STATEMENT OF THE HONORABLE JEFFREY RUSH, JR.

INSPECTOR GENERAL

DEPARTMENT OF THE TREASURY

BEFORE THE HOUSE COMMITTEE ON GOVERNMENT REFORM

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,

INTERGOVERNMENTAL RELATIONS AND THE CENSUS

MARCH 16, 2004

Mr. Chairman, Ranking Member Clay, Members of the Subcommittee, thank you for the opportunity to testify in this hearing on "Information Security in the Federal Government: One Year into the Federal Information Security Management Act." In your letter of February 26, 2004, you asked me to address three points in my statement: (1) a summary of the state of information security at Treasury, (2) the methodology used to audit Treasury and the resources available to my office, and (3) the circumstances that led to the delay in reporting our results under the Federal Information Security Management Act (FISMA).

First, although we have been reporting on serious information security weaknesses since 1998, I will limit my testimony to work done in the past 3 years. This is the third year we have assessed the information security programs and practices in Treasury. Our reporting for Fiscal Years (FY) 2001 and 2002 was under the Government Information Security Reform Act (GISRA). All three assessments, as well as management's own assessments, have identified serious deficiencies in information security throughout the Department. We issued our most recent evaluation report pursuant to FISMA on December 15, 2003, and a separate, classified FISMA report on Treasury's national security systems on December 24, 2003. These deficiencies include:

- Most systems have not been certified and accredited.
- Treasury has been unable to provide an accurate inventory year-to-year of systems to be certified and accredited.
- Treasury's plans of action and milestones for fixing serious security weaknesses were not always complete or consistently reported on.
- Treasury does not have a fully functioning computer security incident response capability. In addition, the requirements for reporting incidents were not being applied consistently among Treasury offices and bureaus.
- Treasury did not use the National Institute of Standards and Technology's (NIST) guidance for all of its program and systems reviews. Other methodologies that Treasury used were not sufficient to substitute for the NIST requirements.

- Interdependencies and interrelationships of mission critical operations and assets were not fully identified.
- Treasury has not provided sufficient information technology (IT) security training to the majority of its employees.

At least some aspect of these weaknesses has been reported in each of the last 3 years. While some progress has been made, these weaknesses have largely gone uncorrected. In fact, in the critical area of certification and accreditation, Treasury's performance has declined.

With respect to certification and accreditation, for FY 2001, 18 percent of Treasury systems were certified and accredited; for FY 2002, 32 percent of Treasury systems were certified and accredited; and for FY 2003, 23 percent of Treasury systems were certified and accredited, Department-wide. It should be noted that the FY 2003 decline was significantly impacted by the number systems operated by the Internal Revenue Service (IRS) that were not certified and accredited. Not including the IRS systems, 69 percent were certified and accredited. Nevertheless, this matter has been further complicated by the Department's inability to provide an accurate inventory of its systems to be certified and accredited on a year-to-year basis. For example, in FY 2002 Treasury identified 626 systems requiring certification and accreditation; in FY 2003, Treasury identified 708 systems requiring certification and accreditation.

To its credit, Treasury management declared the lack of substantial compliance with information security requirements as a material weakness under the Federal Manager's Financial Integrity Act based on our FY 2002 evaluation. It continued to report this deficiency as a material weakness for FY 2003.

Second, in conducting our FY 2003 evaluation of Treasury's information security program and practices, we followed the guidance issued by the Office of Management and Budget (OMB) on August 6, 2003. For your reference, I have attached a copy of the guidance to this statement. The guidance prescribed a set of questions to be answered by both agency management and by the Offices of Inspector General (OIG). In this regard, OIGs were to evaluate a representative sample of all types of agency systems. FISMA also supports the OIGs' use of results of other IT-related reviews performed during the reporting period. One area that was emphasized this year was the OIGs' assessment, against specific criteria, of whether the agency developed, implemented, and was managing an agency-wide plan of action and milestones process. The plans of action and milestones process is key to effective remediation of IT security weaknesses and instrumental for an agency to get to "green" under the Expanding E-Government Scorecard of the President's Management Agenda.

For FY 2003, we participated with the Department's Office of Chief Information Officer and the Treasury Inspector General for Tax Administration in a joint data call to Treasury offices and bureaus. We performed limited verification of the data received. We also considered the results of our work performed during the year that directly impacted information security. For example, we observed a disaster recovery test for the Treasury Communications System and audited the Department's implementation of its critical infrastructure protection program. We also considered IT security audit work that was performed in connection with the audits of the Department and bureau FY 2003 financial statements.

Finally, as background to the reason for our delayed FISMA reporting, during March 2003, we divested approximately 70 percent of our staff to the Department of Homeland Security Office of Inspector General pursuant to the Homeland Security Act of 2002. Our audit staff was reduced from 165 to 62 during the last six months of the fiscal year. Our annual audit plan had to be completely revised. This divesture and subsequent attrition reduced our IT audit group from 14 to 5.

We had planned to complete our FISMA review by the OMB-prescribed deadline of September 22, 2003. However, with our much reduced staffing, we determined that we could not complete FISMA on schedule and sustain an accelerated audit of the Department's FY 2003 financial statements. In consultation with the Department and OMB, priority was given to our audit of the Department's FY 2003 financial statements, and we committed to issue our FISMA report 1 month later. Accordingly, the financial statement audit was completed on November 14, 2003, and we issued our FISMA report on December 15, 2003.

Considering our current staffing levels and looking forward, we have not been able, and do not anticipate being able to hire additional IT audit staff in the near future that would enable us to meet the anticipated FY 2004 FISMA reporting deadline. Thus, we plan to contract out the independent FY 2004 FISMA evaluation for non-national security systems. We will perform the FY 2004 FISMA evaluation for Treasury's national security systems with our staff. We also plan to perform audit work in certain key areas of vulnerability identified by our previous FISMA work. For example, we plan to audit Treasury's computer security incident response capability and conduct vulnerability scans of computer networks at selected bureaus. The results from these audit efforts, as well as any information security findings identified from our financial statement audits, will be integrated into our FISMA reporting for FY 2004.

This concludes my testimony. I would be pleased to answer any questions that the Committee may have. Thank you.

ATTACHMENT TO
TESTIMONY OF THE HONORABLE JEFFREY RUSH, JR.
INSPECTOR GENERAL, DEPARTMENT OF THE TREASURY
BEFORE THE HOUSE COMMITTEE ON GOVERNMENT REFORM,
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS
MARCH 10, 2004

Office of Management and Budget Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting*, dated August 6, 2003

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

August 6, 2003

THE DIRECTOR

M-03-19

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten
Director

SUBJECT: Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting

As you know, the security of the Federal government's information and information systems is a responsibility shared by every agency. The Administration's policy requires Federal agencies to take a risk-based, cost-effective approach to secure their information and systems, identify and resolve current IT security weaknesses and risks, as well as protect against future vulnerabilities and threats.

To assist Federal agencies in meeting their responsibilities, the President signed into law on December 17, 2002, the Electronic Government Act. Title III of this Act, the Federal Information Security Management Act (FISMA) along with OMB policy, lays out a framework for annual IT security reviews, reporting, and remediation planning. Under this framework, the Federal government is able to quantitatively determine both IT security progress and problems. This information is essential to ensuring that remediation efforts and IT resources are prioritized resulting in the timely resolution of IT security weaknesses.

This guidance provides direction to agencies on implementing FISMA and consists of the following four attachments:

- Attachment A – The information in this attachment is new and highlights the more substantive changes introduced by FISMA from previous IT security legislation.
- Attachment B – This attachment contains the FY03 FISMA reporting instructions for agencies and Inspectors General.
- Attachment C – This attachment contains directions for agencies on quarterly reporting on IT security efforts. It includes both the continued quarterly plan of action and milestones updates and performance measure updates.
- Attachment D – This attachment contains definitions in law and policy referenced in the guidance.

I would also like to take this opportunity to inform you of a number of actions OMB has undertaken to further assist agencies in improving their IT security status through the President's Management Agenda and the budget process. On a quarterly basis, agencies provide updates to OMB on their IT security efforts through quantitative performance measures and progress in remediating IT security weaknesses. This information is used to inform the agency's E-Government Scorecard under the President's Management Agenda.

Additionally, I am directing my staff to work with your agency to ensure that system remediation plans are implemented and appropriate resources are identified through the budget process to resolve critical IT security weaknesses.

Agency reports are due to OMB on September 22nd, 2003. Agency heads should transmit to OMB the agency report (containing both the agency and IG components) and copies of the IG's independent evaluations. This transmission represents a confirmation by the agency head of the agency's IT security status as detailed in the agency report. Your CIO and IG received an electronic copy of this guidance and templates to assist them in reporting. Agency reports will continue to serve as the primary basis for OMB's annual summary report to Congress.

A letter from the agency head that transmits the required information should be delivered to:

Joshua B. Bolten
OMB Director
Eisenhower Executive Office Building
Room 252
Washington, DC 20503

The agency reports along with copies of the independent evaluations and any other appropriate information should be sent electronically to Kamela White at kgwhite@omb.eop.gov. Instructions for submitting the quarterly IT security reports can be found in Attachment C.

Attachments

Table of Attachments

Attachment A – Transition from the Government Information Security Reform Act (GISRA) to the Federal Information Security Management Act (FISMA)

The information in this attachment is new and highlights the more substantive changes or additions introduced by FISMA from GISRA.

Attachment B – Reporting on Federal Government Information Security Management

This attachment contains the FY03 FISMA reporting instructions for agencies and IGs and a set of questions and answers to assist agencies and IGs. Most of the information in this attachment is identical to the FY02 reporting instructions, including the performance measures introduced in last year's guidance. One significant change directs IGs to assess against specific criteria, whether the agency has developed, implemented, and manages an agency-wide plan of action and milestones (POA&M) process. Additionally, there is a strong focus on performance measures to answer many of the questions and as a result the reporting instructions have been formatted to emphasize a quantitative rather than a narrative response.

Attachment C – Reporting on Remediation Efforts and Updating Performance Measures

This attachment contains directions for agencies on quarterly reporting on IT security efforts. This information is largely the same as in the FY02 guidance. It includes both the continued quarterly reporting of agency remediation efforts (through agency POA&Ms) and a new requirement for quarterly reporting of agency progress against a subset of the IT security performance measures in the FY03 reporting instructions.

Attachment D – Definitions

The definitions in this attachment are largely the same as those included in the FY02 GISRA guidance but have been updated to include new definitions introduced in FISMA.

This FY03 FISMA guidance and POA&M guidance replaces M-02-09, "Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones").

ATTACHMENT A

TRANSITION FROM GOVERNMENT INFORMATION SECURITY REFORM ACT TO FEDERAL INFORMATION SECURITY MANAGEMENT ACT

On December 17th, 2002, the President signed into law the E-Government Act (P.L. 107-347) which includes Title III, the Federal Information Security Management Act (FISMA). FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000 (GISRA) which expired in November 2002. FISMA continues the annual review and reporting requirements introduced in GISRA. In addition, FISMA includes new provisions aimed at further strengthening the security of the Federal government's information and information systems, such as the development of minimum standards for agency systems. The National Institute of Standards and Technology (NIST) will work with agencies in the development of those standards per their statutory role in providing technical guidance to Federal agencies.

Please note that an earlier version of FISMA was enacted as part of the Homeland Security Act (P.L. 107-296). As provided in 44 U.S.C. 3549 and as stated by the President in his signing statement for the E-Government Act, the version of FISMA in the Homeland Security Act is not in effect. The version of FISMA in effect and to which all agencies are held accountable is the version found in the E-Government Act referenced above.

This attachment highlights the significant changes from GISRA to FISMA.

A. Definitions

1. FISMA introduces a statutory definition for information security. This definition is not substantively different than that used in current OMB and agency policies or NIST guidelines. Therefore, this new definition does not require changes to current policies or programs. It reads: "The term 'information security' means 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."

All Federal information and information systems require some degree of security under one or more of the three elements of the forgoing definition.

2. Like GISRA, FISMA (section 3542(b)(3)) cites the Clinger-Cohen definition of IT which includes "equipment used by an executive agency directly or is used by a contractor under contract with the executive agency." However, FISMA's applicability is broadened by two other provisions.

First, 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." Second, 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."

Thus, 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, i.e., 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.

B. Changes to annual reporting requirements

FISMA (section 3544(c)(1)) makes the following modifications to agencies' annual reporting requirements:

Annual reports under FISMA must now 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.

Because of this broader distribution, the agency reports should not contain internal Executive Branch predecisional, deliberative information. FISMA requires that OMB report to Congress no later than March 1, but does not prescribe a date by which agency reports must be sent. Agency reports (including the Inspector General's independent evaluation) are due to OMB on September 22, 2003. Agencies shall forward their reports to the appropriate Congressional Committees and GAO after the reports have been reviewed by OMB and OMB has notified the agency. Copies of the Inspector Generals independent evaluations may be released to Congress any time following their submission to OMB.

FISMA requires that each agency's report include information regarding: 1) agency risk assessments; 2) security policies and procedures; 3) subordinate plans (i.e., individual system security plans); 4) training; 5) annual testing and evaluation; 6) corrective action process; 7) security incident reporting; and 8) continuity of operations. Each of these categories fit into the existing reporting categories prescribed in OMB guidance and thus require no additional data gathering or reporting on the part of the agencies.

C. System configuration requirements determined by the agency

FISMA (section 3544(b)(2)(D)(iii)) requires that each agency develop specific system configuration requirements that meet their own needs and ensure compliance with them. This provision encompasses traditional system configuration management, employing clearly defined system security settings, and maintaining up-to-date patches. Simply establishing such configuration requirements is not enough. It must be accompanied by adequate ongoing monitoring and maintenance.

OMB's reporting guidance will seek information on agency progress in meeting this new requirement, but for the first year will not judge the adequacy of that process.

One example to aid compliance with FISMA would be to employ the Windows 2000 configuration settings recently developed by NIST and NSA. Other configuration guides, for this and other operating systems and software applications are available or are also being developed by other sources and absent guidance from NIST could also be helpful. Agencies are reminded however, that OMB policy requires agency procedures be consistent with guidance issued by NIST when such is available.

Additionally, while many agencies have established patch authentication and distribution accounts through FedCIRC's government-wide patch management contract, actual usage of those accounts are extremely low. To ensure that agencies maintain up-to-date patches, it is critical that usage increase.

D. Annual testing and evaluation of security controls

FISMA (section 3544(b)(5)) requires each agency to perform for each system "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 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 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. Agencies certification and accreditation processes must conform to NIST guidance. Additionally, the flexibility described does not dilute the statutory requirement that all systems must be reviewed annually.

E. Continuity of system operations

FISMA (section 3544(b)(8)) codifies a longstanding policy requirement that each agency's security program (and particularly each system security plan) include the provision for the continuity of operations for information systems that support the operations and assets of the agency. FISMA explicitly includes in this requirement, information and information systems "provided or managed by another agency, contractor, or other source." For the purposes of agency implementation, "other source" has the same meaning as "other organization on behalf of an agency" discussed above.

F. NIST Standards and Guidelines

FISMA (sections 302 and 303) directs the Department of Commerce through NIST to develop, subject to direction by the President and in coordination with OMB, compulsory and binding standards that will be used to "categorize all information and information systems collected or maintained by or on behalf of each agency".

As NIST develops these minimum requirements for standards and guidelines, agencies will have ample opportunity to review drafts and provide feedback and comments. OMB strongly encourages agencies to actively review and participate in these drafts. As these standards and guidelines are finalized OMB will issue, when necessary, accompanying implementing guidance for the NIST standards and guidelines.

G. Senior Agency Information Security Officer Responsibilities

FISMA (section 3544(a)(3)(A)(i-iv)) provides additional details on the responsibilities and qualifications of the senior agency information security officer. All agencies shall have a senior information security officer, designated by the agency CIO, who reports to the agency CIO. Commonly referred to as a chief information security officer this officer must: (1) carry out the CIO's IT security responsibilities; (2) possess professional qualifications, including training and experience, required to administer FISMA requirements; (3) have information security duties as that official's primary duty; and (4) head an office with the mission and resources to assist in ensuring agency compliance with FISMA.

H. Reporting of Significant Deficiencies

FISMA (section 3544(c)) provides additional detail regarding the reporting of significant deficiencies. Specifically, FISMA requires agencies to "report any significant deficiency in a policy, procedure, or practice identified [in agency reporting] – (A) as a material weakness in reporting under section 3512 of title 31; and (B) if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note)." Accordingly, agency heads must consider such significant deficiencies when providing assurance on controls under the Federal Managers Financial Integrity Act (FMFIA) and determining compliance with the Federal Financial Management Improvement Act (FFMIA).

I. Inventory of Major Information Systems

FISMA (section 305(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.

The FISMA amendments requires that the identification of information systems in this inventory include an identification of the interfaces between each system and all other systems and networks, including those not operated by or under the control of the agency. It is OMB's expectation that each agency should have such an inventory via its work on developing its enterprise architecture. The FISMA amendments also provide that 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.

ATTACHMENT B

REPORTING ON FEDERAL GOVERNMENT INFORMATION SECURITY MANAGEMENT

Attachment B consists of two parts:

- Part I – which provides reporting instructions and the format for developing the agency and IG reports.
- Part II – which provides a series of 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 FY03 FISMA reviews remain nearly identical to the FY02 instructions. Agencies are not requested to collect any new type of information. The two significant changes are an increased emphasis on performance measures and additional guidance to IGs to assess whether agencies have an agency-wide remediation process that meets OMB criteria.

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 weaknesses1 reflected in their POA&Ms, and the results of IGs independent evaluations. Additionally, the agency head shall send copies of complete IG independent evaluations. This report shall be based on work conducted during the FY03 reporting period only.

For national security programs and systems, FISMA includes the same program and review requirements as for non-national security programs and systems, but limits OMB's role to one of management and budget oversight. Thus, agency reporting to OMB in this area should be limited to providing within the report a separate section describing how the agency is implementing the requirements of FISMA for national security programs and systems.

The program description should include whether or 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 Attachment 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, nor should they be sent to OMB.

1 Unless specified as a material weakness, the term weakness refers to any and all IT security weaknesses. When the guidance refers to material weakness, the term material weakness will be used.

The agency report shall consist of two separate components. One is to be prepared by the IG2, 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.

These reports continue to be the primary basis of OMB's summary report to Congress. As such, please note that reporting performance against the provided measures is not optional. All agencies shall respond to each of the performance measures in the format provided. Agencies must provide empirical data in their report at a level of detail appropriate to support OMB's executive level review. The best illustration of this level of detail is that customarily found in IG and General Accounting Office (GAO) audit reports. Including many volumes of agency policies and instructions is not appropriate for an executive level review.

The report, consisting of both the IG and agency components, shall be submitted in the spreadsheet format provided. Annual reports under FISMA must now 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 any time following their submission to OMB.

Each agency head shall submit their report (both agency and IG components), and copies of the IG independent evaluations to OMB on September 22, 2003. Please note that this information should be sent to OMB following the directions in the cover memorandum to which these reporting instructions are attached.

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

Specific Instructions for the Agency Report

Responses to the questions below must be in the format provided. To assist agencies and oversight authorities in distinguishing between weak and strong performing agency components, each question below requires two responses, unless otherwise specified, an agency total and a breakdown by major agency component or bureau.

A. Overview of FISMA IT Security Reviews

In this section, the agency must respond to performance measures and may provide narrative responses where appropriate.

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

A.1. Identify the agency's total IT security spending and each individual major operating division or bureau's IT security spending as found in the agency's FY03 budget enacted. This should include critical infrastructure protection costs that apply to the protection of government operations and assets. Do not include funding for critical infrastructure protection pertaining to lead agency responsibilities such as outreach to industry and the public.	
Bureau Name	**FY03 IT Security Spending ($ in thousnds)**
Agency Total	

A.2a. Identify the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials and CIOs in FY03, the total number of contractor operations or facilities, and the number of contractor operations or facilities reviewed in FY03. Additionally, IGs shall also identify the total number of programs, systems, and contractor operations or facilities that they evaluated in FY03.						
	FY03 Programs		**FY03 Systems**		**FY03 Contractor Operations or Facilities**	
Bureau Name	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed
Agency Total						
b. For operations and assets under their control, have agency program officials and the agency CIO used appropriate methods (e.g., audits or inspections, agreed upon IT security requirements for contractor provided services or services provided by other agencies) to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy?	Yes			No		
c. If yes, what methods are used? If no, please explain why.						
d. Did the agency use the NIST self-assessment guide to conduct its reviews?	Yes			No		
e. If the agency did not use the NIST self-assessment guide and instead used an agency developed methodology, please confirm that all elements of the NIST guide were addressed in the agency methodology.	Yes			No		
f. Provide a brief update on the agency's work to develop an inventory of major IT systems.						

A.3. Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law in FY03. Identify the number of material weaknesses repeated from FY02, describe each material weakness, and indicate whether POA&Ms have been developed for all of the material weaknesses.				
	FY03 Material Weaknesses			
Bureau Name	Total Number	Total Number Repeated from FY02	Identify and Describe Each Material Weakness	POA&Ms developed? Y/N
Agency Total				

A.4. This question is for IGs only. Please assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone process that meets the criteria below. Where appropriate, please include additional explanation in the column next to each criteria.	Yes	No
Agency program officials develop, implement, and manage POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.		
Agency program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.		
Agency CIO develops, implements, and manages POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.		
The agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis.		
The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.		
System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11) to tie the justification for IT security funds to the budget process.		
Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms.		
The agency's POA&M process represents a prioritization of agency IT security weaknesses that ensures that significant IT security weaknesses are addressed in a timely manner and receive, where necessary, appropriate resources.		

B. Responsibilities of Agency Head

In this section, the agency must respond to performance measures and may provide narrative responses where appropriate to the following questions:

B.1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced?	
B.2. Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?	
B.3. How does the head of the agency ensure that the agency's information security plan is practiced throughout the life cycle of each agency system?	
B.4. During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system? Please describe.	
B.5. Has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., continuity of operations, and physical and operational security)? Please describe.	
B.6. Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?	

B.7. Identification of agency's critical operations and assets (both national critical operations and assets and mission critical) and the interdependencies and interrelationships of those operations and assets.				
a. Has the agency fully identified its national critical operations and assets?	Yes		No	
b. Has the agency fully identified the interdependencies and interrelationships of those nationally critical operations and assets?	Yes		No	
c. Has the agency fully identified its mission critical operations and assets?	Yes		No	
d. Has the agency fully identified the interdependencies and interrelationships of those mission critical operations and assets?	Yes		No	
e. If yes, describe the steps the agency has taken as a result of the review.				
f. If no, please explain why.				

B.8. How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities?				
a. Identify and describe the procedures for external reporting to law enforcement authorities and to the Federal Computer Incident Response Center (FedCIRC).				
b. Total number of agency components or bureaus.				
c. Number of agency components with incident handling and response capability.				
d. Number of agency components that report to FedCIRC.				
e. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?				
f. What is the required average time to report to the agency and FedCIRC following an incident?				
g. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?				
h. Is the agency a member of the Patch Authentication and Distribution Capability operated by FedCIRC?	Yes		No	
i. If yes, how many active users does the agency have for this service?				
j. Has the agency developed and complied with specific configuration requirements that meet their own needs?	Yes		No	
k. Do these configuration requirements address patching of security vulnerabilities?	Yes		No	

B.9. Identify by bureau, the number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported and those reported to FedCIRC or law enforcement.			
Bureau Name	Number of incidents reported	Number of incidents reported externally to FedCIRC	Number of incidents reported externally to law enforcement

C. Responsibilities of Agency Program Officials and Agency Chief Information Officers

In this section, the agency must respond to performance measures and may provide narrative responses where appropriate to identify and describe the performance of agency program officials and the agency CIO in fulfilling their IT security responsibilities.

C.1. Have agency program officials and the agency CIO: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques? By each major agency component and aggregated into an agency total, identify actual performance in FY03 according to the measures and in the format provided below for the number and percentage of total systems.

a. Bureau Name	b. Total Number of Systems	c. Number of systems assessed for risk and assigned a level or risk		d. Number of systems that have an up-to-date IT security plan		e. Number of systems certified and accredited		f. Number of systems with security control costs integrated into the life cycle of the system		g. Number of systems for which security controls have been tested and evaluated in the last year		h. Number of systems with a contingency plan		i. Number of systems for which contingency plans have been tested	
		No. of Systems	% of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total															

C.2. Identify whether the agency CIO has adequately maintained an agency-wide IT security program and ensured the effective implementation of the program and evaluated the performance of major agency components.

Has the agency CIO maintained an agency-wide IT security program? Y/N	Did the CIO evaluate the performance of all agency bureaus/components? Y/N	How does the agency CIO ensure that bureaus comply with the agency-wide IT security program?	Has the agency CIO appointed a senior agency information security officer per the requirements in FISMA?	Do agency POA&Ms account for all known agency security weaknesses including all components?

C.3. Has the agency CIO ensured security training and awareness of all agency employees, including contractors and those employees with significant IT security responsibilities?

Total number of agency employees in FY03	Agency employees that received IT security training in FY03		Total number of agency employees with significant IT security responsibilities	Agency employees with significant security responsibilities that received specialized training		Briefly describe training provided	Total costs for providing training in FY03
	Number	Percentage		Number	Percentage		

C.4. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were IT security requirements and costs reported on every FY05 business case (as well as in the exhibit 53) submitted by the agency to OMB?

Bureau Name	Number of business cases submitted to OMB in FY05	Did the agency program official plan and budget for IT security and integrate security into all of their business cases? Y/N	Did the agency CIO plan and budget for IT security and integrate security into all of their business cases? Y/N	Are IT security costs reported in the agency's exhibit 53 for each IT investment? Y/N

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

A. Guidance for CIOs and Agency Program Officials

CIOs working with program officials must respond to all the questions in Part I. Responses must follow the prescribed format and should be based on the results of the annual system and program reviews, the agency's work in correcting weaknesses identified in their POA&Ms3, and any other work performed throughout the reporting period. Incomplete reporting against the provided performance measures will make the entire report incomplete and unacceptable.

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. Such reviews are not adequate without a review of all systems supporting such programs. 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

3 Agency POA&Ms must reflect all 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.

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 performance measures must agencies use?
OMB has provided performance measures for a number of the questions. Some of the questions have specific management performance measures against which agencies (including major components) must measure their actual level of performance. In many cases, completing the performance measures is an adequate response to the question. However, agencies may provide a narrative response, if necessary, in addition to the numerical response to the performance measures. The OMB provided performance measures represent a minimum required response and must be completed. If an agency has developed additional performance measures, they may be reported as well.

What reporting is required for national security programs and systems?
FISMA requires that all programs, including national security programs, be reviewed every year. Reporting to OMB in this area should be limited to describing within the report how the agency is implementing the requirements of FISMA for national security programs and systems. The program description should include whether or 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.

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 constitutes a significant deficiency?
OMB interprets a significant deficiency to include failure to meet FISMA's delineated requirements for an agency security program including the failure to substantially comply with related policies, guidance, and standards (e.g., this implementing guidance, OMB reporting guidance, OMB policy circulars and memoranda, and NIST guidelines and standards).

In the IT security program context, a significant deficiency would include the failure to perform adequate annual program and system reviews, failure to maintain comprehensive POA&Ms, and failure to adequately train agency employees and contractors.

In the context of individual systems, OMB Circular A-130 Appendix III provides three specific examples of a significant deficiency, each of which must be reported as such – the failure to assign responsibility for security of the system or application, the lack of system security plan, and the absence of authorization to process (certification and accreditation). Depending on the level of risk and magnitude of harm to the system, other weaknesses may also rise to the level of a significant deficiency.

B. Guidance for 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 including a review of 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. FISMA also permits IGs to use the results of any other review in performing their work which occurred during the FY03 reporting period.

IGs should respond to all questions in Part I with the exception of question A.1. IGs should use the performance measures to assist in evaluating agency officials' performance. IG responses should be based on the results of the independent evaluations, including agency progress in implementing and maintaining their POA&Ms, and any other work performed throughout the reporting period (e.g., financial statement audits).

Additionally, IGs are asked this year to assess against specific criteria whether the agency has developed, implemented, and is managing an agency-wide POA&M process. The IG's assessment in this area is critical. 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 agency's ability to get to green under the Expanding E-Government Scorecard of the President's Management Agenda. Agencies must meet three criteria to get to green for security under the E-Gov scorecard, one of which is the positive assessment by their IG that an agency-wide POA&M process has been implemented.

<u>Should IGs audit an agency's IT security program</u>?
Within the context of FISMA an audit is not contemplated. FISMA directs IGs or their designee, to perform an annual independent evaluation. 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.

Should IGs review the agency CIO/program official report to OMB to develop their independent evaluation?
Not as the exclusive input for their review, no. Neither FISMA nor OMB guidance requires such a review nor does such a review constitute meeting FISMA's requirements for IGs. Inasmuch as IGs, CIOs, and program officials should work together throughout the year to ensure the development and maintenance of a comprehensive POA&M and collaborate on preparing the report to OMB, a separate review of the CIO/program officials' report should not be necessary. 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 nor should any such IG review 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 for those systems they evaluate.

ATTACHMENT C

Attachment C consists of three parts:

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

I. Updated Guidance on Quarterly Reporting – Agency Plans of Action and Milestones and Performance Measures

A. Agency POA&Ms

OMB policy requires agencies to prepare and submit 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 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.
3. Be shared with the agency IG to ensure independent verification and validation.
4. Follow the format detailed in the examples under Part II of this attachment.
5. Be submitted twice a year to OMB (October 1, 2003 and March 15, 2004).

Quarterly Updates on POA&M Implementation

Agencies must provide on a quarterly basis in the table format below an update on their IT security remediation efforts. The first FY03 quarterly update is due on October 1, 2003. Remaining quarterly updates are due on December 15, 2003, March 15, 2004, and June 15, 2004. The quarterly updates must be reported in the format below.

Quarterly POA&M Updated Information	Programs	Systems
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 complete 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.).		

Assisting Congressional Oversight

OMB's guidance to agencies on their POA&Ms was designed to: 1) first and foremost be a management tool to assist agencies in closing their security performance gaps; 2) secondly, assist IGs in their evaluation work of agency security performance; and 3) lastly, 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 FY03 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 these quarterly updates have also been requested by the House Government Reform's Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census. Agencies shall send their updates to the Subcommittee after review and notification by OMB.

B. Quarterly Reporting on Performance Measures

Beginning with the December 15, 2003, quarterly update, agencies will also provide a quarterly update on their performance against a subset of the performance measures in OMB reporting instructions. This update should be submitted with the quarterly POA&M updates and must follow the format below.

Quarterly IT Security Performance Measures Update																
Bureau Name	Total Number of Systems	Number of systems assessed for risk and assigned a level or risk		Number of systems that have an up-to-date IT security plan		Number of systems certified and accredited		Number of systems with security control costs integrated into the life cycle of the system		Number of systems for which security controls have been tested and evaluated in the last year		Number of systems with a contingency plan		Number of systems for which contingency plans have been tested	
		No. of Systems	% of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Agency Total															

C. Quarterly IT Security Reporting and the President's Management Agenda Scorecard

Both the POA&Ms and IT security performance measures quarterly updates enable the agency and OMB to monitor agency remediation efforts to more accurately identify progress and problems. Additionally, these updates are also 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.

To get to green for the IT security component of the E-Gov Scorecard agencies must:

- Demonstrate consistent progress in remediating IT security weaknesses through their POA&Ms;
- Have IG verify that there is a Department-wide IT security POA&M process; and
- Have 90% of operational IT systems properly secured (e.g., certified and accredited), including mission-critical systems.

To get to yellow for the IT security component of the E-Gov Scorecard agencies must:

- Demonstrate consistent progress in remediating IT security weaknesses through their POA&M updates and either:
  - Have IG verify that there is a Department-wide IT security POA&M process; **OR**
  - Have 80% of operational IT systems properly secured (e.g., certified and accredited).

In the instance where an IG finds through their FY03 FISMA evaluation that the agency does not have an agency-wide IT security POA&M process that meets OMB criteria, OMB will work with the agency and IG to ensure that after the agency has addressed the weaknesses identified by the IG, a 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.

II. POA&M Instructions

The following instructions explain how the POA&M should be completed. 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.[4]

Column 1 -- Type of weakness. Describe weaknesses 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).

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 -- Milestone changes. 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

[4]OMB Circular A-11 requires that agencies develop and submit to OMB business cases (exhibit 300) for major IT projects. Additionally, each agency submits an exhibit 53, a list of both major and non-major IT systems. The agency assigns a unique identifier to each system and includes it with these exhibits.

audit, etc.) of the weakness. Weaknesses that have been identified as a material weakness, significant deficiency, or other reportable condition in the latest agency Inspector General audit under other applicable law (e.g., financial system audit under the Financial Management Integrity Act, etc). If yes is reported, also identify and cite the language from the pertinent audit report.

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-- No program-level security program/plan	Program office and agency CIO	None	3/1/02	Draft plan prepared and circulated for user input -- 11/30/01		Yes--5/17/01 report	Ongoing
				Comments reviewed, final draft to Administrator for approval and publication -- 3/1/02			
2 -- No documented program to report external security incidents to law enforcement and GSA	Program office and agency CIO	None	10/31/01	Consult with agency IG, FBI/NIPC, and GSA - 10/15/01			Completed
				Procedures published, employees trained 10/30/01			
3 -- No documentation for data sensitivity levels -- thus cannot document acceptable risk and security needs	Program office and agency CIO	$25K	1/30/02	Review enterprise architecture (process and data layers) to define and categorize data type and sensitivity -- 12/1/01			Ongoing
				Identify acceptable risk for each level, identify protection needs, document, publish, and implement -- 1/30/02			
4 -- Security not integrated w/capital planning. Not shown in exhibits 300 & 53	Agency CIO	Estimated $15K	1/30/02	Review and update all program exhibits 300 & 53			Ongoing

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 -- Password controls improperly configured and not tested	Program office	None	10/1/01	Reconfigure and test password controls -- 10/1/01		Yes	Completed
2 -- Security plan is out of date, more than one year since last update despite new interconnections	Program office	None	11/30/01	Update plan and obtain independent review -- 11/30/01		No	Ongoing
3 -- No written management authorization prior to system operations	Program office & Agency CIO	None	12/30/01	Complete certification and accreditation procedures per up-to-date security plan and NIST guidance. Obtain written auth -- 12/15/01		Yes	Ongoing
4 -- System is contractor operated and contract does not include FAR security and privacy clause nor are contractor practices evaluated by agency	Program office, contracting officer, and agency CIO	None	1/30/02	Identify specific security requirements, including for contractor personnel, and revise contract accordingly -- 1/30/02		No	Ongoing
5 -- System vulnerabilities have not been periodically tested as specified in OMB policy and Security Act	Program office and agency CIO	$50K	1/15/02	Arrange for system vulnerability testing -- 10/15/01		Yes	Ongoing
				Identify from test report, additional required security controls -- 11/15/01			
				Implement and test new security controls and schedule retest -- 1/15/02			
6 -- Life cycle system costs not incorporated into system funding	Program office and agency CIO	None	10/30/01	Identify costs. Update Exh. 300 & 53. Reallocate funds from lower system priorities -- 10/30/01			

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

What is a POA&M?
A plan of action and milestones (POA&M) 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 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.

How many POA&Ms should an agency prepare?
An agency should develop a separate POA&M for every program and system for which weaknesses5 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.

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 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[6] (exhibit 300) was submitted or was a part of the exhibit 53, the

5 The term weakness refers to any and all weaknesses, not just material weaknesses.
[6]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

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.

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. We have made special arrangements with the Department of Defense and could adapt that procedure for the use of other agencies in reporting on national security systems.

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 may 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 may be emailed to OMB 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;

---

to OMB. Agencies assign a unique identifier to each system and apply it to the exhibit 300 and 53.

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.

ATTACHMENT D

Definitions of Key Words Referenced in OMB Guidance

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.

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 Information System (defined in OMB Circular A-11, section 300)
A 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. Large infrastructure investments (e.g., major purchases of personal computers or local area network improvements) should also be evaluated against these criteria. Your agency Capital Planning and Investment Control Process may also define a "major system or project." All major systems or projects must be reported on exhibit 53. In addition, a "major" IT system is one reported on your "Capital Asset Plan and Business Case," exhibit 300. For the financial management mission area, "major" is any system that costs more than $500,000. Additionally, if the project or initiative directly supports the President's Management Agenda Items, then the project meets the criteria of "high executive visibility". Projects that are E-Government in nature or use e-business technologies must be identified as major projects regardless of the costs. If you are unsure about what systems to consider as "major," consult your agency budget officer or OMB representative. Systems not considered "major" are "small/other."

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.

IT Security Costs (defined in FY05 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 Inspector General. 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.