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

August 20, 2009

M-09-29

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Jeffrey D. Zients
Deputy Director for Management

Vivek Kundra
U.S. Chief Information Officer

SUBJECT: FY 2009 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

This memorandum provides instructions for meeting your agency's FY 2009 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.

The reporting categories and questions are generally the same as last year, and the report will cover the same areas as in previous years. However, while the content of the report has changed little since 2008, the means of collection have changed substantially. This year, rather than using spreadsheets, the annual FISMA report data collection will occur via an automated reporting tool. This tool will allow both manual data entry and automatic upload of data. Therefore, the attachments to this memo only contain lists of questions and not reporting templates.

The Chief Information Officers (CIO), Inspectors General (IG), and the Senior Agency Officials for Privacy (SAOP) will all report through the automated collection tool. A test version will be available in August and further instructions will be issued. Please note that OMB will only accept reports submitted through the automated tool. Reporting to the Congress will continue as in prior years. **Due to the new collection system, the due date for FISMA reports will be November 18, 2009**.

Agencies should also submit the following information related to OMB Memorandum M-07-16, of May 22, 2007, "Safeguarding Against and Responding to the Breach of Personally Identifiable Information."[1] This information should be provided as separate documents submitted through the automated reporting tool and should include the following items for your agency:

- Breach notification policy if it has changed significantly since last year's report;

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

- Progress update on eliminating unnecessary use of Social Security Numbers (SSN); and
- Progress update on review and reduction of holdings of personally identifiable information (PII).

Agency reports must reflect the agency head's determination of the adequacy and effectiveness of information security and privacy policies, procedures, and practices. The new automated reporting tool will allow agencies to submit an electronic copy of the signed official transmittal letter.

Agency staff may contact Suzanne Lightman, slightman@omb.eop.gov, regarding security questions or Sharon Mar, smar@omb.eop.gov, regarding privacy questions.

Attachments:

- List of FISMA FAQs
- CIO Questions
- IG Questions
- SAOP Questions
- Microagency Questions

FY 2009 Reporting Instructions for the
Federal Information Security Management Act and
Agency Privacy Management

Table of Contents

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 a report from the automated reporting tool 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 set of questions should my agency fill out in the automated reporting tool?

All agencies, except for microagencies, should complete the Chief Information (CIO), Inspector General (IG) and Senior Agency Official for Privacy (SAOP) questions in the automated reporting tool for submission to OMB no later than November 18, 2009.

Microagencies (i.e., agencies employing 100 or fewer FTEs) should answer the abbreviated questions (see Microagencies Questions attached) for their annual report.

Please note that only submissions through the automated reporting tool will be accepted by OMB.

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. 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.

5. Is the use of the automated reporting tool mandatory?

Yes, OMB will only accept submissions through the automated reporting tool. Full instructions for the use of the tool will be available in August, 2009 along with a test version.

Security Reporting

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. Currently, NIST, DoD and the DNI are working on harmonizing system categorization and security control selection requirements. Once guidance is harmonized, less explanation of differences will be required.

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 guidelines. For legacy information systems, agencies are expected to be in compliance with NIST standards and guidelines within one year of the publication date unless otherwise directed by OMB. The one year compliance date for revisions to NIST publications applies only to the new and/or updated material in the publications. For information systems under development or for legacy systems undergoing significant changes, agencies are expected to be in compliance with the NIST publications immediately upon deployment of the information system.

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 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?

OMB gives equal weight to both assessments. In asking different questions of each party, OMB seeks complementary and not conflicting reporting. While 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.

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 Authorizing Official 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.

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 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 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?

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.

In FY 2007, OMB 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. The acquisition language in OMB M-07-18 was published in the Federal Register, FAR 2007-004. For all contracts, the following language should be included, to encompass Federal Desktop Core Configurations:

> "(d) In acquiring information technology, agencies shall include the appropriate information technology security policies and requirements, including use of common security configurations available from the National Institute of Standards and Technology's website at http://checklists.nist.gov. Agency contracting officers should consult with the requiring official to ensure the appropriate standards are incorporated."

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.

44. What resources are available to assist agencies in providing annual information security and privacy training to their employees?

The Information System Security Line of Business (ISSLOB) has been working with agencies to develop a standardized curriculum, and, to select information security Shared Service Centers (SSC). The ISSLOB SSC's provide an efficient and cost-effective solution for agencies to procure general information security training for employees and contractors. For more information on this program, contact the ISSLOB program management office at the Department of Homeland Security.

Privacy Reporting

45. 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.

46. 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 as shown in the SAOP Questions will satisfy agencies' privacy reporting obligations under the E-Government Act. OMB will not include privacy reporting in the E-Government Act reporting template.

47. 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.

48. 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.

49. 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.

50. 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 (OMB Memorandum M-03-22, Section II.B.3.a.).

51. 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?

No, 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.

Electronic Authentication

52. What is Electronic Authentication (e-authentication)?

In December 2003, OMB issued Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," which requires agencies to review new and existing electronic transactions to ensure the authentication processes provide the appropriate level of assurance. It establishes and describes four levels of identity assurance for electronic transactions requiring authentication. Specifically, agencies are to determine assurance levels using the following steps:

1. Conduct an e-authentication risk assessment of the e-government system.
2. Map identified risks to the appropriate assurance level.
3. Select technology based on e-authentication technical guidance.
4. Validate that the implemented system has achieved the required assurance level.
5. Periodically reassess the system to determine technology refresh requirements.

An e-authentication application is an application that meets the following criteria:

1. Is web-based;
2. Requires authentication; and
3. Extends beyond the borders of your enterprise (e.g. multi-agency, government-wide, or public facing)

For additional e-authentication requirements, please refer to NIST Special Publication 800-63, "Electronic Authentication Guidance" at http://csrc.nist.gov/publications.

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 M-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.