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

July 17, 2006

M-06-20

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Clay Johnson III
Deputy Director for Management

SUBJECT: FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

This memorandum provides instructions for meeting your agency's FY 2006 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 your report to evaluate agency-specific and government-wide security performance, it is especially important your agency's report clearly and accurately reflects the overall status of your program and not include conflicting views of, or unresolved differences among, the various parties contributing to the report such as your Chief Information Officer and Inspector General.

Although the reporting categories and questions are unchanged from last year, there are several additional actions you must take, additional information you must provide, and slightly altered timeframes for doing so.

- First, you should provide with your report, as an appendix or separate attachment, the results of the review your agency's senior official for privacy conducted pursuant to my memorandum (M-06-15) of May 22, 2006, "Safeguarding Personally Identifiable Information."[1]

- Second, this memorandum requests that Inspectors General provide a list of any systems they have found missing from the agency's inventory of major information systems. As you know, your agency is required, under the E-Government Act of 2002, to provide an inventory of major information systems (*see*, Pub. L. No. 107-347, §305(c)(2), codified at 44 U.S.C. § 3505(c)).

- Third, this memorandum requires agency privacy updates be submitted quarterly with your security updates to support the President's Management Agenda scorecard. These updates are now due on the first day of September, December, March, and June.

- Finally, in accordance with OMB memorandum (M-06-19) of July 12, 2006, "Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology

[1] http://www.whitehouse.gov/omb/memoranda/fy2006/m-06-15.pdf

Investments,"[2] we want you to identify any physical or electronic incidents involving the loss of or unauthorized access to personally identifiable information and report them according to the policies that are outlined in M-06-19.

Please send one formal copy of your report to me and an electronic copy to fisma@omb.eop.gov by October 1, 2006. Each report must include a transmittal letter from the agency head reconciling any differences between the findings of the agency CIO and IG. The report must reflect the agency head's determination of the adequacy and effectiveness of information security policies, procedures, and practices. More details on reporting are found in the attachments to this memorandum. Your staff may contact Kim Johnson, Kim_A._Johnson@omb.eop.gov, or Kristy Lalonde, klalonde@omb.eop.gov, regarding security questions or Hillary Jaffe, HJaffe@omb.eop.gov, regarding privacy questions.

Attachments

- Instructions for Preparing the FISMA Report and Privacy Management Report
- Reporting Template for Micro Agencies (Excel)
- Reporting Template for Agency CIOs (Excel)
- Reporting Template for Agency IGs (Excel)
- Reporting Template for Senior Agency Officials for Privacy (Excel)
- Quarterly Reporting Template (Excel)

[2] http://www.whitehouse.gov/omb/memoranda/fy2006/m-06-19.pdf

Instructions for Preparing the Annual Federal Information Security Management Act Report and Privacy Management Report

Table of Contents

If an agency has developed additional performance measures beyond those provided by OMB, they may report them as well. However, incomplete reporting on OMB's performance measures will be noted in OMB's public report to Congress and will be a consideration in OMB's annual approval or disapproval of the agency's security program. When completing the reporting template, agencies may find it useful to refer to the definitions section provided.

Frequently Asked Questions

Security Reporting – Questions 1 through 36.
Privacy Reporting– Questions 37 through 47.

Security Reporting

1. *What systems should be reported under FISMA?*
   FISMA applies to information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. All general support systems and applications, whether major or non-major, meeting this definition shall be included in the report. NIST Special Publication 800-37 provides information on establishing information system boundaries which can help you identify your systems.

2. *When are quarterly updates due?*
   Unlike past years, quarterly updates are due to OMB on September 1, December 1, March 1, and June 1. The dates have been adjusted to accommodate the timing of your quarterly President's Management Agenda scorecards.

3. *Is use of National Institute of Standards and Technology (NIST) publications required?*
   Yes. For non-national security programs and systems, agencies must follow NIST standards and guidance.

4. *Must the Department of Defense and the Central Intelligence Agency follow OMB policy and NIST guidance?*
   Provided DOD and CIA internal security standards and policies are as stringent as OMB's policies and NIST's standards, they must only follow OMB's reporting policies.

5. *Must agencies report at both an agency wide level and by individual component?*
   Yes. Agencies must provide an overall agency view of their security 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 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.

6. *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. The description shall include the extent to which the management and internal oversight of an agency's national security programs and systems are being handled differently than the program for non-national security programs and systems and why. DoD and the Director of National Intelligence shall report on compliance with their policies and guidance.

The intelligence community CIO reports on systems processing or storing sensitive compartmentalized information (SCI) across the intelligence community and those other systems for which the Director of National Intelligence 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.

7. *When should program officials, CIOs, and IGs share the results of their reviews?*
Inasmuch as the goal of FISMA is stronger agency and government-wide security, information regarding an agency's security program should be shared as it becomes available. This helps promote timely correction of weaknesses and resolution of issues. Waiting until the completion of a report or the year's end does not promote stronger security.

8. *Should agencies set an internal FISMA reporting cut-off date?*
Yes, OMB suggests agencies set an internal cut-off date by which FISMA data collection and report preparation by the CIO and the IG are completed. A cut-off date should permit enough time for meaningful cross-review and comment by all parties as well as resolution of any disputes before finalizing the agency's report to OMB. However, with respect to an IG review of the CIO'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.

9. *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.

10. *Certifying and accrediting systems doesn't guarantee a secure system. Why place such an emphasis on C&A?*
    While no process will guarantee a secure system, when performed properly C&A provides a systematic approach for determining whether appropriate security controls are in place, functioning properly, and producing the desired outcome. It also provides authorizing officials with the information they need to make informed decisions based on knowledge of the remaining risks.

    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.

11. *Is certification and accreditation required for all systems? OMB Circular A-130 requires authorization to process only for general support systems and major applications.*
    Yes, certification and accreditation is required for all 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. However, as recognized in NIST guidance, the complexity of the process for an individual system or application depends on a number of factors including the system complexity, size, and risk impact level. (See also the discussion of annual system testing and evaluation.)

12. *Why does OMB not recognize interim authority to operate for certification and accreditation?*
    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.

13. *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?

Ultimately, the agency head is responsible for deciding the acceptable level of risk for their agency. Primary input for this decision comes from system owners, program officials, and most certainly CIOs. Such decisions must of course reflect policies and guidance from OMB and NIST (most particularly FIPS 199 and FIPS 200). A system's designated approving authority takes responsibility for accepting any residual risk, thus they are to be held accountable for managing the security for that system.

IG evaluations must also be risk-based. When reviewing the C&A of an individual system, for example, the IG would generally assess whether: 1) the certification 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 risk 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.

14. *Must all agency systems be tested and evaluated (reviewed) 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.

It is especially important to note, FIPS 200 (Special Publication 800-53) requires agencies to monitor selected security controls for all systems on a continuous basis. NIST Special Publication 800-37 provides guidance on the continuous monitoring process.

15. *What level of review is required for an individual system?*

Program officials and CIOs are responsible for reviewing the security of all systems under their respective control. Clearly, the necessary depth and breadth of an annual system review depends on several factors such as: 1) the potential risk and magnitude of harm to the system or data; 2) the relative comprehensiveness of the most recent past review; and 3) the adequacy and successful implementation of the POA&M for weaknesses in the system. For example, if last year a system underwent a complete certification and accreditation (consistent with NIST or national security guidance), this year a relatively simple update or maintenance review may be sufficient, provided it has been adequately documented. An effective security program demands comprehensive and continuous understanding of program and system weaknesses. At a minimum, agency program officials and CIOs must take into account the three criteria listed above in determining the

appropriate level of annual review. IGs may report on the adequacy of such reviews.

16. *What NIST guidance must agencies use for their annual testing and evaluations?*
For FY 2006, agencies may again use either NIST Special Publication 800-26 or FIPS 200/NIST Special Publication 800-53 for the specification and assessment of security controls for federal information systems. **Agencies should note however, for FY07 and beyond, agencies will be required to use FIPS 200/NIST Special Publication 800-53 for the specification of security controls and NIST Special Publication 800-53A for the assessment of security control effectiveness.** DOD and CIA may use their internal policies, directives and guidance provided that they are as stringent as the NIST security standards.

17. *If an agency chooses to use 800-53 for its annual testing and evaluation, must each of the security controls be tested?*
No. The agency must test a subset of controls based on:

- The security categorization of the information system
- The specific security controls selected and employed by the organization to protect the information system; and
- The level of assurance (or confidence) that the organization must have in determining the effectiveness of the security controls in the information system.

18. *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. Systems with secure configurations have fewer vulnerabilities and are better able to thwart network attacks.

A number of commercial and government-owned products are available for configuring and testing software for adherence to security configuration requirements. Agencies are to cite in their report the frequency by which they implement system configuration requirements.

Security configuration checklists are now available for computer software widely used within the Federal Government. The checklists may be found on the NIST Computer Security Division website as well as the NSA System and Network Attack Center website. OMB expects agencies to use the published configurations or be prepared to justify why they are not doing so. Inspectors General should review such use.

19. *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 DOD and CIA are not required to follow NIST guidance nor does it apply to national security systems, OMB expects all agencies to implement a reasonably similar process.

20. *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 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, 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 risk impact level in this circumstance must be agreed to by the provider and all of their customers.

21. *My inspector general 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.

22. *When OMB asks if an agency has a process, are you also asking if the process is effective*?
Yes. OMB wants to know whether processes are working as intended to safeguard information and information systems. An ineffective process cannot be relied upon to achieve its IT security objectives. To gauge the effectiveness of a particular IT security program process, we rely on responses to questions asked of the agency IG.

23. *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 in one location an agency's security weaknesses. 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.

24. *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.

OMB's policies regarding funding security were articulated in OMB Memorandum M-00-07 dated February 28, 2000. They remain in effect 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 (C&A) 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 testing from the funds intended for development, modernization or enhancement.

OMB recognizes however, unlike the examples above which are clearly understood and basic requirements for all systems and costs are predictable, other unanticipated security needs may arise from time-to-time. In such cases, agencies should ensure risks are managed at an appropriate level and prioritize available resources to correct the most significant weaknesses. Correcting such weaknesses would still be required prior to spending funds on development. In any case, compensating controls as described in FIPS 200 (NIST Special Publication 800-53) must be used until an agency has implemented final corrections.

25. *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, or 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.

26. *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 by another source.

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 IT security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems – on behalf of a Federal agency. Such other organizations may include contractors, grantees, State and local governments, industry partners, 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 (in addition to 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.

27. *Could you provide examples of "incidental" contractor equipment which is not subject to FISMA?*
Again, 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.

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.

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

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 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).

   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 certification and accreditation 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.

   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 offsite 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.

29. *How do agencies ensure FISMA compliance for connections to non-agency systems? Do 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 effective internal controls at service organizations. 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.

30. *Should agencies modify contracts and grants to include FISMA requirements?*
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. Agencies have had several years to make these contract modifications and OMB expects them to have done so.

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 the Department of Commerce's National Institute of Standards and Technology.

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

31. *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 discussion concerning interconnection agreements and below regarding C&A and accreditation boundaries.

32. *Are all IT systems operated by a contractor on behalf of an agency subject to the same type of certification and accreditation process?*

Yes, they must be addressed in the same way. As with agency operated systems, the level of effort required for certification and accreditation depends on the impact level of the information contained on each system. Certification and accreditation 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 certification and accreditation 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.

33. *Who is responsible for the POA&M process for contractor systems that are 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.

34. *If an agency has employees with job categories that do not require system access, how are these employees counted in overall training totals?*

Agencies should report all security and awareness training for all employees, including those without system access. If the agency can distinguish between employees who access a system as part of their job and those who do not, the agency may make this distinction in the annual report to OMB. Agencies must report IT security awareness and training numbers for all computer users.

35. *OMB asks agencies whether they have provided IT 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*

Section A - Instructions for Completing the Annual Federal Information Security Management Act (FISMA) Report and Privacy Management Report

This section contains instructions for annual FISMA and privacy reporting. The reporting templates are contained in Sections B, C, and D. Each of the templates are to be completed by the appropriate agency officials, as part of one combined report signed by the agency head and transmitted to the Director, Office of Management and Budget (OMB) each year by October 1. In addition to formal transmission, an electronic copy of the report should be sent to fisma@omb.eop.gov .

Each agency head's annual report to OMB shall comprise:

1. Transmittal letter from the agency head reconciling any differences between the findings of the agency CIO and IG. The report must reflect the agency head's determination of the adequacy and effectiveness of information security policies, procedures, and practices.

2. Section B Template completed by the CIO - Results of annual IT security reviews of systems and programs.

3. Section C Template completed by the IG - Results of the IG independent evaluation.

4. Section D Template completed by the Senior Agency Official for Privacy - Status of agency compliance with OMB privacy policies.

When to send reports 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 and C 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 Government Reform and Science 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.

Agency responses shall be based on the results of the annual system and program reviews, the agency's work in correcting weaknesses identified in their POA&Ms, and any other work performed throughout the reporting period. Extensive narrative responses are strongly discouraged, but agencies may provide brief comments in the space provided. IGs are however encouraged to provide any additional narrative in an appendix to the report to the extent they provide meaningful insight into the status of the agency's security or privacy program.

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 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 e. of Question 6.

36. *Why is OMB continuing to ask about Peer to Peer file sharing in IT security training?*
IT security awareness training should evolve as emerging technologies enter into the workplace. A type of file sharing (known as Peer to Peer or P2P) generally refers to any software or system allowing individual users of the Internet to connect to each other and trade computer files. These systems are usually highly decentralized and are designed to facilitate connections between persons who are looking for certain types of files. While there are many appropriate uses of this technology, a number of studies show the vast majority of files traded on P2P networks are copyrighted music files and pornography. Data also suggests P2P is a common avenue for the spread of computer viruses within IT systems.

Federal computer systems, as well as those operated by contractors on the government's behalf, must not be used for the downloading of illegal and/or unauthorized copyrighted content, including illegal downloads using file sharing programs. Further information is detailed in the Chief Information Officers Council's recommended guidance on "Limited Personal Use of Government Office Equipment Including Information Technology[1]". Agency policies and training programs shall be consistent with the CIO Council guidance.

Privacy Reporting

37. *Which agency official should complete the privacy questions in this FISMA report?*
These questions shall be completed or supervised by the Senior Agency Official for Privacy. 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 Senior Agency Official for Privacy shall consult with these officials when responding to these questions, and note (Section IV) those who contributed and/or reviewed the responses to the questions.

38. *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.

[1] http://www.cio.gov/documents/peruse_model_may_1999.pdf (May 19, 1999)

39. *Should the IGs answer the privacy questions?*
OMB encourages IGs to provide any meaningful data they have regarding the agency's privacy program and related activities. IGs may submit this information to OMB along with the agency's response to Section D, or they may separately submit additional comments as an appendix to the report. However, this information shall not be included in the IG's report to Congress or GAO.

40. *What is the source of the requirements reflected in Items #3, #4, and #5 of Subsection III ("Internal Oversight")?*
Section 522 of the Consolidated Appropriations Act of 2005 requires agencies governed by Title V of that Act to designate Chief Privacy Officers to assume primary responsibility for privacy and data protection policy. For the most part, the duties of these Chief Privacy Officers mirror the duties of the Agency Senior Officials for Privacy, enumerated in OMB in Memorandum 05-08 (February 2005). However, items #3, #4 and #5 of Subsection III reflect additional responsibilities Section 522 imposes on the Chief Privacy Officers of covered agencies. While agencies governed by Section 522 are most likely to answer these questions with "yes," no provision of law or policy precludes other agencies from adopting the procedures or practices reflected in these questions.

41. *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, additional training or development of internal guidance or policy might be appropriate. Agencies should report incidents also reported elsewhere for security purposes. This reporting includes breaches that are either intentional or negligent, regardless of whether the source of the breach is internal or external or was a physical or electronic incident.

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.

42. *Will OMB send agencies' privacy reporting (Section D) to Congress as part of the FISMA report?*
We have not decided how we will report this information to Congress for FY2006. For agency IG reporting to Congress and GAO, they should not include the privacy section. However, agencies subject to the annual privacy reporting requirement mandated by Section 522 of the Consolidated Appropriations Act of 2005 may wish to use the framework provided by Section D as a guide in developing that agency's required reports to Congress.

43. *Can OMB provide clarification as to what "verification of intent to comply" in Section D.III, Question 4 means?*

Subsection c ("Recording") of Section 522 of the Consolidated Appropriations Act of 2005 requires agencies governed by the provision to provide their Inspector General a report detailing how the agency uses and protects information in identifiable form. The provision requires the report be signed by the agency privacy officer "to verify that the agency intends to comply with procedures in the report... [and verifying that]... that the agency is only using information in identifiable form as detailed in the report." By signing the report transmitted to the IG, the Chief Privacy Officer affirms his/her best understanding and belief that the agency's actual information handling practices fully comport with the practices and policies reflected in its formal, written documentation.

44. *Can OMB provide clarification and examples as to the required content of an agency's "summary of the use of information in identifiable form?"*

Again, Subsection c ("Recording") of Section 522 of the Consolidated Appropriations Act of 2005 requires agencies governed by the provision to "prepare a written report of its use of information in identifiable form, along with its privacy and data protection policies and procedures and record it with the Inspector General of the agency to serve as a benchmark for the agency." Agencies reflect their use of information in identifiable form in Privacy Act Systems of Records Notices and Privacy Impact Assessments. Agencies may wish to develop their reports regarding the use of information in identifiable form using excerpts from these pertinent sources.

45. *Must all agencies submit an annual report to OMB detailing privacy activities? If yes, what is the source of the requirement?*

Yes, agencies must submit an annual report detailing privacy activities. This report is required by the E-Government Act of 2002.

46. *Why was the fiscal year time limitation removed from question II.D.5 relating to reporting privacy procedures and practices?*

OMB removed the fiscal year time limitation to clarify the reporting requirements in parts "a," "b," and "c" of question II.D.5.

- II.D.5.a. seeks the total number of systems that contain Federally-owned information in identifiable form.
- II.D.5.b. part 1 seeks the total number of systems which contain Federally-owned information in an identifiable form that require a PIA. (Note: the number provided for b part 1 should be equal to or smaller than the number provided for "a.")
- II.D.5.b. part 2 seeks the following information - OF the systems included in II.D.5.b. part 1, what is the TOTAL number of systems for which a PIA exists AND that PIA is current*? A PIA must be drafted each time an applicable new system is created and revised each time an applicable existing system is

substantially altered. (Note: the number provided for part 2 should be equal to or smaller than the number provided in part 1.)

- II.D.5.c. part 1 seeks the TOTAL number of systems for which Federally-owned information is retrieved by name or unique identifier.
- II.D.5.c. part 2 seeks the following information - OF the systems included in part 1, what is the TOTAL number of systems for which a SORN has been published in the federal register AND that SORN is current*? (Note: The number provided for part 2 should be equal to, but may be greater than, the number provided in part 1.)
- A PIA or SORN is "current" if that document satisfies the applicable requirements and subsequent substantive changes have not been made to the system.

47. *Do agencies have to conduct a Privacy Impact Assessment for information technology systems that contain or administer information in identifiable form strictly about agency employees or agency 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 (Memorandum 03-22) 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.

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, (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 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.

Information System (defined in OMB Circular A-130)
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.

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 Agency CIOs

A reporting template tool will be sent at a later date, and will be posted at http://www.omb.gov . Below are the questions to be included in the template, in a narrative format.

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. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of information systems used or operated by your agency, and the number of information systems used or operated by a contractor of your agency or other organization on behalf of your agency.

   Note: 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.

   To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
   1) Continue to use NIST Special Publication 800-26, or,
   2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

   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 risk impact level was determined through another method, please explain below in item (d.).**

   a. Agency Systems

- By bureau: total number, number evaluated
- By FIPS 199 impact level (high, moderate, low, not categorized): total number, number evaluated

b. Contractor Systems
- By bureau: total number, number evaluated
- By FIPS 199 impact level (high, moderate, low, not categorized): total number, number evaluated

c. Total Number of Systems
- By bureau: total number of agency systems and contractor systems, number evaluated
- By FIPS 199 impact level (high, moderate, low, not categorized): total number, number evaluated

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

2. For each part of this question, identify actual performance this reporting period by risk impact level and bureau, in the format provided below. From the Total Number of Systems, identify the number of systems which have: a current certification and accreditation[2], a contingency plan tested within the past year, and security controls tested within the past year. 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.

a. Number of systems certified and accredited
- By bureau
- By FIPS 199 impact level (high, moderate, low, not categorized).

b. Number of systems for which security controls have been tested and evaluated in the last year
- By bureau
- By FIPS 199 impact level (high, moderate, low, not categorized).

c. Number of systems for which contingency plans have been tested in accordance with policy and guidance
- By bureau
- By FIPS 199 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:

[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. Agencies must implement the recommended security controls in NIST Special Publication 800-53.

a. Do you have a plan in place to fully implement the security controls recommended in NIST Special Publication 800-53? Yes or No.
b. Have you fully implemented the security controls recommended in NIST Special Publication 800-53? Yes or No.

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. Information gathered in this question will be forwarded to the Department of Homeland Security for validation.

For each category of incident listed: identify the total number of successful incidents this reporting period, the number of incidents reported to US-CERT, and the number reported to law enforcement. If your agency considers another category of incident type to be high priority, include this information in category e., "Other". If appropriate or necessary, include comments in the area provided below.

a. Unauthorized Access
- Number reported internally
- Number reported to US-CERT
- Number reported to law enforcement

b. Denial of Service (DoS)
- Number reported internally
- Number reported to US-CERT
- Number reported to law enforcement

c. Malicious Code
- Number reported internally
- Number reported to US-CERT
- Number reported to law enforcement

d. Improper Usage
- Number reported internally
- Number reported to US-CERT
- Number reported to law enforcement

e. Other
- Number reported internally
- Number reported to US-CERT
- Number reported to law enforcement

Comments: Space provided for narrative comments.

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

a. Total number of employees

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

c. Total number of employees with significant IT security responsibilities

d. 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).

e. Total costs for providing IT security training in the past fiscal year

f. Briefly describe the training provided in b. and d.

Comments: Space provided for narrative comments.

7. 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.
Comments: Space for narrative comments.

b. Configuration guides are available for the products listed below. With a checkmark, identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.

 Windows XP Professional
Are any agency systems running this software? Yes or No.
To what extent has this configuration been implemented?
- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software

- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

 Windows NT

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

 Windows 2000 Professional

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

 Windows 2000 Server

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

 Windows 2003 Server

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software

- Almost Always, or on approximately 96-100% of the systems running this software

□ Solaris

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ HP-UX

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Linux

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Cisco Router IOS

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Oracle

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□Other. Specify:

9. Indicate whether or not the following policies and procedures are in place at your agency. 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 documented policies and procedures for external reporting to law enforcement authorities. Yes or No.

c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.

Comments: Space provided for narrative comments.

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 & evaluations, specific configuration requirements, additional monitoring, or specialized training.

Section C – Reporting Template for Agency IGs

A reporting template tool will be sent at a later date, and will be posted at http://www.omb.gov . Below are the questions to be included in the template, in a narrative format.

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. IGs may also submit additional narrative in an appendix to the report.

1. As required in FISMA, the IG shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. By FIPS 199 risk impact level (high, moderate, low, or not categorized) and by bureau, identify the number of systems reviewed in this evaluation for each classification below (a., b., and c.).

   To meet the requirement for conducting a NIST Special Publication 800-26 review, agencies can:
   1) Continue to use NIST Special Publication 800-26, or,
   2) Conduct a self-assessment against the controls found in NIST Special Publication 800-53

   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 bureau
   - By FIPS 199 impact level (high, moderate, low, not categorized).

   b. Contractor Systems
   - By bureau
   - By FIPS 199 impact level (high, moderate, low, not categorized).

   c. Total Number of Systems
   - By bureau
   - By FIPS 199 impact level (high, moderate, low, not categorized).

2. For each part of this question, identify actual performance over the past fiscal year by risk impact level and bureau, in the format provided below. From the representative subset of systems evaluated, identify the number of systems which have completed the

following: have a current certification and accreditation[3], a contingency plan tested within the past year, and security controls tested within the past year.

a. Number of systems certified and accredited
- By bureau
- By FIPS 199 impact level (high, moderate, low, not categorized).

b. Number of systems for which security controls have been tested and evaluated in the last year
- By bureau
- By FIPS 199 impact level (high, moderate, low, not categorized).

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

3. In the format below, evaluate the agency's oversight of contractor systems, and agency system inventory.

a. 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. Self-reporting of NIST Special Publication 800-26 and/or 800-53 requirements by a contractor or other organization is not sufficient, however, self-reporting by another Federal agency may be sufficient.

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

b. 1. The agency has developed an 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:
- Approximately 0-50% complete

[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.

- Approximately 51-70% complete
- Approximately 71-80% complete
- Approximately 81-95% complete
- Approximately 96-100% complete

b.2. If the Agency IG does not evaluate the Agency's inventory as 96-100% complete, please list the systems that are missing from the inventory.
Missing agency systems
Missing contractor systems

c. The OIG **generally** agrees with the CIO on the number of agency owned systems. Yes or No.
d. The OIG **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. The agency has completed system e-authentication risk assessments. Yes or No.

4. Through this question, and in the format provided below, 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 the following statements reflect the status in your agency by choosing from the responses provided in the drop down menu. If appropriate or necessary, include comments in the area provided below.

a. The POA&M is an agency wide process, incorporating all known IT 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.

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

b. When an IT 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).

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

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

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

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

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

e. OIG findings are incorporated into the POA&M process.

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

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

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

Comments: Space provided for narrative comments.

5. OIG Assessment of the Certification and Accreditation Process

OMB is requesting IGs to provide a qualitative assessment of the agency's certification and accreditation process, including adherence to existing policy, guidance, and standards. 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 (February, 2004), "Standards for Security Categorization of Federal Information and Information Systems," to determine an impact level, as well as associated NIST documents used as guidance for completing risk assessments and security plans[4].

Assess the overall quality of the Department's certification and accreditation process.

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

Comments: Space for narrative comments.

6. Configuration Management.

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

b. Configuration guides are available for the products listed below. With a checkmark, identify which software is addressed in the agency wide security configuration policy. Indicate whether or not any agency systems run the software. In addition, approximate the extent of implementation of the security configuration policy on the systems running the software.

□ Windows XP Professional
Are any agency systems running this software? Yes or No.
To what extent has this configuration been implemented?
- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Windows NT
Are any agency systems running this software? Yes or No.
To what extent has this configuration been implemented?
- Rarely, or, on approximately 0-50% of the systems running this software

[4] 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.

- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Windows 2000 Professional

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Windows 2000 Server

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Windows 2003 Server

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

□ Solaris

Are any agency systems running this software? Yes or No.

To what extent has this configuration been implemented?

- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software

- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

 HP-UX
Are any agency systems running this software? Yes or No.
To what extent has this configuration been implemented?
- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

 Linux
Are any agency systems running this software? Yes or No.
To what extent has this configuration been implemented?
- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

 Cisco Router IOS
Are any agency systems running this software? Yes or No.
To what extent has this configuration been implemented?
- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

 Oracle
Are any agency systems running this software? Yes or No.
To what extent has this configuration been implemented?
- Rarely, or, on approximately 0-50% of the systems running this software
- Sometimes, or on approximately 51-70% of the systems running this software
- Frequently, or on approximately 71-80% of the systems running this software
- Mostly, or on approximately 81-95% of the systems running this software
- Almost Always, or on approximately 96-100% of the systems running this software

 Other. Specify:

7. Indicate whether or not the following policies and procedures are in place at your agency. 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 documented policies and procedures for external reporting to law enforcement authorities. Yes or No.
   c. The agency follows defined procedures for reporting to the United States Computer Emergency Readiness Team (US-CERT). http://www.us-cert.gov Yes or No.

   Comments: Space provided for narrative comments.

8. Has the agency ensured security training and awareness of all employees, including contractors and those employees with significant IT security responsibilities?
   - Rarely, or, approximately 0-50% of employees have sufficient training
   - Sometimes, or approximately 51-70% of employees have sufficient training
   - Frequently, or approximately 71-80% of employees have sufficient training
   - Mostly, or approximately 81-95% of employees have sufficient training
   - Almost Always, or approximately 96-100% of employees have sufficient training

9. 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.

Section D - Reporting Template for Senior Agency Officials for Privacy

A reporting template tool will be sent at a later date. Below are the questions to be included in the template, in a narrative format. This shall be completed by all agencies.

I. Senior Agency Official for Privacy Responsibilities

1. 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.

2. 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. 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.

II. Procedures and Practices

1. Does your agency have a training program to ensure that all agency personnel and contractors 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.

2. Does your agency have a program for job-specific information privacy training (i.e., detailed training for individuals (including contractor employees) directly involved in the administration of personal information or information technology systems, or with significant information security responsibilities)?
Yes or No.

3. Section 3, Appendix 1 of OMB Circular A-130 requires agencies conduct -- and be prepared to report to the Director, OMB on the results of -- reviews of activities mandated by the Privacy Act.
Please indicate by component (e.g., bureau, agency) which of the following reviews were conducted in the last fiscal year.
[make chart with the following headings]

Section M Contracts	Records Practices	Routine Uses	Exemptions	Matching Programs	Training	Violations: Civil Action	Violations: Remedial Action	Systems of Records

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

a. Does you agency have a written process or policy for:

(i) determining whether a PIA is needed?	Yes/No
(ii) conducting a PIA?	Yes/No
(iii.) evaluating changes in business process or technology that the PIA indicates may be required?	Yes/No
(iv.) ensuring that systems owners and privacy and IT experts participate in conducting the PIA?	Yes/No
(v.) making PIAs available to the public in the required circumstances?	Yes/No
(vi.) making PIAs available in other than required circumstances?	Yes/No

b. Does your agency have a written process for determining continued compliance with stated web privacy policies?
Yes or No.

c. Do your public-facing agency web sites have machine-readable privacy policies (i.e., are your web privacy policies P3P-enabled or automatically readable using some other tool)?
Yes or No.

(i.) if not, provide date for compliance:

5. By bureau, identify the number of information systems containing Federally-owned information in an identifiable form. For the applicable systems, on how many have you conducted a Privacy Impact Assessment and published a Systems of Records Notice?

a. Total number of systems that contain Federally-owned information
- By bureau: number that contain Federally-owned information in identifiable form
  - Agency Systems
  - Contractor Systems
  - Total number of systems

b. Privacy Impact Assessments
- By bureau: total number requiring a Privacy Impact Assessment (systems that contain information from or about the public)
  - Agency Systems
  - Contractor Systems
  - Total number of systems

- By bureau: number of applicable systems that have a current Privacy Impact Assessment.
  - Agency Systems
  - Contractor Systems
  - Total number of systems

c. Systems of Records Notices
- By bureau: number of systems from which Federally-owned information is retrieved by name or unique identifier
  - Agency Systems
  - Contractor Systems
  - Total number of systems

- By bureau: number of systems for which a current Systems of Records Notice has been published in the Federal register
  - Agency Systems
  - Contractor Systems
  - Total number of systems

d. Contact Information for preparer of question 5.

6. OMB policy (Memorandum 03-22) 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).

a. Does your agency use persistent tracking technology on any web site?
Yes/No
b. Does your agency annually review the use of persistent tracking?
Yes/No
c. Can your agency demonstrate through documentation the continued justification for and approval to use the persistent technology?
Yes/No
d. Can your agency provide the notice language used or cite to the web privacy policy informing visitors about the tracking?
Yes or No.

III. Internal Oversight

1. Does your agency have current documentation demonstrating review of compliance with information privacy laws, regulations and policies?
Yes or No.
(i.) If so, provide the date the documentation was created.

2. Can your agency provide documentation demonstrating corrective action planned, in progress or completed to remedy identified compliance deficiencies?
Yes or No.
(i.) If so, provide the date the documentation was created.

3. Does your agency use technologies that allow for continuous auditing of compliance with stated privacy policies and practices?
Yes or No.

4. Does your agency coordinate with the agency Office of Inspector General on privacy program oversight by providing to OIG the following materials:

a. compilation of the agency's privacy and data protection policies and procedures? Yes/No
b. summary of the agency's use of information in identifiable form? Yes/No
c. verification of intent to comply with agency policies and procedures? Yes/No

5. Is your agency required to submit an annual report to Congress (OMB) pursuant to § 522 of the Appropriations Act detailing your privacy activities, including activities under the Privacy Act and any violations that have occurred?
Yes or No.
(i.)If so, when was this report submitted to OMB for clearance?

IV. 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: