not have to be a hyperlink) of the centrally located page on the agency web site listing working links to agency PIAs.

b. Provide the URL (does not have to be a hyperlink) of the centrally located page on the agency web site listing working links to the published SORNs:

3. Senior Agency Official for Privacy (SAOP) Responsibilities

a. Can your agency demonstrate through documentation that the privacy official participates in all agency information privacy compliance activities (i.e., privacy policy as well as IT information policy)? Yes or No.

b. Can your agency demonstrate through documentation that the privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19? Yes or No.

c. Can your agency demonstrate through documentation that the privacy official participates in assessing the impact of technology on the privacy of personal information? Yes or No.

4. Information Privacy Training and Awareness

a. Does your agency have a policy in place to ensure that all personnel (employees, contractors, etc.) with access to Federal data are generally familiar with information privacy laws, regulations and policies, and understand the ramifications of inappropriate access and disclosure? Yes or No.

b. Does your agency have a program for job-specific and comprehensive information privacy training for all personnel (employees, contractors, etc.) directly involved in the administration of personal information or information technology systems, or with significant information security responsibilities? Yes or No.

5. PIA and Web Privacy Policies and Processes

Section 208 of the E-Government Act requires that agencies (a) conduct PIAs under appropriate circumstances, (b) post web privacy policies on their web sites, and (c) ensure machine-readability of web privacy policies.

Does the agency have a written policy or process for each of the following? Indicate Yes or No for each item in the table below.

PIA Policies
a. Determining whether a PIA is needed

b. Conducting a PIA

c. Evaluating changes in business process or technology that the PIA indicates may be required

d. Ensuring that systems owners and privacy and information technology experts participate in conducting the PIA

e. Making PIAs available to the public in the required circumstances

f. Making PIAs available in other than required circumstances

Web Policies
g. Determining continued compliance with stated web policies

h. Requiring machine-readability of public-facing agency web sites (i.e. use of P3P)

6. Reviews Mandated by Privacy Act

OMB Circular A-130 (Section 3, Appendix 1) requires agencies to conduct Privacy Act mandated reviews, and to be prepared to report to the Director of OMB on the results of those reviews.

In the table provided, indicate which of the following reviews were conducted in the last year by component/bureau:

a. Section M Contracts

b. Records Practices

c. Routine Uses

d. Exemptions

e. Matching Programs

f. Training

g. Violations: Civil Action

h. Violations: Remedial Action

i. Systems of Records

Extend the table as necessary to include all components/bureaus.

7. Policy Compliance Review

a. Does the agency have current documentation demonstrating review of compliance with information privacy laws, regulations, and policies? Yes or No.

b. Can the agency provide documentation of planned, in progress, or completed corrective actions necessary to remedy deficiencies identified in compliance reviews? Yes or No.

c. Does the agency use technologies that enable continuous auditing of compliance with stated privacy policies and practices? Yes or No.

d. Does the agency coordinate with the agency's Inspector General on privacy program oversight? Yes or No.

8. Agency Use of Persistent Tracking Technology

OMB policy stated in M-03-22 "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," prohibits agencies from using persistent tracking technology on web sites, except in compelling circumstances as determined by the head of the agency (or designee reporting directly to the agency head).

Indicate Yes or No for each item in the table below.
a. Does the agency use persistent tracking technology on any web site?

b. Does the agency annually review the use of persistent tracking?

c. Can the agency demonstrate through documentation the continued justification for, and approval to use, the persistent tracking technology?

d. Can the agency provide the notice language or citation for the web privacy policy that informs visitors about the persistent tracking?

9. Contact Information

Please provide the names, phone numbers, and e-mail addresses of the following officials:

Agency head:

Chief Information Officer:

Agency Inspector General:

Chief Information Security Officer:

Senior Agency Official for Privacy:

Chief Privacy Officer:

Privacy Advocate:

Privacy Act Officer:

Reviewing Official for PIAs:

POC for URL links provided in question number 2:

TAB B

EXECUTIVE OFFICE OF THE PRESIDENT
OFFICE OF MANAGEMENT AND BUDGET
WASHINGTON, D.C. 20503

DEPUTY DIRECTOR
FOR MANAGEMENT

May 22, 2007

M-07-16

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Clay Johnson III
Deputy Director for Management

SUBJECT: Safeguarding Against and Responding to the Breach of Personally Identifiable Information

Safeguarding personally identifiable information[1] in the possession of the government and preventing its breach are essential to ensure the government retains the trust of the American public. This is a responsibility shared by officials accountable for administering operational and privacy and security programs, legal counsel, Agencies' Inspectors General and other law enforcement, and public and legislative affairs. It is also a function of applicable laws, such as the Federal Information Security Management Act of 2002 (FISMA)[2] and the Privacy Act of 1974.[3]

As part of the work of the Identity Theft Task Force,[4] this memorandum requires agencies to develop and implement a breach[5] notification policy[6] **within 120 days**. The attachments to this memorandum outline the framework within which agencies must develop this breach notification policy[7] while ensuring proper safeguards are in place to protect the information. Agencies should

---

[1] The term "personally identifiable information" refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

[2] Title III of the E-Government Act of 2002, Pub. L. No. 107-347.

[3] 5 U.S.C. § 552a.

[4] Executive Order 13402 charged the Identity Theft Task Force with developing a comprehensive strategic plan for steps the federal government can take to combat identity theft, and recommending actions which can be taken by the public and private sectors. On April 23, 2007 the Task Force submitted its report to the President, titled "Combating Identity Theft: A Strategic Plan." This report is available at www.idtheft.gov.

[5] For the purposes of this policy, the term "breach" is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.

[6] Agencies should use a best judgment standard to develop and implement a breach notification policy. Using a best judgment standard, the sensitivity of certain terms, such as personally identifiable information, can be determined in context. For example, an office rolodex contains personally identifiable information (name, phone number, etc.). In this context the information probably would not be considered sensitive; however, the same information in a database of patients at a clinic which treats contagious disease probably would be considered sensitive information. Similarly, using a best judgment standard, discarding a document with the author's name on the front (and no other personally identifiable information) into an office trashcan likely would not warrant notification to US-CERT.

[7] Terms not specifically defined within this Memorandum (*e.g.*, sensitive) should be considered to reflect the definition found in a commonly accepted dictionary.

note the privacy and security requirements addressed in this Memorandum apply to all Federal information and information systems.[8] Breaches subject to notification requirements include both electronic systems as well as paper documents. In short, agencies are required to report on the security of information systems in any formant (*e.g.*, paper, electronic, etc.). [9]

In formulating a breach notification policy, agencies must review their existing requirements with respect to Privacy and Security (see Attachment 1). The policy must include existing and new requirements for Incident Reporting and Handling (see Attachment 2) as well as External Breach Notification (see Attachment 3). Finally, this document requires agencies to develop policies concerning the responsibilities of individuals authorized to access personally identifiable information (see Attachment 4).

Within the framework set forth in the attachments, agencies may implement more stringent policies and procedures reflecting the mission of the agency. 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[10] 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.

This Memorandum should receive the widest possible distribution within your agency and each affected organization and individual should understand their specific responsibilities for implementing the procedures and requirements. 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.

Consistent with longstanding policy requiring agencies to incorporate the costs for securing their information systems, all costs of implementing this memorandum, including development,

---

[8] FISMA security requirements apply to Federal information and information systems, including both paper and electronic format.

[9] A plan to review the controls for information systems not previously included in other security reviews must be addressed in the agency's breach notification policy (*e.g.*, timeframe for completion of review, etc.); however, completion of the review for those systems is not required to be finished within the 120-day timeframe for development of the policy.

[10] In this policy, "access" means the ability or opportunity to gain knowledge of personally identifiable information.

implementation, notification to affected individuals, and any remediation activities, will be addressed through existing agency resources of the agency experiencing the breach.

Because of the many alternate ways to implement a risk-based program within the framework provided, this Memorandum, or its attachments, should not be read to mean an agency's failure to implement one or more of the many security provisions discussed within[11] would constitute less than adequate protections required by the Privacy Act. These new requirements do not create any rights or benefits, substantive or procedural, which are enforceable at law against the government.

Questions about this Memorandum should be directed to Hillary Jaffe of my staff at hjaffe@omb.eop.gov.

Attachments

[11] For example, FISMA or associated standards, policies, or guidance issued by OMB or the National Institute of Standards and Technology (NIST).

Attachment 1: Safeguarding Against the Breach of Personally Identifiable Information

This Attachment reemphasizes the responsibilities under existing law, executive orders, regulations, and policy to appropriately safeguard personally identifiable information and train employees on responsibilities in this area (Section A).[12] It also establishes two new privacy requirements and discusses five security requirements as described below (Sections B and C).

A. Current Requirements

1. Privacy Act Requirements. In particular, the Privacy Act of 1974 (Privacy Act)[13] requires each agency to:

a. Establish Rules of Conduct. Agencies are required to establish "rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of [the Privacy Act], including any other rules and procedures adopted pursuant to [the Privacy Act] and the penalties for noncompliance." (5 U.S.C. § 552a(e)(9))

b. Establish Safeguards. Agencies are also required to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained." [14]

c. Maintain accurate, relevant, timely and complete information. The Privacy Act also requires personally identifiable information within a system of records to be maintained in a manner that is accurate, relevant, timely, and complete including through the use of notices to the public.[15] It is important for agencies to fulfill their responsibilities with respect to identifying systems of records and developing and publishing notices as required by the Privacy Act and

---

[12] This Memorandum, or its attachments, should not be read to mean an agency's failure to implement one or more of the many provisions of FISMA or associated standards, policies, or guidance issued by OMB or the National Institute of Standards and Technology (NIST) would constitute less than adequate protections required by the Privacy Act of 1974.

[13] 5 U.S.C. § 552a.

[14] 5 U.S.C. § 552a (e)(10).

[15] The Privacy Act requires agencies to "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination" in their systems of records. 5 U.S.C. § 552a(e)(5).

OMB's implementing policies.[16] By collecting only the information necessary and managing it properly, agencies can often reduce the volume of information they possess, the risk to the information, and the burden of safeguarding it.

2. Security Requirements.

Below are four particularly important existing security requirements agencies already should be implementing:

a. Assign an impact level to all information and information systems. Agencies must 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). Agencies should generally consider categorizing sensitive personally identifiable information (and information systems within which such information resides) as moderate or high impact.

b. Implement minimum security requirements and controls. For each of the impact levels identified above, agencies must 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.

c. Certify and accredit information systems. Agencies must certify and accredit (C&A) all information systems supporting the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.[17] The specific procedures for conducting C&A are set out in NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, and include guidance for continuous monitoring of certain security controls. Agencies' continuous monitoring should assess a subset of the management, operational, and technical controls used to safeguard such information (*e.g.*, Privacy Impact Assessments).

d. Train employees. Agencies must initially train employees (including managers) on their privacy and security responsibilities before permitting access to agency information and information systems. Thereafter, agencies must provide at least annual refresher training to

---

[14] The Privacy Act requires agencies to publish a notice of any new or intended use of information maintained in a system of records in the Federal Register to provide an opportunity for the public to submit comments. 5 U.S.C. § 552a(e)(4). Agencies are also required to publish notice of any subsequent substantive revisions to the use of information maintained in the system of records. 5 U.S.C. § 552a(e)(11). OMB Circular A-130 ("Management of Federal Information Resources") offers additional guidance on this issue. OMB Circular A-130, App. I, sec. 4.c.

[17] 44 U.S.C. 3544(b).

ensure employees continue to understand their responsibilities.[18] Additional or advanced training should also be provided commensurate with increased responsibilities or change in duties.

Both initial and refresher training must include acceptable rules of behavior and the consequences when the rules are not followed. For agencies implementing tele-work and other authorized remote access programs, training must also include the rules of such programs.[19]

B. Privacy Requirements

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

a. Review Current Holdings. Agencies must now also review their current holdings of all personally identifiable information and ensure, to the maximum extent practicable, such holdings are accurate, relevant, timely, and complete, and reduce them to the minimum necessary for the proper performance of a documented agency function.[20] Agency-specific implementation plans and progress updates regarding this review will be incorporated as requirements in agencies' annual report under FISMA.

Following this initial review, agencies must develop and make public a schedule by which they will periodically update the review of their holdings. This schedule may be part of an agency's annual review and any consolidated publication of minor changes of Privacy Act systems of records notices.

To help safeguard personally identifiable information, agencies are reminded they must meet the requirements of FISMA and associated policies and guidance from the OMB and NIST.[21] FISMA requires each agency to implement a comprehensive security program to protect the agency's information and information systems; agency Inspectors General must independently evaluate the agency's program; and agencies must report annually to OMB and Congress on the effectiveness of their program.

---

[18] Agencies may schedule training to coincide with existing activities, such as ethics training. Communications and training related to privacy and security must be job-specific and commensurate with the employee's responsibilities. The Department of Defense, the Office of Personnel Management, and the Department of State offer agencies a minimum baseline of security awareness training as part of the Information Systems Security Line of Business.

[19] Agencies should also consider augmenting their training by using creative methods to promote daily awareness of employees' privacy and security responsibilities, such as weekly tips, mouse pads imprinted with key security reminders, privacy screens for public use of laptops, and incentives for reporting security risks.

[20] To the extent agencies are substantively performing these reviews, agencies should leverage these efforts to meet the new privacy requirements. This provision does not apply to apply to the accessioned holdings (archival records) held by the National Archives and Records Administration (NARA).

[21] The Department of Defense and Intelligence Community establish their own policy and guidance for the security of their information systems. 44 U.S.C. 3543(c).

Within the above framework, agencies may implement more stringent procedures governed by specific laws, regulations, and agency procedures to protect certain information, for example, taxpayer data, census information, and other information.

2. Reduce the Use of Social Security Numbers.

a. Eliminate Unnecessary Use. Agencies must now also review their use of social security numbers in agency systems and programs to identify instances in which collection or use of the social security number is superfluous. Within 120 days from the date of this memo, agencies must establish a plan in which the agency will eliminate the unnecessary collection and use of social security numbers within eighteen months.[22]

b. Explore Alternatives. Agencies must 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.).

C. Security Requirements

While agencies continue to be responsible for implementing all requirements of law and policy, below are five requirements[23] agencies must implement which derive from existing security policy and NIST guidance. These requirements are applicable to all Federal information, *e.g.*, law enforcement information, etc.

- Encryption. Encrypt, using only NIST certified cryptographic modules, [24] all data on mobile computers/devices carrying agency data unless the data is determined not to be sensitive, in writing, by your Deputy Secretary[25] or a senior-level individual he/she may designate in writing;
- Control Remote Access. Allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access;
- Time-Out Function. Use a "time-out" function for remote access and mobile devices requiring user re-authentication after thirty minutes of inactivity;
- Log and Verify. Log all computer-readable data extracts from databases holding sensitive information and verify each extract, including whether sensitive data has been erased within 90 days or its use is still required; and

---

[22] Agencies with questions addressing this assignment regarding the Paperwork Reduction Act of 1995 (44 U.S.C. 3501 *et seq.*) should contact their respective desk officer at the Office of Management and Budget.
[23] See OMB Memo 06-16 "Protection of Sensitive Agency Information" (www.whitehouse.gov/omb/memoranda/fy2006/m06-16.pdf).
[24] See NIST's website at http://csrc.nist.gov/cryptval/ for a discussion of the certified encryption products.
[25] Non cabinet agencies should consult the equivalent of a Deputy Secretary.

- Ensure Understanding of Responsibilities. Ensure all individuals with authorized access to personally identifiable information and their supervisors sign at least annually a document clearly describing their 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.

Attachment 2: Incident Reporting and Handling Requirements

This Attachment applies to security incidents involving the breach of personally identifiable information whether in electronic or paper format. For the purposes of reporting, agencies must continue to follow existing requirements, as modified and described below.

A. Existing Requirements

1. FISMA Requirements. FISMA requires each agency to:

- 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.[26]
- implement NIST guidance and standards[27]

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*[28]; 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).[29]

---

[26] 44 U.S.C. § 3544(b)(7).

[27] For additional information on NIST guidance and standards, see www.nist.gov.

[28] See "Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology" (http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61.pdf).

[29] The responsibilities of US-CERT are outlined in 44 U.S.C. § 3546. Its complete set of operating procedures may be found on the US-CERT website (www.us-cert.gov/federal/reportingRequirements.html). Separate procedures are in place for the Department of Defense as identified in Directive O-8530-1 and all components report incidents to the Joint Task Force Global Network Operations (JTF-GNO), which, in turn, coordinates directly with the US-CERT.

2. Incident Handling and Response Mechanisms. When faced with a security incident, an agency must be able to respond in a manner protecting both its own information and helping to protect the information of others who might be affected by the incident. To address this need, agencies must establish formal incident response mechanisms. To be fully effective, incident handling and response must also include sharing information concerning common vulnerabilities and threats with those operating other systems and in other agencies. In addition to training employees on how to prevent incidents, all employees must also be instructed in their roles and responsibilities regarding responding to incidents should they occur.

B. Modified Agency Reporting Requirements

1. US-CERT Modification. Agencies must report all incidents involving personally identifiable information to US-CERT. This reporting requirement does not distinguish between potential and confirmed breaches. The US-CERT concept of operations for reporting Category 1 incidents is modified as follows:

> Category 1. Unauthorized Access or Any Incident Involving Personally Identifiable Information. In this category agencies must report when: 1) an individual gains logical or physical access without permission to a federal agency network, system, application, data, or other resource; or 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.
>
> - 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.

2. Develop and Publish a Routine Use.

a. Effective Response. A federal agency's ability to respond quickly and effectively in the event of a breach of federal data is critical to its efforts to prevent or minimize any consequent

harm.[30] 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.

b. Disclosure of Information. Often, the information to be disclosed to such persons and entities is maintained by federal agencies and is subject to the Privacy Act (5 U.S.C. § 552a). The Privacy Act prohibits the disclosure of any record in a system of records by any means of communication to any person or agency absent the written consent of the subject individual, unless the disclosure falls within one of twelve statutory exceptions.31 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:

> To appropriate agencies, entities, and persons when (1) [the agency] suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.[32]

As described in the President's Identity Theft Task Force's Strategic Plan, all agencies should publish a routine use for their systems of records allowing for the disclosure of information in the course of responding to a breach of federal data.[33] Such a routine use will serve to protect the interests of the individuals whose information is at issue by allowing agencies to take appropriate steps to facilitate a timely and effective response, thereby improving their ability to prevent, minimize, or remedy any harm resulting from a compromise of data maintained in their systems of records.

---

[30] Here, "harm" means damage, fiscal damage, or loss or misuse of information which adversely affects one or more individuals or undermines the integrity of a system or program.

[31] 5 U.S.C. §§ 552a(b)(1)-(12).

[32] See Appendix B of the Identity Theft Task Force report (www.identitytheft.gov/reports/StrategicPlan.pdf).

[33] *Id.*

Attachment 3: External Breach Notification

To ensure consistency across government, 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.[34] This Attachment does not attempt to set a specific threshold for external notification since breaches are specific and context dependant and notification is not always necessary or desired. The costs of any notifications must be borne by the agency experiencing the breach from within existing resources.

A. Background

1. Harm. Breaches can implicate a broad range of harms to individuals, including the potential for identity theft; however, this Section does not discuss actions to address possible identity theft or fraud. Agencies are referred to the ID Theft Task Force's Strategic Plan for guidance.

2. Requirement. Agencies must implement the one specific new requirement discussed below; *i.e.*, develop a breach notification policy and plan (see Section B. below).

3. Threshold questions. Both the decision to provide external notification on the occasion of a breach and the nature of the notification will require agencies to resolve a number of threshold questions.[35] The likely risk of harm and the level of impact will determine when, what, how and to whom notification should be given.[36]

Notification of those affected and/or the public allows those individuals the opportunity to take steps to help protect themselves from the consequences of the breach. Such notification is also consistent with the "openness principle" of the Privacy Act that calls for agencies to inform individuals about how their information is being accessed and used, and may help individuals mitigate the potential harms resulting from a breach.

4. Chilling Effects of Notices. A number of experts have raised concerns about unnecessary notification and the chilling effect this may have on the public.[37] In addition, agencies should

---

[34] These factors do not apply to an agency's notification to US-CERT. Agencies must report all incidents – potential and confirmed – involving personally identifiable information to US-CERT.

[35] Notice may not be necessary if, for example, the information is properly encrypted because the information would be unusable.

[36] See OMB's September 20, 2006 memorandum titled "Recommendations for Identity Theft Related Data Breach Notification" for information and recommendations for planning and responding to data breaches which could result in identity theft (www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf).

[37] Federal Trade Commission, *Prepared Statement of the Federal Trade Commission Before the Committee on Commerce, Science, and Transportation, U.S. Senate, on Data Breaches and Identity Theft* (Washington, D.C.: June 16, 2005), p. 10. In this testimony, the Federal Trade Commission raised concerns about the threshold for which consumers should be notified of a breach, cautioning that too strict a standard could have several negative effects.

consider the costs to individuals and businesses of responding to notices where the risk of harm may be low. Agencies should exercise care to evaluate the benefit of notifying the public of low impact incidents.

B. New Requirement

Each agency should develop a breach notification policy and plan comprising the elements discussed in this Attachment. In implementing the policy and plan, the Agency Head will make final decisions regarding breach notification.

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

To ensure adequate coverage and implementation of the 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.[38] A more detailed description of these elements is set forth below:

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. Agencies should consider a wide range of harms, such as harm to reputation and the potential for harassment or prejudice, particularly when health or financial benefits information is involved in the breach.[39] Agencies should bear in mind that notification when there is little or no risk of harm might create

---

[38] Non-Cabinet-level agencies should include their functional equivalent.

[39] For reference, the express language of the Privacy Act requires agencies to consider a wide range of harms: agencies shall "establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." 5 U.S.C. § 552a (e)(10).

unnecessary concern and confusion.[40] Additionally, under circumstances where notification could increase a risk of harm, the prudent course of action may be to delay notification while appropriate safeguards are put in place.

Five factors should be considered to assess the likely risk of harm:

a. Nature of the Data Elements Breached. The nature of the data elements compromised is a key factor to consider in determining when and how notification should be provided to affected individuals.[41] It is difficult to characterize data elements as creating a low, moderate, or high risk simply based on the type of data because the sensitivity of the data element is contextual. A name in one context may be less sensitive than in another context.[42] In assessing the levels of risk and harm, consider the data element(s) in light of their context and the broad range of potential harms flowing from their disclosure to unauthorized individuals.

b. Number of Individuals Affected. The magnitude of the number of affected individuals may dictate the method(s) you choose for providing notification, but should not be the determining factor for whether an agency should provide notification.

c. Likelihood the Information is Accessible and Usable. Upon learning of a breach, agencies should assess the likelihood personally identifiable information will be or has been used by unauthorized individuals. An increased risk that the information will be used by unauthorized individuals should influence the agency's decision to provide notification.

The fact the information has been lost or stolen does not necessarily mean it has been or can be accessed by unauthorized individuals, however, depending upon a number of physical, technological, and procedural safeguards employed by the agency. (See Attachment 1 above.) If the information is properly protected by encryption, for example, the risk of compromise may be low to non-existent.[43]

Agencies will first need to assess whether the personally identifiable information is at a low, moderate, or high risk of being compromised. The assessment should be guided by NIST

---

[40] Another consideration is a surfeit of notices, resulting from notification criteria which are too strict, could render all such notices less effective, because consumers could become numb to them and fail to act when risks are truly significant.

[41] For example, theft of a database containing individuals' names in conjunction with Social Security numbers, and/or dates of birth may pose a high level of risk of harm, while a theft of a database containing only the names of individuals may pose a lower risk, depending on its context.

[42] For example, breach of a database of names of individuals receiving treatment for contagious disease may pose a higher risk of harm, whereas a database of names of subscribers to agency media alerts may pose a lower risk of harm.

[43] In this context, proper protection means encryption has been validated by NIST.

security standards and guidance. Other considerations may include the likelihood any unauthorized individual will know the value of the information and either use the information or sell it to others.

d. Likelihood the Breach May Lead to Harm

1. Broad Reach of Potential Harm. The Privacy Act requires agencies to protect against any anticipated threats or hazards to the security or integrity of records which could result in "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."[44] Additionally, 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 and emotional distress, the disclosure of address information for victims of abuse, the potential for secondary uses of the information which could result in fear or uncertainty, or the unwarranted exposure leading to humiliation or loss of self-esteem.

2. Likelihood Harm Will Occur. The likelihood a breach may result in harm will depend on the manner of the actual or suspected breach and the type(s) of data involved in the incident. Social Security numbers and account information are useful to committing identity theft, as are date of birth, passwords, and mother's maiden name. If the information involved, however, is a name and address or other personally identifying information, the loss may also pose a significant risk of harm if, for example, it appears on a list of recipients patients at a clinic for treatment of a contagious disease.

In considering whether the loss of information could result in identity theft or fraud, agencies should consult guidance from the Identity Theft Task Force.[45]

e. Ability of the Agency to Mitigate the Risk of Harm. Within an information system, the risk of harm will depend on how the agency is able to mitigate further compromise of the system(s) affected by a breach. 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.[46] Such mitigation may not prevent the use of the personal information for identity theft, but it can limit the associated harm. Some harm may be more difficult to mitigate than others, particularly where the potential injury is more individualized and may be difficult to determine.

---

[44] 5 U.S.C. § 552a(e)(10).

[45] See "Recommendations for Identity Theft Related Data Breach Notification" (www.whitehouse.gov/omb/memoranda/fy2006/task_force_theft_memo.pdf).

[46] For example, if the information relates to disability beneficiaries, monitoring a beneficiary database for requests for change of address may signal fraudulent activity.

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. In some circumstances, law enforcement or national security considerations may require a delay if it would seriously impede the investigation of the breach or the affected individual. However, any delay should not exacerbate risk or harm to any affected individual(s).

3. Source of the Notification

In general, notification to individuals affected by the breach should be issued by the Agency Head, or senior-level individual he/she may designate in writing, or, in those instances where the breach involves a publicly known component of an agency, such as the Food and Drug Administration or the Transportation Security Administration, the Component Head. This demonstrates it has the attention of the chief executive of the organization. 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 or Senior Agency Official for Privacy. This approach signals the agency recognizes both the security and privacy concerns raised by the breach.

When the 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. The roles, responsibilities, and relationships with contractors or partners should be reflected in your breach notification policy and plan, your system certification and accreditation documentation, and contracts and other documents.

4. Contents of the Notification

The notification should be provided in writing and should be concise, conspicuous, plain language. 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.

Given the amount of information required above, you may want to consider layering the information as suggested in Section 5 below, providing the most important information up front, with the additional details in a Frequently Asked Questions (FAQ) format or on your web site. If you have knowledge the affected individuals are not English speaking, notice should also be provided in the appropriate language(s). You may seek additional guidance on how to draft the notice from the Federal Trade Commission, a leader in providing clear and understandable notices to consumers, as well as from communication experts who may assist you in designing model notices.[47] A standard notice should be part of your approved breach plan.

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. Notice provided to individuals affected by a breach should be commensurate with the number of people affected and the urgency with which they need to receive notice. The following examples are types of notice which may be considered.

a. Telephone. Telephone notification may be appropriate in those cases where urgency may dictate immediate and personalized notification and/or when a limited number of individuals are affected. Telephone notification, however, should be contemporaneous with written notification by first-class mail.

---

[47] Additional guidance on how to draft a notice is available in the FTC publication titled "Dealing with a Data Breach" (www.ftc.gov/bcp/edu/microsites/idtheft/business/data-breach.html). Although the brochure is designed for private sector entities that have experienced a breach, it contains sample notice letters that could also serve as a model for federal agencies. You may also seek guidance from communications experts who may assist you in designing model notices.

b. First-Class Mail. First-class mail notification to the last known mailing address of the individual in your agency's records should be the primary means notification is provided. Where you have reason to believe the address is no longer current, you should take reasonable steps to update the address by consulting with other agencies such as the US Postal Service. The notice should be sent separately from any other mailing so that it is conspicuous to the recipient. If the agency which experienced the breach uses another agency to facilitate mailing (for example, if the agency which suffered the loss consults the Internal Revenue Service for current mailing addresses of affected individuals), care should be taken to ensure the agency which suffered the loss is identified as the sender, and not the facilitating agency. The front of the envelope should be labeled to alert the recipient to the importance of its contents, *e.g.*, "Data Breach Information Enclosed" and should be marked with the name of your agency as the sender to reduce the likelihood the recipient thinks it is advertising mail.

c. E-Mail. E-mail notification is problematic, because individuals change their e-mail addresses and often do not notify third parties of the change. Notification by postal mail is preferable. However, where an individual has provided an e-mail address to you and has expressly given consent to e-mail as the primary means of communication with your agency, and no known mailing address is available, notification by e-mail may be appropriate. E-mail notification may also be employed in conjunction with postal mail if the circumstances of the breach warrant this approach. E-mail notification may include links to the agency and www.USA.gov[48] web sites, where the notice may be "layered" so the most important summary facts are up front with additional information provided under link headings.

d. Existing Government Wide Services. Agencies should 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.

e. Newspapers or other Public Media Outlets. Additionally, you may supplement individual notification with placing notifications in newspapers or other public media outlets. You should also set up toll-free call centers staffed by trained personnel to handle inquiries from the affected individuals and the public.

f. Substitute Notice. Substitute notice in those instances where your agency does not have sufficient contact information to provide notification. Substitute notice should consist of a conspicuous posting of the notice on the home page of your agency's web site and notification to major print and broadcast media, including major media in areas where the affected individuals reside. The notice to media should include a toll-free phone number where an individual can learn whether or not his or her personal information is included in the breach.

---

[48] The current domain name for the Federal Internet portal required by section 204 of the E-Government Act of 2002 is www.usa.gov.

g. Accommodations. Special consideration to providing notice to individuals who are visually or hearing impaired consistent with Section 508 of the Rehabilitation Act of 1973 should be given. Accommodations may include establishing a Telecommunications Device for the Deaf (TDD) or posting a large type notice on the agency web site.

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

a. Notification of Individuals. The final consideration in the notification process when providing notice is to whom you should provide notification: the affected individuals, the public media, and/or other third parties affected by the breach or the notification. Unless notification to individuals is delayed or barred for law enforcement or national security reasons, once it has been determined to provide notice regarding the breach, affected individuals should receive prompt notification.

b. Notification of Third Parties including the Media. If communicating with third parties regarding a breach, agencies should consider the following.

1. Careful Planning. An agency's decision to notify the public media will require careful planning and execution so that it does not unnecessarily alarm the public. When appropriate, public media should be notified as soon as possible after the discovery of a breach and the response plan, including the notification, has been developed. Notification should focus on providing information, including links to resources, to aid the public in its response to the breach. Notification may be delayed upon the request of law enforcement or national security agencies as described above in Section 2. To the extent possible, when necessary prompt public media disclosure is generally preferable because delayed notification may erode public trust.

2. Web Posting. Agencies should post information about the breach and notification in a clearly identifiable location on the home page of your agency web site as soon as possible after the discovery of a breach and the decision to provide notification to the affected individuals. 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.[49] The information should also appear on the www.USA.gov web site. You may also consult with GSA's USA Services regarding using their call center.

3. Notification of other Public and Private Sector Agencies. Other public and private sector agencies may need to be notified on a need to know basis, particularly those that may be

[49] See the FAQ posted by the Department of Veterans Affairs in response to the May 2006 incident for examples of links to identity theft resources and a sample FAQ (www.usa.gov/veteransinfo.shtml).

affected by the breach or may play a role in mitigating the potential harms stemming from the breach.[50]

4. Congressional Inquiries. Agencies should be prepared to respond to inquires from other governmental agencies such as the Government Accountability Office and Congress.

c. 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.[51] The impact levels – low, moderate, and high, describe the (worst case) potential impact on an organization or individual if a breach of security occurs.[52]

- **Low:** the loss of confidentiality, integrity, or availability is expected to have a **limited** adverse effect on organizational operations, organizational assets or individuals
- **Moderate:** the loss of confidentiality, integrity, or availability is expected to have a **serious** adverse effect on organizational operations, organizational assets or individuals.
- **High:** the loss of confidentiality, integrity, or availability is expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets or individuals.

The impact levels will help determine when and how notification should be provided. Where there is a range of risk levels attributed to the factors, the decision to provide notification should give greater weight to the likelihood the information is accessible and usable and whether the breach may lead to harm. If agencies appropriately apply the five risk factors discussed in section 1 of this attachment within the fact-specific context, it is likely notification will only be given in those instances where there is a reasonable risk of harm and will not lead to the overuse of notification.

---

[50] For example, a breach involving medical information may warrant notification of the breach to health care providers and insurers through the public or specialized health media, and a breach of financial information may warrant notification to financial institutions through the federal banking agencies.

[51] See FIPS 199 and Attachment 1 of this memorandum. Reassessment is suggested as the context of any breach may alter your original designation.

[52] The determination of the potential impact of loss of information is made by the agency during an information system's certification and accreditation process.

Attachment 4: Rules and Consequences

A. New Requirement: Rules and Consequences Policy.

Fairness requires that managers, supervisors and employees be informed and trained regarding their respective responsibilities relative to safeguarding personally identifiable information and the consequences and accountability for violation of these responsibilities. Therefore, it is the 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. Consequences should be commensurate with level of responsibility and type of personally identifiable information involved. Supervisors also must be reminded of their responsibility to instruct, train and supervise employees on safeguarding personally identifiable information. Agencies should develop and implement these policies in accordance with the agency's respective existing authorities.

As with any disciplinary action, the particular facts and circumstances, including whether the breach was intentional, will be considered in taking appropriate action. Supervisors also should be reminded that any action taken must be consistent with law, regulation, applicable case law, and any relevant collective bargaining agreement. Supervisors should understand they may be subject to disciplinary action for failure to take appropriate action upon discovering the breach or failure to take required steps to prevent a breach from occurring.

Agencies having questions regarding development of a rules and consequences policy may contact OPM's Center for Workforce Relations and Accountability Policy at (202) 606-2930.

1. 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.

2. 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[53] or unauthorized disclosure of personally identifiable information;

---

[53] Here, "control" means the authority of the government agency that originates information, or its successor in function, to regulate access to the information. Having control is a condition or state and not an event. Loss of control is also a condition or state which may or may not lead to an event, *i.e.*, a breach.

- 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.

3. 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.

TAB C

DoD Supplementary of FY07 FISMA (Narrative Statement) Privacy Guidance

References:

(a) The Privacy Act of 1974, as amended (5 USC 552a)

(b) E-Government Act of 2002, Section 208 (Public Law 107-347)

(c) OMB Circular A-130, Appendix I, February 25, 2003

(d) OMB Memo, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, September 26, 2003

(e) OMB Memo, M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007

(f) DoD Directive 5400.11, "DoD Privacy Program," May 8, 2007

(g) DoD 5400.11-R, "DoD Privacy Program," May 14, 2007

(h) Deputy Secretary of Defense Memorandum, "Web Site Administration," December 17, 1998, as amended

Introduction

This guidance is intended to supplement and expand upon the OMB guidance. Therefore, it shall be read in conjunction with that guidance. Each of the OMB questions is discussed below where, if appropriate, expanded guidance is furnished regarding how the review should be conducted. If there is a conflict between the OMB guidance and the supplementary guidance, the OMB guidance shall be followed.

Though many of the OMB questions are framed as "yes" or "no" questions, each answer shall be supported by a narrative statement that expands upon the Component reply. Because the DoD Privacy Program is decentralized, the approach taken by Components is not uniform. In order to properly reflect the current DoD program, a detailed explanation shall be furnished for each question, where applicable, so that a complete picture may be obtained for the Component's Privacy Program.

In responding to each of the OMB questions, care must be taken to document how you arrived at your response. Though unknown, it may be that the Privacy section of the FISMA report will be independently evaluated. We must ensure that the responses furnished by the Components and the Department are in fact supportable. Therefore, it is imperative that you ensure, incident to preparing the Component's report, that the information being provided is based on Component policies, procedures and practices.

References (a) through (g) can be found at www.defenselink.mil/privacy and reference (h) at www.defenselink.mil/webmasters. A copy of reference (b) is set forth as Attachment B to OMB Memo M-07-19 (reference (d)).

Section D – Reporting Narrative Statement for Senior Agency Officials for Privacy (SAOP)

1. Inventory of Systems that Contain Federal Information in Identifiable Form which requires a Privacy Impact Access (PIA) or System of Records Notice (SORN).

Background: All IT systems do not contain identifiable information on individuals. This question is only directed at those IT systems, either within or without the Component IT Registry, containing information about U.S. citizens and resident aliens. A PIA is required whenever a new or a substantially altered IT system will collect, maintain, or disseminate information on such individuals unless the system is exempt from the PIA requirement pursuant to the E-Gov Act, as implemented by OMB. In addition, not all IT systems containing information about U.S. citizens and resident aliens are covered by the Privacy Act. IT systems are only covered when information about individuals is retrieved by the name of the individual or some other unique personal identifier. If so retrieved, a Privacy Act system of records notice must be published in the Federal Register giving notice as to the existence and character of the system.

In summary, not all IT systems contain identifiable information; but if they do, a PIA is required unless exempt. IT systems containing such information that is retrieved by a name or other identifier are covered by the Privacy Act, thus triggering the need for publication of a system of records notice in the Federal Register. In short, a PIA may be required, but a Privacy Act system of records notice may not be.

2. Links to PIAs and SORNs

a. Provide your Component link to your Privacy Impact Assessments (PIAs) as stated in question 2a. of the SAOP.
b. To ensure the accurate answer on the location of SORNS, the Defense Privacy Office's website URL http://www.defenselink.mil/privacy/ is provided.

3. Senior Agency Official for Privacy (SAOP) Responsibilities

It is recognized that the senior Component official having oversight responsibility for privacy normally is not directly involved in the day-to-day operations of the Component Privacy Program. Section 3a, 3b, and 3c are self-explanatory; please provide documentation to your answers in the narrative.

4. Information Privacy Training and Awareness

Questions 4a and 4b: DoD 5400.11-R, Chapter 7, establishes the privacy training requirements for the agency. Paragraph C7.4.1 provides that each DoD Component is responsible for the

development of training procedures and methodology. If your training requirements are set forth in Component regulatory or other authority, identify such authority and advise what those training policies are, keyed to the specific OMB questions being asked. It is acknowledged that each Component has developed training programs that best serve its Component. The Component shall report what those training programs are. To the extent some Components have developed non-standard training, such as web-based training or video Conference training, the Component shall identify such programs and include an assessment as to their success or failure.

5. PIA and Web Privacy Polices and Processes

Questions 5a through 5h will be answer by the DoD office of the CIO.

6. Reviews Mandated by Privacy Act

All Components shall complete section 6a through 6i in the OMB template.

Appendix I, paragraph 3 of the OMB Circular A-130 provides that each agency shall conduct a review with a frequency as specified in the Circular and be prepared to report to OMB the results of such reviews and the corrective actions taken to resolve problems uncovered. For example, Section M contracts are reviewed every two years, routine uses are reviewed every four years, and matching programs are reviewed annually.

It is possible that a review for one or more of the identified areas will not be conducted in FY07. If a review is not conducted, advice when the review was last conducted or when it will be conducted. It is recognized that Components with a significant number of Privacy Act systems of records are not able to review each and every system notice for which it has responsibility. Where so, the Component shall indicate how it accomplishes the mandated OMB reviews, e.g., a statistical viable sample is reviewed, etc.

Insofar as the review for matching programs is concerned, Components need not respond. Computer Matching for the Department is centralized and the Defense Privacy Office, which has direct responsibility for the Department's matching program, shall address this part of the question.

7. Policy Compliance Review

The Component Privacy Official must coordinate with the Component CIO to determine what compliance technologies are used to ensure that IT systems are being monitored to ensure that they are being operated consistent with law and regulation. This question covers both IT systems that are subject to the PIA requirement but not the Privacy Act and those IT systems that are covered by both the PIA requirement and the Privacy Act notice requirement.

Each Component shall identify those circumstances where it coordinates with its IG in the administration of its privacy program. To the extent the Component regulatory or other authority provides for IG involvement, the authority shall be identified. If such authority does not exist,

each Component shall discuss to what extent, if any, the IG has been involved in the areas identified by OMB.

If a Component does not identify a compliance deficiency, the DoD Privacy office should be advice in the narrative as an enclosure. Identification of deficiencies is based, in part, on whether the Component has established compliance policies, procedures, and practices.

8. Agency Use of Persistent Tracking Technology

Section 8a, 8b, 8c will be answered by the CIO DoD office.

9. Contact Information

Self Explanatory.

TAB D

Section D - Senior Agency Official for Privacy (SAOP): Question 1

Agency Name: **Submission date:**

1. Inventory of Systems that Contain Federal Information in Identifiable Form which require a PIA or SORN

In column (a) of the table below, identify by component/bureau the number of agency and contractor information systems that contain Federal information in identifiable form. In column (b), identify the number of agency and contractor systems in (a) for which a Privacy Impact Assessment (PIA) is required under the E-Gov Act. In column (c), identify the number of agency and contractor systems in (b) covered by an existing PIA. In column (d), identify the number of systems in (a) for which a system of records notice (SORN) is required under the Privacy Act. In column (e), identify the number of systems in (d) for which a current SORN has been published in the Federal Register.

Extend the table as necessary to include all components/bureaus.

For the purposes of this inventory, the number of systems covered by an existing PIA cannot exceed the number of systems for which a PIA is required under the E-Government Act, and the number of systems for which a current SORN has been published cannot exceed the number of systems for which a SORN is required under the Privacy Act.

	a. Number of systems that contain Federal information in identifiable form			b. Number of systems in (a) for which a Privacy Impact Assessment (PIA) is required under the E-Gov Act			c. Number of systems in (b) covered by an existing PIA				d. Number of systems in (a) for which a system of records notice (SORN) is required under the Privacy Act			e. Number of systems in (d) for which a current SORN has been published in the Federal Register			
Component/Bureau	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	% Complete	Agency Systems	Contractor Systems	Total Systems	Agency Systems	Contractor Systems	Total Systems	% Complete
Example Component ABC	*100*	*100*	*200*	*75*	*35*	***110***	*75*	*25*	***100***	***91%***	*82*	*69*	***151***	*80*	*68*	***148***	***98%***
			0			**0**			**0**				**0**			**0**	
			0			**0**			**0**				**0**			**0**	
			0			**0**			**0**				**0**			**0**	
			0			**0**			**0**				**0**			**0**	
			0			**0**			**0**				**0**			**0**	
			0			**0**			**0**				**0**			**0**	
			0			**0**			**0**				**0**			**0**	
			0			**0**			**0**				**0**			**0**	
			0			**0**			**0**				**0**			**0**	
			0			**0**			**0**				**0**			**0**	
			0			**0**			**0**				**0**			**0**	
			0			**0**			**0**				**0**			**0**	
			0			**0**			**0**				**0**			**0**	
			0			**0**			**0**				**0**			**0**	
			0			**0**			**0**				**0**			**0**	
			0			**0**			**0**				**0**			**0**	
			0			**0**			**0**				**0**			**0**	
			0			**0**			**0**				**0**			**0**	
			0			**0**			**0**				**0**			**0**	

Section D - Senior Agency Official for Privacy (SAOP): Questions 2, 3, 4, and 5

Agency Name:

2. Links to PIAs and SORNS		
2.a.	Provide the URL of the centrally located page on the agency web site listing working links to agency PIAs: (Hyperlink not required)	
2.b.	Provide the URL of the centrally located page on the agency web site listing working links to the published SORNs: (Hyperlink not required)	

3. Senior Agency Official for Privacy (SAOP) Responsibilities		
3.a.	Can your agency demonstrate through documentation that the privacy official participates in all agency information privacy compliance activities (i.e., privacy policy as well as IT information policy)? Yes or No.	
3.b.	Can your agency demonstrate through documentation that the privacy official participates in evaluating the ramifications for privacy of legislative, regulatory and other policy proposals, as well as testimony and comments under Circular A-19? Yes or No.	
3.c.	Can your agency demonstrate through documentation that the privacy official participates in assessing the impact of technology on the privacy of personal information? Yes or No.	

4. Information Privacy Training and Awareness		
4.a.	Does your agency have a policy in place to ensure that all personnel (employees, contractors, etc.) with access to Federal data are generally familiar with information privacy laws, regulations and policies, and understand the ramifications of inappropriate access and disclosure? Yes or No.	
4.b.	Does your agency have a program for job-specific and comprehensive information privacy training for all personnel (employees, contractors, etc.) directly involved in the administration of personal information or information technology systems, or with significant information security responsibilities? Yes or No.	

5. PIA and Web Privacy Policies and Processes

Section 208 of the E-Government Act requires that agencies (a) conduct PIAs under appropriate circumstances, (b) post web privacy policies on their web sites, and (c) ensure machine-readability of web privacy policies.

Does the agency have a written policy or process for each of the following? Indicate Yes or No for each item in the table below.

PIA Policies		
a.	Determining whether a PIA is needed	
b.	Conducting a PIA	
c.	Evaluating changes in business process or technology that the PIA indicate as necessary	
d.	Ensuring systems owners and privacy and IT experts participate in conducting the PIA	
e.	Making PIAs available to the public in the required circumstances	
f.	Making PIAs available in other than required circumstances	
Web Policies		
g.	Determining continued compliance with stated web policies	
h.	Requiring machine-readability of public-facing agency web sites (i.e. use of P3P)	

Section D - Senior Agency Official for Privacy (SAOP): Question 6

6. Reviews Mandated by Privacy Act

6.a. OMB Circular A-130 (Section 3, Appendix 1) requires agencies to conduct Privacy Act mandated reviews, and to be prepared to report to the Director of OMB on the results of those reviews.

In the table provided, indicate which reviews were conducted in the last year by component/bureau by placing an X in the corresponding cells.

Extend the table as necessary to include all components/bureaus.

Component/Bureau	a. Section M Contracts	b. Records Practices	c. Routine Uses	d. Exemptions	e. Matching Programs	f. Training	g. Violations: Civil Action	h. Violations: Remedial Action	i. System of Records

Section D - Senior Agency Official for Privacy (SAOP): Questions 7, 8, and 9

Agency Name:

	7. Policy Compliance Review	
7.a.	Does the agency have current documentation demonstrating review of compliance with information privacy laws, regulations, and policies? Yes or No.	
7.b.	Can the agency provide documentation of planned, in progress, or completed corrective actions necessary to remedy deficiencies identified in compliance reviews? Yes or No.	
7.c.	Does the agency use technologies that enable continuous auditing of compliance with stated privacy policies and practices? Yes or No.	
7.d.	Does the agency coordinate with the agency's Inspector General on privacy program oversight? Yes or No.	

8. Agency Use of Persistent Tracking Technology

OMB policy stated in M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002", prohibits agencies from using persistent tracking technology on web sites, except in compelling circumstances as determined by the head of the agency (or designee reporting directly to the agency head).

Indicate Yes or No for each item in the table below.

Persistent Tracking		
a.	Does the agency use persistent tracking technology on any web site?	
b.	Does the agency annually review the use of persistent tracking?	
c.	Can the agency demonstate through documentation the continued justification for, and approval to use, the persistent tracking technology?	
d.	Can the agency provide the notice language or citation for the web privacy policy that informs visitors about the persistent tracking?	

9. Privacy Points of Contact Information

Please provide the names, phone numbers, and e-mail addresses of the following officials:

Title/Role	Name	Phone	E-mail
Agency Head			
Chief Information Officer			
Agency Inspector General			
Chief Information Security Officer			
Senior Agency Official for Privacy			
Chief Privacy Officer			
Privacy Advocate			
Privacy Act Officer			
Reviewing Official for PIAs			
POC for URL links provided in question #2			