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

THE DIRECTOR

M-04-25

August 23, 2004

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten
Director

SUBJECT: FY 2004 Reporting Instructions for the Federal Information Security Management Act

This memorandum provides updated instructions for agency reporting under the Federal Information Security Management Act of 2002 (FISMA). Agency Chief Information Officers and Inspectors General have also received a copy of the attached instructions.

FISMA provides the framework for securing the Federal government's information technology. All agencies covered by the Paperwork Reduction Act must implement the requirements of FISMA and report annually to the Office of Management and Budget (OMB) and Congress on the effectiveness of their security programs. The reports must also include independent evaluations by the agency Inspector General.

Agencies are to transmit their FY04 reports to OMB by October 6, 2004. Guidance for transmitting the reports to Congress is set out in the attached instructions.

OMB uses the reports to help evaluate government-wide security performance, develop its annual security report to Congress, assist in improving and maintaining adequate agency security performance, and inform development of the E-Government Scorecard under the President's Management Agenda.

In addition to the formal report transmittal to OMB, an electronic copy of the report should also be sent to Kristy LaLonde at klalonde@omb.eop.gov and Daniel Costello at daniel_j._costello@omb.eop.gov. Please contact Glenn Schlarman at 202-395-4951 if you have any questions.

We appreciate your ongoing efforts in addressing this critical issue and for completing these reports in an accurate and timely manner.

Attachments

Reporting Instructions

Section A – Instructions for Completing the Annual Federal Information Security Management Act (FISMA) Report.

This section contains instructions for completing the FY04 FISMA reporting template. The reporting template is attached and is to be used by agencies as their FY 04 FISMA report.

Section B – Reporting on Remediation Efforts and Updating Performance Measures

This section contains directions for agencies on quarterly reporting on IT security efforts. It includes the quarterly reporting of agency remediation efforts through agency plan of action and milestones (POA&Ms) and the quarterly reporting of agency progress against a subset of IT security performance measures.

Section C – Definitions

The definitions in this section reference terms and concepts used in the report and for implementing FISMA.

Section D – Reporting Template for Micro-agencies

All the requirements established in FISMA apply to all agencies regardless of their size. OMB has developed an abridged reporting format for micro-agencies. This abridged template for micro-agencies does not exempt them from FISMA requirements and OMB guidance, and reporting requirements for quarterly updates and POA&Ms are the same for micro-agencies as they are for other agencies. Micro-agencies employ fewer than 100 Federal employees.

Section E – Reporting Template for the Annual Report

This section is the reporting template for agencies to use in completing their FY 2004 FISMA report.

SECTION A

REPORTING ON FEDERAL GOVERNMENT INFORMATION SECURITY MANAGEMENT

Section A consists of two parts:

- Part I – Reporting instructions for developing the agency report.
- Part II – Questions and answers to further assist agencies and IGs in meeting the annual review and reporting requirements.

In general, these instructions for reporting the results of FY04 FISMA reviews remain nearly identical to earlier instructions. These instructions continue OMB emphasis on performance measures and provide additional instructions for clarification.

I. Instructions for the Agency and IG Report

Each agency head shall transmit to the OMB Director a report that summarizes the results of annual IT security reviews of systems and programs, agency progress on correcting weaknesses[1] reflected in their POA&Ms, and the results of IG independent evaluations. Additionally, the agency head shall send copies of complete IG independent evaluations. These reports continue to be the primary basis of OMB's summary report to Congress, and all agencies shall provide responses for each of the performance measures in the attached spreadsheet format.

The reporting template is an excel file of performance measures. Responses to the questions found in the excel file are numerical in nature, and must follow the prescribed format provided. The responses should be based on the results of the annual system and program reviews, the agency's work in correcting weaknesses identified in their POA&Ms[2], and any other work performed throughout the reporting period. Extensive narrative responses are discouraged, and agencies can provide any further qualitative assessment from their evaluation in corresponding comment boxes. If an agency has developed additional performance measures, they may be reported as well. Incomplete reporting against the provided performance measures will make the entire report incomplete and unacceptable.

The agency report shall consist of two separate components. One is to be prepared by the IG[3], characterizing the results of their independent evaluations and agency progress in implementing their POA&Ms. The other component is to be prepared by the CIO, working with program officials, reflecting the results of their annual system and program reviews and progress in implementing their POA&Ms.

[1] The term weakness refers to any and all IT security weaknesses pertaining to that system. When the guidance refers to a significant deficiency, the term significant deficiency will be used.

[2] Agency POA&Ms must reflect known security weaknesses within an agency including its components or bureaus and shall be used by the agency, major components and program officials, and the IG as the authoritative agency management mechanism to prioritize, track, and manage all agency efforts to close security performance gaps.

[3] Per FISMA, for each agency without an IG, the head of the agency shall engage an independent external auditor to perform the evaluation.

Annual reports under FISMA are to be sent to OMB and the Committees on Government Reform and Science of the House, the Committees on Government Affairs and Commerce, Science, and Transportation of the Senate, the authorization and appropriations committees for each individual agency of Congress, and GAO. Agencies may forward their report to the appropriate Congressional Committees and GAO after it has been reviewed by OMB and OMB has notified the agency.   Copies of the IG's independent evaluations may be released to Congress at any time following their submission to OMB.

Part II of this section provides additional information, in the form of Q&As, to agencies to assist them in implementing FISMA and OMB requirements.

II. Q&As for CIOs, Agency Program Officials, and IGs

A. Guidance Pertaining to CIOs and Agency Program Officials

Must government contractors abide by FISMA requirements?

Yes. 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 that each agency 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."

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 that of 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).

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 is responsible for ensuring that FISMA requirements are met.

Is use of NIST publications required?

Yes, for non-national security programs and systems, agencies must follow NIST standards and guidance. Federal Information Processing Standards (FIPS) must be implemented as written; the only flexibility exists within the standard itself. Special publications of the NIST 800 series and other NIST publications are guidance. As a general rule, use of NIST guidance is more flexible, provided agency implementation is consistent with the principles and processes outlined within the NIST guidance. However, from time to time, OMB policy will mandate stricter use of NIST guidance. For example, NIST Special Publication 800-26 is mandatory for use for agency annual systems reviews.

Reviews and evaluations of agency IT security programs and systems should consider adherence to standards and consistency with NIST guidance. Where flexibility exists, evaluations must consider unique operational environments and allow for a reasonable degree of discretion.

What is the link between the E-Authentication Risk Assessment and the FISMA Risk Assessment and Certification and Accreditation Security Requirements?

The E-Authentication Guidance for Federal Agencies established the requirement that agencies conduct an e-authentication risk assessment on those systems that remotely authenticate users over a network for purposes of e-government and commerce.

On December 16, 2003 OMB issued M-04-04, "E-Authentication Guidance for Federal Agencies." As stated in M-04-04, agencies must categorize all existing transactions/systems requiring user authentication into one of the described assurance levels by September 15, 2005. Agencies should accomplish this in the following order:

- Systems categorized as "major" must be completed by December 15, 2004.
- New authentication systems should begin to be categorized, as part of the system design on September 24, 2004. This is 90 days following the completion of the final E-Authentication Technical Guidance issued by NIST. NIST Special Publication 800-63 "Recommendation for Electronic Authentication" is available at http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63v6_3_3.pdf.

This risk assessment should be conducted in parallel with the overall system risk assessment and in the context of greater policy issues, and should be conducted with the advice of agency legal, policy, privacy, and agency business process owners. Additionally, agencies should address the requirements of M-04-04 in their System Security Plans and certify the requirements prior to authorization to process.

Why is OMB asking 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[4]". OMB expects agency policies and training programs to be consistent with the CIO Council guidance.

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

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 should confirm that the agency-wide security program or the security program of the major component which operates the field offices is effectively overseeing and measuring field performance, that any weaknesses are included in the agency's POA&M, and that the office responsible for programs and systems are developing, implementing, and maintaining their POA&Ms.

When should program officials and CIOs provide the results of their reviews to their agency IG?
Program officials and CIOs should share the findings from program and system security reviews with their IG as they become available.

Do all agency systems have to be reviewed annually?
Yes. Senior agency program officials and CIOs must review all programs and systems at least annually. The purpose of the security program discussed in FISMA is to ensure the protection of the systems and data covered by the program, thus a review of each system is essential to determine the program's effectiveness. Only the depth and breadth of such system reviews are flexible.

What level of review is required for an individual system?
Program officials and CIOs are responsible for reviewing the security of all programs and 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 last year's 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 within the agency. The salient point is that 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 review for their systems with the understanding that all systems must be reviewed annually. IGs may report on the adequacy of such reviews.

What methodology must agencies use to review systems?
Agencies should use NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems" to conduct their annual reviews. Another guide may be used if the agency and the IG confirm in their report, that any agency developed methodology captures all elements of the NIST guide.

What reporting is required for national security programs and systems?

FISMA requires that all programs, including national security programs, be reviewed every year. Agencies should include all agency national security systems when completing the FISMA report. Agencies can choose to provide responses to the questions in the template either in aggregate with or separate from their non-national security systems.

Furthermore, agencies should describe how they are implementing the requirements of FISMA for national security programs and systems in their report. The description should 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. The description should also identify the number of independent evaluations conducted. Agencies must also develop POA&Ms (see Section C) for identifying and managing weaknesses in their national security programs and systems, but for obvious sensitivity reasons, they need not be fully integrated with POA&Ms for non-national security programs.

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.

What is a significant deficiency in the context of reporting as a material weakness or lack of substantial compliance under FISMA section 3544(c)(3)?

This discussion applies only to the reporting of significant deficiencies pursuant to FISMA section 3544(c)(3). Use question B.1 on the attached annual reporting spreadsheet to report significant deficiencies.

> **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. A significant deficiency under FISMA is to be reported as a material weakness under the Federal Managers Financial Integrity Act (FMFIA).
>
> **Reportable Condition –** A reportable condition exists when a security or management control weakness does not rise to level of a significant deficiency, yet is still important enough to be reported to internal management. A security weakness not deemed to be a significant deficiency by agency management, yet affecting the efficiency and effectiveness of agency operations, may be considered a reportable condition. However, due to lower risk, corrective action may be scheduled over a longer period of time. A reportable condition under FISMA is not reported as a material weakness under FMFIA.

FISMA requires the reporting of any significant deficiency in a policy, procedure, or practice to be identified as a material weakness under the FMFIA and if relating to financial management systems, as an instance of a lack of substantial compliance under FFMIA.

Depending upon the risk and magnitude of harm that could result, weaknesses identified during the review of security controls should be reported as deficiencies in accordance with OMB Circular No. A-123, "Management Accountability and Control" and FMFIA. In particular, if a basic management control such as assignment of responsibility, a workable security plan, or management authorization are missing, then consideration should be given to identifying a significant deficiency.

Determining whether a security weakness is a significant deficiency must be a risk-based decision. Before designating a weakness as a significant deficiency, agency management and IGs must carefully consider if weaknesses are systemic in nature and adversely affect other forms of management control as well as the gravity of the risk and magnitude or harm which may result should the weakness remain uncorrected.

Simply put, not all security weaknesses introduce the same level of risk. For example, never having performed a certification and accreditation of a system is more problematic than having certification and accreditation expire simply due to passage of time. Similarly, failure to test and evaluate security controls within a high-risk national security system is starkly different than the same failure for a low-risk publicly accessible website. Additionally, a general failure to adequately train agency employees on their security responsibilities introduces different risks than not training systems administrators on their specialized security responsibilities. Whether any of the circumstances in the examples warrants designation as a significant deficiency can only be determined after thoughtful consideration of the actual risk on a case-by-case basis.

Reportable conditions are not required to be reported in the annual FISMA report, but as with all other weaknesses, are to be included in the agencies' POA&M.

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 that maintain 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.

How often do I need to test and evaluate my security controls?

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 evaluation will include the testing of management, operational, and technical controls.

This provision does not require annual testing of the complexity required for certification and accreditation of systems as described in NIST guidance. Rather, it recognizes the importance of maintaining a continuous process of assessing risk and ensuring that security controls maintain risk at an acceptable level. This provision also underscores the need to understand the security status of each system in order to accurately maintain system-level POA&Ms and report annually on the overall health of an agency's IT security program.

The necessary depth and breadth of an annual FISMA review depends on several factors such as: 1) the acceptable level of risk and magnitude of harm to the system or information; 2) the extent to which system configurations and settings are documented and continuously monitored; 3) the extent to which patch management is employed for the system; 4) the relative comprehensiveness of the most recent past review; and 5) the vintage of the most recent in-depth testing and evaluation as part of system certification and final accreditation.

For example, if in the previous year a system underwent a complete certification and received final (not interim) authority to operate, has documented configuration settings, employs automated scanning tools to monitor configurations, threats, and vulnerabilities, and has an effective patch management capability, a simple maintenance review using NIST's self assessment tool may meet the FISMA annual review requirement. If none or only some of the foregoing are true, then the annual testing and evaluation must be far more comprehensive and commensurate with the acceptable level of risk and magnitude of harm. Agency officials must use sound judgment when determining the scope and rigor of FISMA's annual test and evaluations. The agency should address shortcomings found during review of risk assessments, security plans, contingency plans, or certification and accreditations as they are discovered.

The flexibility described above does not alter OMB policy requiring system reauthorization (certification and accreditation) at least every three years or when significant changes are made, e.g., connecting to new systems or changes to configurations, hardware, or software. For non-national security systems, agency certification and accreditation processes must be consistent with NIST guidance. All certifications and accreditations initiated after finalization of NIST Special Publication 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems", must be consistent with NIST Special Publication 800-37. Consistent with earlier guidance, complete certifications and accreditations include up-to-date and complete risk assessments and security plans, and only systems granted a full and final authorization to operate are to be considered certified and accredited. Additionally, the flexibility described does not dilute the statutory requirement that all systems must be reviewed annually.

What data is included in an agency's inventory of systems?
FISMA (see section 3505(c)) amends the Paperwork Reduction Act and requires the head of each agency to develop and maintain an inventory of major information systems (including major national security systems) operated by or under the control of the agency. An inventory of each agency's major information systems has been required for many years by the Paperwork Reduction Act and, more recently, by the 1996 Electronic Freedom of Information Act amendments. The definition of "major information system" is found in OMB Circular A-130 (and in the attached glossary).

FISMA also states (see section 3505(c)(2)) "the identification of information systems in this inventory under this subsection shall include 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." OMB expects agencies to have an inventory based on work in developing an enterprise architecture. Agencies inventories must appropriately identify system criticality and risk levels.

The FISMA amendments also state the inventory be updated at least annually, made available to the Comptroller General when requested, and used to support information resources management including monitoring, testing, and evaluation of information security controls.

B. Guidance Pertaining to Agency Inspectors General

FISMA directs IGs or their designee, to perform "an annual independent evaluation of the information security program and practices of the agency to determine the effectiveness of such program and practices." The evaluation shall include testing of the effectiveness of information security policies, procedures and practices, to make an assessment of the compliance with information technology security policies, procedures, standards and guidelines. The testing should include an appropriate subset of agency systems. In this regard, FISMA does not limit the subset to financial systems. To ensure a complete picture of an agency program, IGs should evaluate a representative sampling of all types of agency systems. The IG evaluation must be sufficiently broad to provide a reasonable view of the entire agency IT security program. FISMA also permits IGs to use the results of any other review in performing their work which occurred during the FY04 reporting period. Assessment of the quality of security procedures and practices remains essential for any evaluation.

Within the context of FISMA, an audit is not contemplated. By requiring an evaluation but not an audit, FISMA intended to provide IGs some flexibility as to the degree of cooperation with CIOs and program officials as well as with the rigor of their review. OMB encourages IGs to take advantage of that flexibility while ensuring the appropriate degree of accuracy, independence, and objectivity.

IGs should respond to all questions using results from their evaluations. IGs should use the CIO responses in addition to their evaluation activities to assist in assessing agency performance. IGs are not requested to validate agency-reported performance measures, but rather to assess the reliability of the data based on their evaluation of their representative subset of systems. IG evaluations are based on a representative subset of systems, therefore it is not expected the IG report and CIO report contain identical responses when a question refers to numbers of systems. For example, if the IG evaluation reviewed security plans for ten systems, and found nine of ten systems with complete and up to date security plans, the IG response to the number of systems with security plans (A.2.a.) would be nine and the response to the number of systems (A.1.b.) would be ten. IG responses should include information on the agency's progress in implementing and maintaining their POA&Ms, and any other work performed throughout the reporting period (e.g., financial statement audits). IGs can use the comment area below each question to explain any qualitative assessment of the activity in question. For example, when asked to evaluate the frequency by which the agency follows documented policies and procedures for reporting incidents, the IG could include a brief synopsis of the strengths and weaknesses associated with that process within the agency.

IGs are again asked to assess against minimum requirements whether the agency has developed, implemented, and is managing an agency-wide POA&M process (see Section C of the reporting template). The IG's POA&M assessment is essential for agencies to establish and maintain effective POA&M processes. Effective remediation of IT security weaknesses is essential to achieving a mature and sound IT security program and securing our information and systems. The IG's assessment of the agency's POA&M process is also instrumental to the agency's ability to get to green under the Expanding E-Government Scorecard of the President's Management Agenda.

Finally, OMB is requesting IGs to assess the agency's certification and accreditation process in order to provide a qualitative assessment of this critical activity. This assessment should consider the quality of the agency certification and accreditation process. Any new certification and accreditation work initiated after completion of NIST Special Publication 800-37 should be consistent with NIST Special Publication 800-37. This includes use of the FIPS 199, "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. Earlier NIST guidance is applicable to any certification and accreditation work completed or initiated before finalization of NIST Special Publication 800-37. Agencies were not expected to use NIST Special Publication 800-37 as guidance before it became final.

Should IGs review the agency CIO/program official report to OMB to develop their independent evaluation?

Not as the exclusive input for their review. IGs, CIOs, and program officials should work together throughout the year to ensure the development and maintenance of a comprehensive POA&M process and collaborate on preparing the report to OMB. Agencies have varying approaches to their review. Regardless of the approach taken, IGs should not rely solely on a review of the CIO/program officials' report as fulfilling their requirements under FISMA. Furthermore, an IG review should not result in artificial deadlines that restrict the amount of time allotted for comprehensive agency program and system reviews by CIOs and program officials.

Should IGs validate agency responses to the IT security performance measures?
No. OMB is not requesting IGs to validate agency responses to the performance measures. Rather, as part of IGs' independent evaluations of a subset of agency systems, IGs should assess the reliability of the data and quality of the processes creating the data for those systems they evaluate.

When should IGs provide the results of their reviews to agency program officials and CIOs?
Agency IGs should share findings from program and system security reviews and evaluations with agency CIOs as they become available, in a manner that preserves their independence. In particular, IGs should consider delivering interim reporting to agency officials in instances where potential significant deficiencies have been identified. Timely sharing and awareness of significant deficiencies helps prevent further loss and damage to the agency's overall performance.

SECTION B

Section B consists of three parts:

- Part I – Provides guidance on the agency-wide POA&M process, including examples of program and system-level POA&Ms.
- Part II – Provides guidance on submitting quarterly POA&M summary updates and guidance on quarterly reporting on performance measures.
- Part III – Provides a series of questions and answers to further assist agencies and IGs in developing, implementing, and reporting on POA&Ms.

I. Agency Plans of Action and Milestones Process

A plan of action and milestones (POA&M) is a tool identifying 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 a 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.

OMB policy requires agencies to prepare POA&Ms for all programs and systems where an IT security weakness has been found. The guidance directs CIOs and agency program officials to develop, implement, and manage POA&Ms for all programs and systems they operate and control (e.g., for program officials this includes all systems that support their operations and assets). Additionally, program officials shall regularly (at least quarterly and at the direction of the CIO) update the agency CIO on their progress to enable the CIO to monitor agency-wide remediation efforts and provide the agency's quarterly update to OMB.

POA&M Requirements

Agency POA&Ms must:

1. Be tied to the agency's budget submission through the unique project identifier of a system. This links the security costs for a system with the security performance of a system.
2. Include all security weaknesses found during any other review done by, for, or on behalf of the agency, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments. These plans should be the authoritative agency-wide management tool, inclusive of all evaluations.
3. Be shared with the agency IG to ensure independent verification and validation of identified weaknesses and completed corrective actions.
4. Follow the format detailed in the examples under Part II of this section.
5. Be submitted to OMB upon request.

Assisting Congressional Oversight

POA&Ms are designed to: 1) be a management tool to assist agencies in closing their security performance gaps; 2) assist IGs in their evaluation work of agency security performance; and 3) assist OMB with our oversight responsibilities. As a result and by design, these plans contain predecisional budget information. Per longstanding Executive Branch policy and practice, OMB and the agencies have a responsibility to maintain the confidentiality of predecisional, deliberative budget related information. OMB has addressed this issue in the guidance last year, which we continue in the FY04 FISMA guidance, to enable agencies to release information from their POA&Ms to Congress so that it may carry out its oversight role, while preserving the confidentiality of the Executive Branch's pre-decisional discussions.

Additionally, copies of the quarterly updates discussed in Part II (below) have also been requested by the House Government Reform's Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census. Agencies can send their updates to the Subcommittee.

POA&M Instructions

Attached is one example POA&M for a program and one for a system. Each illustrates the appropriate level of detail required. Once an agency has completed the initial POA&M, no changes should be made to the data in columns 1, 4, 5, and 7. The heading of each POA&M must include the unique project identifier from the exhibits 300 and 53, where applicable.[5]

Column 1 **–** Severity and brief description of the weakness. There are three severities of weaknesses: significant deficiency, reportable condition, and other weakness. The description of the weakness includes those identified by the annual program review, IG independent evaluation, or any other work done by or on behalf of the agency. Sensitive descriptions of specific weaknesses are not necessary, but sufficient data must be provided to permit oversight and tracking. Where it is necessary to provide more sensitive data, the POA&M should note the fact of its special sensitivity. Where more than one weakness has been identified, agencies should number each individual weakness as shown in the examples.

Column 2 **–** Identity of the office or organization that the agency head will hold responsible for resolving the weakness.

Column 3 **–** Estimated funding resources required to resolve the weakness. Include the anticipated source of funding (i.e., within the system or as a part of a cross-cutting security infrastructure program). Include whether a reallocation of base resources or a request for new funding is anticipated. This column should also identify other, non-funding, obstacles and challenges to resolving the weakness (e.g., lack of personnel or expertise, development of new system to replace insecure legacy system, etc).

[5] OMB Circular A-11 requires that agencies develop and submit to OMB capital asset plans (exhibit 300) for major acquisition projects. For information technology projects, plans for major systems must be reported to OMB on an exhibit 300 and 53. The agency assigns a unique identifier to each system and applies it to both exhibits.

Column 4 **–** Scheduled completion date for resolving the weakness. Please note that the initial date entered should not be changed. If a weakness is resolved before or after the originally scheduled completion date, the agency should note the actual completion date in Column 8, "Status."

Column 5 **–** Key milestones with completion dates. A milestone will identify specific requirements to correct an identified weakness. Please note that the initial milestones and completion dates should not be altered. If there are changes to any of the milestones the agency should note them in the Column 6, "Changes to Milestones."

Column 6 – Changes to Milestones. This column would include new completion dates for the particular milestone. See example.

Column 7 **–** The agency should identify the source (e.g., program review, IG audit, GAO audit, etc.) of the weakness. Sources include weaknesses that have been identified as a significant deficiency, or reportable condition, or other in the latest agency IG audit under other applicable law (e.g., financial system audit under the Financial Management Integrity Act, etc).

Column 8 **–** Status. The agency should use one of the following terms to report status of corrective actions: Ongoing or completed. "Completed" should be used only when a weakness has been fully resolved and the corrective action has been tested. Include the date of completion. See example.

Sample Agency or Program-level Plan of Action and Milestones
Agency, Component, and Program Name -- Department of Good Works, Major Service Administration

Weaknesses	POC	Resources Required	Scheduled Completion Date	Milestones with Completion Dates	Changes to Milestones	Identified in CFO Audit or other review?	Status
1—Reportable Condition. No program-level security program or plan	Program office and agency CIO	$10k	3/1/04	Draft plan prepared and circulated for user input -- 11/30/04		Yes--1/17/04 report	Ongoing, 9/1/04
				Comments reviewed, final draft to Administrator for approval and publication -- 3/1/04			
2 – Reportable Condition. No documented program to report external security incidents to law enforcement and GSA	Program office and agency CIO	None	10/31/03	Consult with agency IG, FBI/NIPC, and GSA - 10/15/04			Completed, 10/31/03
				Procedures published, employees trained 10/30/04			
3 – Weakness. No documentation for data sensitivity levels -- thus cannot document acceptable risk and security needs	Program office and agency CIO	$25K	5/30/04	Review enterprise architecture (process and data layers) to define and categorize data type and sensitivity -- 12/1/04			Ongoing,12/ 30/04
				Identify acceptable risk for each level, identify protection needs, document, publish, and implement -- 1/30/05			
4 – Reportable Condition. Security not integrated w/capital planning process. Security costs not shown in exhibits 300 & 53.	Agency CIO	Estimated $15K	1/30/04	Review and update all program exhibits 300 & 53			Ongoing, 8/1/04

System-level Security Plan of Action and Milestones

Cite unique project ID and name shown on exhibit 300 and security costs from exhibit 53. If no 300 or 53 cite name only:

Project ID = Project name = Security costs =

Weaknesses	POC	Resources Required	Scheduled Completion Date	Milestones with Completion Dates	Milestone Changes	Identified in CFO Audit or other review?	Status
1 – Weakness. Password controls improperly configured and not tested	Program office, name and contact info of accountable person	$5k	10/1/04	Reconfigure and test password controls -- 10/1/04		Yes	Completed, 10/1/04
2 – Weakness. Security plan is out of date, more than one year since last update despite new interconnections	Program office	$20k	11/30/04	Update plan and obtain independent review -- 11/30/04		No	Ongoing, 11/30/04
3 – Significant Deficiency. No written management authorization prior to system operations	Program office & Agency CIO	$25k	12/30/04	Complete certification and accreditation procedures per up-to-date security plan and NIST guidance. Obtain written auth -- 12/15/04		Yes	Ongoing, 1/30/05
4 – Significant Deficiency. System is contractor operated and contract does not include any security and privacy requirements nor are contractor practices evaluated by agency	Program office, contracting officer, and agency CIO	None	1/30/04	Identify specific security requirements, including for contractor personnel, and revise contract accordingly -- 1/30/04		No	Ongoing, 12/30/04
5 – Reportable Condition. System vulnerabilities have not been periodically tested.	Program office and agency CIO	$50K	1/15/05	Arrange for system vulnerability testing -- 10/15/04		Yes	Ongoing, 1/15/05
				Implement and test new security controls and schedule retest -- 1/15/05			
6 – Weakness. Life cycle system costs not incorporated into system funding	Program office and agency CIO	None	10/30/04	Identify costs. Update Exh. 300 & 53. Reallocate funds from lower system priorities -- 10/30/01			

II. Quarterly Reporting of the POA&M Summary Table and IT Security Performance Measures

Agencies must provide on a quarterly basis summary information on the POA&M progress and an update on IT security performance measures. The quarterly updates are to be submitted together and should follow the table formats below. Quarterly updates are due September 15, 2004, December 15, 2004, March 15, 2005, and June 15, 2005. Quarterly updates are to be sent electronically to Kristy LaLonde at klalonde@omb.eop.gov and Dan Costello at daniel_j._costello@omb.eop.gov.

The quarterly updates enable the agency and OMB to monitor agency remediation efforts and identify progress and problems. Additionally, these updates are used to assess agency IT security status and progress under the Expanding E-Government Scorecard under the President's Management Agenda.

IT security is one of a number of critical components agencies must meet to get to green (or yellow) for the E-Gov Scorecard. If the IT security criteria are not successfully met, agencies will not be able to move forward to yellow or green, regardless of their performance against other E-Gov criteria. These quarterly updates from agencies directly inform the quarterly scorecard assessment.

If an IG finds through their FY04 FISMA evaluation that the agency does not have an agency-wide IT security POA&M process meeting OMB criteria, OMB will work with the agency and IG to ensure the agency addresses the weaknesses identified by the IG and timely follow-on review by the IG occurs. This step will avoid unnecessary delays in preventing an agency from moving forward on their E-Gov Scorecard.

POA&M Summary Table						
		a. Total number of weaknesses identified at the start of the quarter.	b. Number of weaknesses for which corrective action was completed on time (including testing) by the end of the quarter.	c. Number of weaknesses for which corrective action is ongoing and is on track to be completed as originally scheduled.	d. Number of weaknesses for which corrective action has been delayed including a brief explanation for the delay.	e. Number of new weaknesses discovered following the last POA&M update and a brief description of how they were identified (e.g., agency review, IG evaluation, etc.).
Bureau						
	Program-level					
	System-level					
Bureau						
	Program-level					
	System-level					
Total						
	Program-level					
	System-level					

Quarterly Update of IT Security Performance Measures											
a. Bureau Name	b. Total Number of Systems	c. Number of systems certified and accredited*		d. Number of systems with security control costs integrated into the life cycle of the system		e. Number of systems for which security controls have been tested and evaluated in the last year		f. Number of systems with a contingency plan		g. Number of systems for which contingency plans have been tested	
		No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total											

*Certified and accredited systems operate with up-to-date and complete risk assessments and security plans

III. Q&As on POA&Ms and Quarterly Updates

When does my agency provide quarterly updates?
There are two components of the quarterly update: the POA&M summary table and the update of performance measures. The POA&M summary table and the update of performance measures are to be provided to OMB on September 15, 2004, December 15, 2004, March 15, 2005, and June 15, 2005.

When do we submit the agency POA&M?
The agency POA&M is to be submitted to OMB upon request.

How many POA&Ms should an agency prepare?
An agency should develop a separate POA&M for every program and system for which weaknesses[6] were identified in the FISMA reports, as well as those discovered during other reviews including GAO audits, financial system audits, and critical infrastructure vulnerability assessments. Thus, the POA&Ms should either reflect consolidation with, or be accompanied by, other agency plans to correct security weaknesses found during any other review done by, for, or on behalf of the agency, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments.

Who in the agency is responsible for developing a POA&M?
Agency program officials must develop, implement, and manage corrective action plans for all systems that support their operations and assets. CIOs must develop, implement, and manage corrective action plans for all programs and systems they operate and control.

[6] The term weakness refers to any and all weaknesses.

Who uses the POA&M?

These plans are designed to be used largely by: (1) CIOs, program officials, and other appropriate agency employees to track progress of corrective actions; (2) IGs to perform follow-up work with agencies; and (3) OMB to assist in its oversight responsibilities and to inform the budget process.

How is the POA&M tied to the budget process?

To promote greater attention to security as a fundamental management priority, OMB integrated IT security into the capital planning and budget process. This integration is already producing tangible benefits by promoting security that comports with the agency's enterprise architecture, supports business operations, and is funded within each information system over its life-cycle. To further assist in this integration, the POA&Ms and annual security reports and executive summaries must be cross-referenced to the budget materials sent to OMB in the fall including exhibits 300 and 53.

Specifically, for each POA&M that relates to a project (including systems) for which a capital asset plan and justification[7] (exhibit 300) was submitted or was a part of the exhibit 53, the unique project identifier must be reflected on the POA&M. This identifier will provide the link to agency budget materials.

On all POA&Ms which reflect estimated resource needs for correcting reported weaknesses, agencies must specify whether funds will come from a reallocation of base resources or a request for new funding. While the POA&Ms will not be used as agency funding requests by OMB, a brief rationale should be provided when a request for new funding is contemplated.

For how long do I report corrected weaknesses?

Weaknesses that are no longer undergoing correction and have been completely mitigated for over a year should no longer be reported in the agency POA&M.

Are there special considerations for POA&Ms for national security systems or DOD mission critical systems?

Yes. Due to their special sensitivity and the unique way they are addressed in FISMA, reporting weaknesses in national security systems as well as certain systems under the control of the Department of Defense and Intelligence Community is being addressed differently than for other systems. Although we certainly suggest that agencies document corrective plans of action for their own use, we are not prescribing a particular format. Prior to reporting such corrective action plans to OMB, we request that you consult with us so that we can make appropriate arrangements as to level of detail and sensitivity of what you should report.

[7] OMB Circular A-11 requires that agencies develop capital asset plans for all capital asset acquisition projects and report to OMB, via an exhibit 300, those plans for all major acquisitions. For information technology projects, plans for major systems must be reported to OMB. Agencies assign a unique identifier to each system and apply it to the exhibit 300 and 53.

What format should an agency use to create a POA&M?
Agencies must use the attached spreadsheet-type format for their POA&Ms. At a minimum, agency POA&Ms must contain the information found on the attached spreadsheet. Each program and system where a weakness was identified should have its own POA&M. Agencies shall submit their POA&Ms to OMB via email or on diskette as a Microsoft Excel spreadsheet.

Should quarterly IT security reports be sent to the OMB Director from the agency head?
No. Quarterly updates are to be emailed to Kristy LaLonde at klalonde@omb.eop.gov and Daniel Costello at daniel_j._costello@omb.eop.gov by the agency CIO.

May agencies release their POA&Ms outside of OMB?
To maximize the usefulness of these plans, OMB intentionally and specifically tied the plans to the budget process. This assists both the agencies and OMB in determining and prioritizing budget decisions. As a result and by design, these plans contain predecisional budget information. Per longstanding Executive Branch policy and practice, OMB and the agencies have a responsibility to maintain the confidentiality of the deliberative discussions that led to the President's budget decisions.

Congress clearly has a need for information about an agency's information security activities and FISMA compliance in order to carry out its oversight role. Therefore agencies may release to Congress, as requested, the following information (as described under section II, POA&M Instructions) from their POA&Ms: 1) type of weakness as reported under column 1; 2) key milestones as reported under column 5; 3) any milestone changes as reported under column 6; 4) source of identification of the weakness as reported under column 7; and 5) the status of the weakness as reported under column 8. This will enable agencies to release information from their POA&Ms to Congress so that it may carry out its oversight role, while preserving the confidentiality of the Executive Branch's pre-decisional budget discussions.

What level of detail and sensitivity should the POA&Ms include?
Detailed descriptions of specific weaknesses are not necessary, but sufficient data is necessary to permit oversight and tracking. For example, to the maximum extent practicable agencies should use the types of descriptions commonly found in reports of the GAO and IGs such as "inadequate password controls," "insufficient or inconsistent data integrity controls," "inadequate firewall configuration reviews," "background investigations not been performed prior to system access," "physical access controls are insufficient," etc. Where it is necessary to provide more detailed data, the POA&M should note the fact of its special sensitivity.

What security precautions is OMB taking to adequately protect the POA&Ms?
As with all sensitive information within OMB, access to POA&Ms (particularly the collection of all POA&Ms) will be limited to those OMB officials and staff that have an explicit business purpose for their use.

SECTION C

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.

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 (OMB 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 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 security of the systems in which they operate.

Major IT Investment (defined in OMB Circular A-11, section 300)
Major IT Investment means a system or investment that requires special management attention because of its importance to an agency’s mission; investment was a major investment in the FY 2004 submission and is continuing; investment is for financial management and spends more than $500,000; investment is directly tied to the top two layers of the Federal Enterprise Architecture (Services to Citizens and Mode of Delivery); investment is an integral part of the agency’s modernization blueprint (EA); investment has significant program or policy implications; investment has high executive visibility; investment is defined as major by the agency’s capital planning and investment control process. OMB may work with the agency to declare other investments as major investments. All major investments must be reported on exhibit 53. All major investments must submit a "Capital Asset Plan and Business Case," exhibit 300. Investments that are e-government in nature or use e-business technologies must be identified as major investments regardless of the costs. If you are unsure about what investments to consider as "major," consult your agency budget officer or OMB representative. Systems not considered "major" are "nonmajor."

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.

Program Review (defined by OMB guidance)
A program review, in the context of the work required under FISMA, is a review of the security status of an operational program and is not a security program itself. Each program must be reviewed annually to ensure: 1) risk assessments occur; 2) policies and procedures are risk-based and cost-effective and comply with existing laws and OMB policy; 3) security awareness training for all employees; 4) management testing and evaluation of the effectiveness of information security policies and procedures; 5) a process for remedial action; and 6) procedures for detecting, reporting, and responding to security incidents.

Reportable Condition
A reportable condition exists when a security or management control weakness does not rise to level of a significant deficiency, yet is still important enough to be reported to internal management and/or external agencies. A security weakness not deemed to be a significant deficiency by agency management, yet affecting the efficiency and effectiveness of agency operations, may be considered a reportable condition. However, due to lower risk, corrective action may be scheduled over a longer period of time. Decisions regarding the significance of deficiencies are risk-based and the agency head should carefully consider if weaknesses are systemic in nature and adversely affect other forms of management control.

IT Security Costs (defined in FY06 OMB Circular A-11, section 53)
In determining information and IT security costs, Federal agencies must consider the following criteria to determine security costs for a specific IT investment:

1. The products, procedures, and personnel (Federal employees and contractors) that are primarily dedicated to or used for provision of IT security for the specific IT investment. Do not include activities performed or funded by the agency IG. This includes the costs of:

    - risk assessment
    - security planning and policy
    - certification and accreditation

- specific management, operational, and technical security controls (to include access control systems as well as telecommunications and network security)
- authentication or cryptographic applications
- education, awareness, and training
- system reviews/evaluations (including security control testing and evaluation)
- oversight or compliance inspections
- development and maintenance of agency reports to OMB and corrective action plans as they pertain to the specific investment
- contingency planning and testing
- physical and environmental controls for hardware and software
- auditing and monitoring
- computer security investigations and forensics
- reviews, inspections, audits and other evaluations performed on contractor facilities and operations.

2. Other than those costs included above, security costs must also include the products, procedures, and personnel (Federal employees and contractors) that have as an incidental or integral component, a quantifiable benefit to IT security for the specific IT investment. This includes system configuration/change management control, personnel security, physical security, operations security, privacy training, program/system evaluations whose primary purpose is other than security; systems administrator functions; and, for example, system upgrades within which new features obviate the need for other standalone security controls.

3. Many agencies operate networks, which provide some or all necessary security controls for the associated applications. In such cases, the agency must nevertheless account for security costs for each of the application investments. To avoid "double-counting" agencies should appropriately allocate the costs of the network for each of the applications for which security is provided.

In identifying security costs, some agencies find it helpful to ask the following simple question, "If there was no threat, vulnerability, risk, or need to provide for continuity of operations, what activities would not be necessary and what costs would be avoided?" Investments that fail to report security costs will not be funded therefore; if the agency encounters difficulties with the above criteria they must contact OMB prior to submission of the budget materials.

Security Plan (defined in OMB Circular A-130, Appendix III, (A)(3)(a)(2)(a-g))
For General Support Systems: Agencies shall implement and maintain a plan for adequate security of each general support system. The security plan shall be consistent with guidance issued by NIST. Independent advice and comment on the security plan shall be solicited prior to the plan's implementation. System security plans must include: 1) a set of rules of behavior concerning use of, security in, and the acceptable level of risk for, the system; 2) required training for all users to ensure security responsibilities are met; 3) personnel controls; 4) an incident response capability to share information concerning common vulnerabilities and threats; 5) continuity of support; 6) cost-effective

technical security products and techniques; and 7) written management authorization, based upon the acceptance of risk to the system, prior to connecting with other systems.

(defined in OMB Circular A-130, Appendix III, (A)(3)(b)(2)(a-g))
For Major Applications: Agencies shall implement and maintain a plan for the adequate security of each major application, taking into account the security of all systems in which the application will operate. The plan shall be consistent with guidance issued by NIST. Advice and comment on the plan shall be solicited from the official responsible for security in the primary system in which the application will operate prior to the plan's implementation. Application security plans must include: 1) a set of rules concerning use of and behavior within the application; 2) specialized training for all individuals prior to access that is focused on their responsibilities and the application rules; 3) personnel security controls; 4) contingency planning; 5) appropriate security controls; 6) appropriate rules garnering the sharing of information from the application; and 7) public access controls where an agency's application promotes or permits public access.

Security Program (defined in OMB Circular A-130, Appendix III, (A)(3))
Agencies shall implement and maintain a program to assure that adequate security is provided for all agency information collected, processed, transmitted, stored, or disseminated in general support systems and major applications.

Each agency's program shall implement policies, standards and procedures which are consistent with government-wide policies, standards, and procedures issued by OMB, the Department of Commerce, the General Services Administration, and the Office of Personnel Management. Different or more stringent requirements for securing national security information should be incorporated into agency programs as required by appropriate national security directives. At a minimum, agency programs shall include the following controls in their general support systems and major applications: 1) assign responsibility for security; 2) have a security plan for all systems and major applications; 3) provide for the review of security controls; and 4) require authorization before processing.

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 Review – review based off procedures established in NIST 800-26 "Security Self-Assessment Guide for Information Technology Systems."

SECTION D

Name of agency	
Budget for IT security (in thousands)	
Was a self assessment using NIST guidelines conducted in FY04? (y/n)	
Was an Independent assessment conducted in FY04? (y/n)	
If yes, please attach. If no, why was assessment not conducted?	
# of significant deficiencies (in policies, procedures, or practices)	
# of significant deficiencies repeated from last year	
Total number of systems	
Number of systems assessed for risk (assessed the risk to operations and assets and determined the level of security appropriate to protect such operations and assets)	
Number of systems with security plans	
Number of systems certified and accredited	
Number of systems with security controls tested FY04	
Number of systems with contingency plans	
Number of systems with tested contingency plans	
Did you report IT security incidents to US-CERT (y/n)	
How many incidents did you report?	
Number of employees (including contractors)	
Number of users receiving IT security awareness training in FY04	
Number of IT security staff including contractors (employees or contractors with significant IT security responsibilities)	
Number of IT security staff who received specialized security training in FY04	
Was an FY04 POA&M submitted to OMB? (y/n)	
Number of weaknesses identified in POA&M	
Number of weaknesses reported corrected as of 9/24/04	