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

July 2, 2002

M-02-09

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Mitchell E. Daniels, Jr.
Director

SUBJECT: Reporting Instructions for the Government Information Security Reform Act and Updated Guidance on Security Plans of Action and Milestones

The President has given a high priority to the security of the Federal government's operations and assets. Protecting the information and information systems on which the Federal government depends, requires agencies to identify and resolve current security weaknesses and risks, as well as protect against future vulnerabilities and threats. Fulfilling the requirements of the Government Information Security Reform Act of 2000 (Security Act) is the key method for meeting this priority.

Background

Last year's efforts in implementing the Security Act resulted in a detailed understanding of the Federal government's information and information technology (IT) security status. As a result of agencies' work, we now have a valuable baseline of security performance, ultimately allowing us to track progress in securing the Federal government's operations and information assets. Per the requirements of the Security Act, OMB summarized agency reports in a report sent to Congress in February, www.whitehouse.gov/omb/inforeg/fy01securityactreport.pdf.

Last year OMB issued memorandum 01-24, guidance on reporting the results of agencies' annual security reviews and evaluations. OMB also issued memorandum 02-01, guidance for security plans of action and milestones to assist agencies in closing security performance gaps identified in their reviews. Based on lessons learned from last year's reporting, along with input from agency officials, Inspectors General (IGs), and the General Accounting Office, this memorandum provides updated guidance.

New Reporting Guidance

While the reporting requirements remain largely the same, high-level management performance measures have been added to the reporting instructions. Additionally, the

attachments address specific areas where agencies requested additional guidance. This new guidance combines and therefore replaces the earlier memoranda.

This guidance has a three part focus on: 1) agency progress in remediating the security weaknesses identified in FY01; 2) the results of FY02 agency reviews and IG evaluations; and 3) specific performance measures for agency officials accountable for information and IT security. OMB's FY02 report to Congress will be based largely on the information agencies report according to these three areas. It will also measure progress against the performance baseline established in last year's security report.

To ensure that agencies' work is optimized, OMB has taken steps to incorporate their work into the budget process. Agency corrective action plans link a system with a security weakness to the budget justification for that system. This link gives the agency and OMB a system's level of security performance against the funding request for that system. This information will help to improve and prioritize budget decisions.

Additionally, OMB is evaluating agency information and information security in the President's Management Agenda Scorecard under the electronic government score. Agencies' corrective action plans and quarterly updates on progress implementing their plans will be the basis for OMB's assessment of agencies' information and IT security for the Scorecard. Agencies will be assessed on the basis of progress at both the Department level and by major operating divisions or bureaus. This step will further reinforce the roles and responsibilities of agency program officials (bureau or division heads) for the security of systems that support their programs and the agency Chief Information Officer (CIO) for the security of their systems and the agency-wide security program. It will also increase accountability and improve the security of the agency's operations and assets.

Please find enclosed with this memorandum the following: 1) Attachment A, updated reporting instructions; 2) Attachment B, updated guidance on developing, submitting, and maintaining security corrective action plans; and 3) Attachment C, a list of common definitions referenced in the OMB guidance.

Instructions for Reporting

Agency Security Act reports are due to OMB on September 16th, 2002. Agency heads should transmit to OMB: 1) the executive summary, developed by the agency CIO, agency program officials, and the IG that is based on the results of their work; 2) copies of the IG's independent evaluations; and 3) for national security systems, audits of the independent evaluations. Your CIO and IG will receive an electronic copy of this guidance and templates to assist them in reporting. Agency executive summaries will serve as the primary basis for OMB's summary report to Congress.

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

Mitchell E. Daniels, Jr.
OMB Director
Eisenhower Executive Office Building
Room 252
Washington, DC 20503

The executive summaries along with copies of the independent evaluations and any other appropriate information should be sent electronically in Microsoft Word or Word Perfect to Kamela White at kgwhite@omb.eop.gov. Instructions for submitting the security corrective action plans can be found in Attachment B.

Attachments

## ATTACHMENT A

### REPORTING ON FEDERAL GOVERNMENT INFORMATION SECURITY REFORM

## I. Reporting Instructions for the Executive Summary

For non-national security programs, each agency head shall transmit to the OMB Director an executive summary that reports the results of annual security reviews of systems and programs, agency progress on correcting weaknesses[1] reflected in their plans of action and milestones (POA&Ms) or corrective action plans, and the results of Inspectors' General (IGs) independent evaluations. Additionally, the agency head shall send copies of complete IG independent evaluations.

For national security programs and systems, the Government Information Security Reform Act (Security Act) 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 describing within the executive summary how the agency is implementing the requirements of the Security Act 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 and the number of audits performed of those evaluations. Additionally, as the Security Act directs, the agency head must transmit to OMB copies of the audits of independent evaluations. Agencies must also develop POA&Ms (see Attachment B) 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.

Like last year, the executive summary shall consist of two separate components. One is to be prepared by the IG, characterizing the results of their independent evaluations and agency progress in implementing their POA&Ms. The other component is to be prepared by the Chief Information Officer (CIO), working with program officials, reflecting the results of their annual system and program reviews and progress in implementing their POA&Ms.

Additionally, this year the agency and IG shall report on agency officials' performance against a set of high-level management measures provided in the reporting instructions. As with last year, the executive summaries will be the primary basis of OMB's summary report to Congress. Agencies must provide empirical data in their executive summary 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

[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.

Office (GAO) audit reports. Including many volumes of agency regulations and instructions is not appropriate for an executive level review.

The executive summary, consisting of both the IG and CIO components, should not exceed 30 pages. After they have been submitted to OMB, the agency's executive summary should be made available to Congress upon request. OMB will include the performance measures information in its report to Congress. OMB requests that IGs submit their evaluations to the agency and OMB before making them public and sending to Congress.

Last year, several agencies and their IGs did not report on particularly significant security weaknesses that already had been reported in the media or were of such significance that such media attention was likely. The Security Act and OMB guidance clearly require agencies to annually review all systems and report findings. It is important that such gaps not exist in annual reports or at other times throughout the year.

Each agency head shall submit their executive summary, copies of the IG independent evaluations, and copies of the audits of independent evaluations on national security systems to OMB on September 16, 2002. Please note that this information should be sent to OMB under separate cover from the agency's budget materials following the directions in the cover memorandum to which these reporting instructions are attached.

Part III of this attachment provides additional information, in the form of Q&As, to agencies to assist them in implementing the Security Act's and OMB's requirements.

## II. Specific Instructions for Executive Summaries

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, all responses to the questions below must be organized by major agency component (e.g., operating division, bureau, or service where specified). Thereafter, the agency should aggregate the findings into an overall agency finding.

For the FY01 reporting, OMB directed agency program officials and CIOs to identify the performance measures they use and the actual level of performance against those measures. Agency IGs were requested to evaluate only the actual level of performance. For this year's reporting, OMB has provided high-level management performance measures at agencies' requests. In addition to providing responses to each question below, some questions also require program officials, CIOs, and IGs to respond to those performance measures. As with last year's reporting guidance, agency program officials, CIOs, and IGs are to provide an actual level of performance against these measures.

### A. General Overview

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

1. Identify the agency's total security funding as found in the agency's FY02 budget request, FY02 budget enacted, and the President's FY03 budget. This should include a breakdown of security costs by each major operating division or bureau and include critical infrastructure protection costs that apply to the protection of government operations and assets.[2] Do not include funding for critical infrastructure protection pertaining to lead agency responsibilities such as outreach to industry and the public[3].

2. Identify and describe as necessary the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials, CIOs, or IGs in both last year's report (FY01) and this year's report (FY02) according to the format provided below. Agencies should specify whether they used the NIST self-assessment guide or an agency developed methodology. If the latter was used, confirm that all elements of the NIST guide were addressed.

---

[2]Agencies should report security costs that agree with those reported on their FY02 and FY03 Exhibit 53s. If security costs detailed in an agency's Exhibit 53 were incomplete or inaccurate, corrected security costs should be reported, and differences with the final FY02 Exhibit 53 noted and with their FY03.

[3]The following agencies have lead agency responsibilities pertaining to critical infrastructure protection: Commerce, Treasury, EPA, Transportation, FEMA, HHS, Energy, Justice, State, DOD, and CIA.

| | FY01 | FY02 |
|---|---|---|
| a. Total number of agency programs. | | |
| b. Total number of agency systems. | | |
| c. Total number of programs reviewed. | | |
| d. Total number of systems reviewed. | | |

3. Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law. (Section 3534(c)(1)-(2) of the Security Act.) Identify the number of reported material weaknesses for FY 01 and FY 02, and the number of repeat weaknesses in FY02.

| | FY01 | FY02 |
|---|---|---|
| a. Number of material weaknesses reported. | | |
| b. Number of material weaknesses repeated in FY02. | | |

B. Responsibilities of Agency Head

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

1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth the Security Act's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced? Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?

2. 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? (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act.) 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?

3. How 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)? (Sections 3534 (a)(1)(B) and (b)(1) of the Security Act.) 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?

4. Has the agency undergone a Project Matrix[4] review? If so, describe the steps the agency has taken as a result of the review. If no, describe how the agency identifies its critical operations and assets, their interdependencies and interrelationships, and how they secure those operations and assets. (Sections 3535(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act.)

5. 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? Identify and describe the procedures for external reporting to law enforcement authorities and to the General Services Administration's Federal Computer Incident Response Center (FedCIRC). Identify actual performance according to the measures and the number of incidents reported in the format provided below. (Section 3534(b)(2)(F)(i)-(iii) of the Security Act.)

| | |
|---|---|
| a. Total number of agency components including bureaus, field activities. | |
| b. Number of agency components with incident handling and response capability. | |
| c. Number of agency components that report to FedCIRC. | |
| d. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance? | |
| e. What is the required average time to report to the agency and FedCIRC following an incident? | |
| f. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner? | |

| | FY01 | FY02 |
|---|---|---|
| g. By agency and individual component, 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 by each component | | |
| h. By agency and individual component, number of incidents reported externally to FedCIRC or law enforcement. | | |

[4] Project Matrix is a program developed by the Department of Commerce's Critical Infrastructure Assurance Office (CIAO) to identify and characterize accurately the assets and associated infrastructure dependencies and interdependencies that the U.S. Government requires to fulfill its most critical responsibilities to the nation. OMB directed most large agencies to undergo a Project Matrix review.

C. Responsibilities of Agency Program Officials

In this section, the agency must respond to performance measures and provide narrative responses where appropriate to identify and describe the performance of agency program officials in fulfilling their security responsibilities. In responding to the performance measures, include the number of systems reviewed, the total number of systems, and the resulting percentage (e.g., 98/102, 96%).

1. Have agency program officials: 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? (Section 3534(a)(2) of the Security Act.)

| COMPONENT OR BUREAU NAME | TOTAL NUMBER OF SYSTEMS |
|---|---|

| TOTAL NUMBER OF AGENCY SYSTEMS | |
|---|---|

By each major agency component and aggregated into an agency total, from last year's report (FY01) and this reporting period (FY02) identify actual performance according to the measures and in the format provided below for the number and percentage of total systems.

| COMPONENT OR BUREAU NAME | | | | |
|---|---|---|---|---|
| | FY01 # | FY01 % | FY02 # | FY02 % |
| a. Systems that have been assessed for risk. | | | | |
| b. Systems that have been assigned a level of risk after a risk assessment has been conducted (e.g., high, medium, or basic). | | | | |
| c. Systems that have an up-to-date security plan. | | | | |
| d. Systems that have been authorized for processing following certification and accreditation. | | | | |
| e. Systems that are operating without written authorization (including the absence of certification and accreditation). | | | | |
| f. Systems that have the costs of their security controls integrated into the life cycle of the system. | | | | |
| g. Systems for which security controls have been tested and evaluated in the last year. | | | | |

| | | | | |
|---|---|---|---|---|
| h. Systems that have a contingency plan. | | | | |
| i. Systems for which contingency plans that have been tested in past year. | | | | |
| **AGENCY TOTAL** | | | | |

2. For operations and assets under their control, have agency program officials used appropriate methods (e.g., audits or inspections) to ensure that contractor provided services (e.g., network or website operations) or services provided by another agency for their program and systems are adequately secure and meet the requirements of the Security Act, OMB policy and NIST guidance, national security policy, and agency policy? Identify actual performance according to the measures and in the format provided below. (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Security Act.)

| **COMPONENT OR BUREAU NAME** | | |
|---|---|---|
| | FY01 | FY02 |
| a. Number of contractor operations or facilities. | | |
| b. Number of contractor operations or facilities reviewed. | | |

D. Responsibilities of Agency Chief Information Officers

In this section, the agency must respond to performance measures and provide narrative responses where appropriate to identify and describe the performance of agency CIOs in fulfilling their security responsibilities. For each category, include the number of systems reviewed, the total number of systems, and the resulting percentage (e.g., 98/102, 96%).

1. Has the agency CIO: 1) adequately maintained an agency-wide security program; 2) ensured the effective implementation of the program and evaluated the performance of major agency components; and 3) ensured the training of agency employees with significant security responsibilities? Identify actual performance according to the measures and in the format provided below. (Section 3534(a)(3)-(5)) and (Section 3534(a)(3)(D), (a)(4), (b)(2)(C)(i)-(ii) of the Security Act.)

| | FY01 | FY02 |
|---|---|---|
| a. Other than GAO or IG audits and reviews, how many agency components and field activities received security reviews? | | |
| b. What percentage of components and field activities have had such reviews? | | |
| c. Number of agency employees including contractors. | | |
| d. Number and percentage of agency employees including contractors that received security training. | | |
| e. Number of employees with significant security responsibilities. | | |

| | | |
|---|---|---|
| f. Number of employees with significant security responsibilities that received specialized training. | | |
| g. Briefly describe what types of security training were available. | | |
| h. Total costs for providing training described in (g). | | |

| | |
|---|---|
| i. Do agency POA&Ms account for all known agency security weaknesses including of all components and field activities? If no, why not? | |
| j. Has the CIO appointed a senior agency information security official? | |

2. For operations and assets under their control (e.g., network operations), has the agency CIO used appropriate methods (e.g., audits or inspections) to ensure that contractor provided services (e.g., network or website operations) or services provided by another agency are adequately secure and meet the requirements of the Security Act, OMB policy and NIST guidance, national security policy, and agency policy? Identify actual performance according to the measures and in the format provided below. (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Security Act.)

| | FY01 | FY02 |
|---|---|---|
| a. Number of contractor operations or facilities. | | |
| b. Number of contractor operations or facilities reviewed. | | |

3. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were security requirements and costs reported on every FY03 capital asset plan (as well as in the exhibit 53) submitted by the agency to OMB? If no, why not? Identify actual performance according to the measures and in the format provided below. (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act.)

| | FY03 Budget Materials | FY04 Budget Materials |
|---|---|---|
| a. Number of capital asset plans and justifications submitted to OMB? | | |
| b. Number of capital asset plans and justifications submitted to OMB without requisite security information and costs? | | |
| c. Were security costs reported for all agency systems on the agency's exhibit 53? | | |
| d. Have all discrepancies been corrected? | | |
| e. How many have the CIO/other appropriate official independently validated prior to submittal to OMB? | | |

## III. 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 II. 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&Ms, and any other work performed throughout the reporting period.[5] Incomplete reporting against the provided performance measures will make the entire report incomplete and unacceptable.

In this year's report to Congress, will OMB include information on agency plans to correct weaknesses as well as identifying the weakness itself?
Yes, this year, when OMB determines that a specific agency or component weakness should be highlighted in its report to Congress, OMB will also include the agency's planned corrective action, provided such weakness and specific planned action are explicitly and completely reflected in the agency narrative and POA&M. Like last year, OMB's reporting of security weaknesses will be at a high level and will not include sensitive or pre-decisional budget related data.

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. The Security Act requires that senior agency program officials review each program for effectiveness at least annually. The purpose of the security programs discussed in the

[5] Agency POA&Ms must reflect all known security weaknesses within an agency including it's 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. OMB has emphasized this point in security program meetings with each agency.

Security Act 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. OMB's FY01 reporting guidance also required a review of all systems.

What level of review is required for an individual system?
Agencies are reminded that section 3534(b)(3) of the Security Act requires annual program reviews by program officials and CIOs. 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 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?
Last year, agencies were encouraged to use the National Institute of Standards and Technology (NIST) self-assessment guide to review their systems. Most agencies used this guide, but because it was not completed until well into the FY01 reporting period, OMB did not require its use. This guide was finalized by NIST in November 2001 as Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems." This year, agencies must use the NIST guide unless they and the IG confirm in their narrative responses to question 2, 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. Last year, most agencies did not provide performance measures or actual levels of performance where asked to do so and requested that OMB develop such measures. 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 also provide a narrative response 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?
The Security Act 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 executive summary how the agency is implementing the requirements of the Security Act 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 and the number of audits performed of those evaluations.

Additionally, the Security Act directs that the agency head transmit to OMB copies of the audits of independent evaluations. An audit of an independent evaluation of a national security system must validate that the evaluation conformed to national security policies and procedures. For OMB's purposes, an audit that validates the use of the NIST self-assessment guide to assess a particular national security system is sufficient, provided that national security policy authorities haven't imposed more stringent requirements on such system evaluations.

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.

**B. Guidance for Agency Inspectors General**

The Security Act 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, the Security Act 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 Security Act also permits IGs to use the results of any other review in performing their work. The intent of the system subset and other review provisions of the Security Act was to recognize that IGs are not equipped to review everything each year.

IGs should respond to all questions in Part II 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 year (e.g., financial statement audits and work by GAO).

Should IGs audit an agency's security program?
Within the context of the Security Act an audit is not contemplated. The Security Act directs IGs or their designee, to perform an annual independent evaluation. By requiring an evaluation but not an audit, the Security Act 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 the IG's report include a review of the agency plan of action and milestones?
Yes, OMB requests that IGs verify that agency POA&Ms identify all known security weaknesses within an agency, including components, and are used by the IG and the agency, major components and program officials within them, as the authoritative agency management mechanism to prioritize, track, and manage all agency efforts to close security performance gaps. OMB has emphasized this point in security program meetings with each agency.

What should IGs review for national security programs and systems?
For national security systems, IGs should audit independent evaluations and provide copies to OMB. An audit of an independent evaluation of a national security system must validate that the evaluation conformed to national security policies and procedures. For OMB's purposes, an audit that validates the use of the NIST self-assessment guide to assess a particular national security system is sufficient, provided that national security policy authorities haven't imposed more stringent requirements on such system evaluations. Additionally, the Security Act directs that the agency head transmit to OMB copies of the audits of independent evaluations.

To the extent that the information within independent evaluations and audits permit, IGs should also respond to all questions with the exception of question A(1). Any work on the agency POA&M for national security programs and systems may also be used. OMB's interest lies solely in obtaining an objective, executive level description of the agency's management and internal oversight of national security programs and systems. To assist oversight by appropriate national security authorities, it is important to specify where practicable which portion of the IG findings pertains to national security programs and systems. Copies of audits of the independent evaluations of national security programs and systems must be sent to OMB with the agency's report.

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. Last year there was some confusion as to whether IGs were required to review the annual CIO and program official review prior to agency reporting to OMB. While some IGs did review the CIO/program officials' reviews, neither the Security Act nor OMB guidance requires such a review nor does such a review constitute meeting the Security Act'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 the Security Act 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.

**ATTACHMENT B**

## I. Updated Guidance on Agency Plans of Action and Milestones

Last year OMB issued memorandum 02-01, "Guidance for Preparing and Submitting Security Plans of Action and Milestones" which directed agencies to prepare and submit plans of action and milestones (POA&Ms) for all programs and systems where a security weakness has been found. The guidance directs Chief Information Officers (CIOs) to develop, implement, and manage corrective action plans for all programs and systems they operate and control. Agency program officials are to develop, implement, and manage corrective action plans for 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 provide the agency's quarterly update to OMB. This guidance updates and replaces M-02-01.

Agencies' corrective action plans 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 Inspector General (IG) to ensure independent verification and validation.

Agencies' corrective action plans are due to OMB October 1, 2002.

Additionally, based largely on agency feedback and their work developing and implementing their plans, this updated guidance provides additional instructions to agencies in the following areas:

1. FY02 POA&M Submission
   Agencies must follow the format detailed in the examples under Part II in developing their POA&Ms. Additionally, agencies must briefly describe the process the agency has developed to ensure that plans are implemented, work is tracked, and progress is reported.

2. Quarterly Updates on POA&M Implementation
   Agencies must report on a quarterly basis the following information for agency programs and agency systems:
   a) total number of weaknesses identified at a program level and a system level;
   b) the number of weaknesses for which corrective action was completed on time (including testing) at a program level and a system level;

c) the number of weaknesses for which corrective action is ongoing and is on track to complete as originally scheduled at a program level and a system level;
d) the number of weaknesses for which corrective action has been delayed including a brief explanation for the delay at a program level and a system level; and
e) the number of new weaknesses discovered following the last POA&M or status update and a brief description of how they were identified.

3. Assisting Congressional Oversight

OMB's guidance to agencies last year 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 OMB policy, predecisional budget related information is not released. However, Congress has an important oversight role in this area and OMB has addressed this issue in the guidance below to enable agencies to release information from their corrective action plans while preserving pre-decisional negotiations between OMB and Federal agencies.

## 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, 5, 6, and 7. The heading of each POA&M must include the unique project identifier from the exhibits 300 and 53, where applicable.[6]

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 9, "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 7, "Changes to Milestones."

Column 6 -- Milestone changes. This column would include new completion dates for the particular milestone. See example.

---

[6] 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 projects must be reported to OMB on an exhibit 300 and 53. The agency assigns a unique identifier to each project and applies it to both exhibits.

Column 7 -- The agency should identify the source (e.g., program review, IG audit, GAO 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 Security POA&Ms

What is a POA&M?
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.

When is the POA&M due?
The first POA&M is due to OMB on October 1st, 2002. Thereafter, brief status updates must be submitted on a quarterly basis. The first quarterly update is due to OMB on January 1, 2003. Agencies will submit their updated plans again at the April quarterly update to inform the mid-year review.

Based upon OMB's judgement of the maturity of an agency's program of development and use of POA&Ms, some agencies will not need to submit all of their POA&Ms. OMB will communicate individually to those agencies with a mature POA&M program through the CIO and OMB will inform the IG. A mature POA&M program must clearly demonstrate that: 1) the POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses; 2) POA&Ms are developed and managed by the program official responsible for the program and systems; 3) agency IGs are an integral part of the POA&M process; and 4) the CIO manages a central process to monitor program officials work and receive updates on progress which enables them to inform senior agency policy officials and OMB of the agency's security status.

For those agencies with a mature POA&M program they may submit the following: 1) all program level POA&Ms; 2) all POA&Ms for their major[7] IT investments; and 3) a representative sampling, from each bureau, of the remaining systems. Of course, for all agencies, OMB may request a POA&M for a specific system or program at any time.

How many POA&Ms should an agency prepare?
An agency should develop a separate POA&M for every program and system for which weaknesses[8] were identified in the Security Act 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,

[7] A major IT investment is a system or program that requires a capital asset plan and justification as defined in OMB Circular A-11 on preparing and submitting budget materials.
[8] The term weakness refers to any and all weaknesses, not just material weaknesses.

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 continues to take steps to integrate 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[9] (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.

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 the Security Act, reporting weaknesses in national security systems as well as certain systems under the control of the Department of Defense and Intelligence Community is being

[9]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 projects must be reported to OMB. Agencies assign a unique identifier to each project and apply it to the exhibit 300 and 53.

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.

What format should be used for the quarterly status updates?
Agency CIOs must report to OMB on a quarterly basis the following information for agency programs and agency systems: 1) total number of weaknesses identified at a program level and a system level; 2) the number of weaknesses for which corrective action was completed on time (including testing) at a program level and a system level; 3) the number of weaknesses for which corrective action is ongoing and is on track to complete as originally scheduled at a program level and a system level; 4) the number of weaknesses for which corrective action has been delayed including a brief explanation for the delay at a program level and a system level; and 5) the number of new weaknesses discovered following the last POA&M or status update and a brief description of how they were identified. The first quarterly update is due to OMB on January 1, 2003.

Quarterly updates may be emailed to OMB by the agency CIO. When sending their quarterly updates, please include the agency name and the word POA&M. Updates should be emailed to Kamela White, kgwhite@omb.eop.gov.

What is OMB doing with agency POA&Ms and the quarterly updates?
As mentioned earlier, OMB, working with the agencies, will use the POA&Ms to inform budget decisions. Additionally, OMB will use the plans and quarterly updates to assist in oversight responsibilities. Finally, agency plans and updates will be the basis for OMB's assessment of agency's IT security status as part of the President's Management Agenda Scorecard under the e-gov score.

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 OMB policy, OMB and the agencies have a

responsibility to maintain the confidentiality of "deliberative information," that led to the President's budget decisions.

However, Congress clearly has an important 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 while preserving pre-decisional negotiations between OMB and Federal agencies.

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 C**

**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.

Agencywide Information Security Program (defined in the Government Information Security Reform Act of 2000, section 3534 (b)(1))

Each agency is required to develop and implement an agencywide information security program. This program must provide information security for the operations and assets of the agency, including operations and assets provided or managed by another agency.

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 Technology (defined by the Clinger Cohen Act of 1196, 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.

National Security System

For security purposes, the definition of national security systems has the following two parts:

1. (defined under section 5142 of the Clinger Cohen Act of 1996)

> "National security system" means any telecommunications or information system operated by the United States Government, the function, operation, or use of which –
> (1) involves intelligence activities
> (2) involves cryptologic activities related to national security;
> (3) involves command and control of military forces;
> (4) involves equipment that is an integral part of a weapon or weapons system; or subject to subsection (b), is critical to the direct fulfillment of military or intelligence missions.
>
> (b) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

2. (defined under section 3532 of the Government Information Security Reform Act of 2000)

> b)(2)(B) a national security system is protected at all times by procedures established for information which has been specifically authorized under criteria established by an Executive order or an Act of Congress to be classified in the interest of national defense or foreign policy;

Thus national security systems are those systems listed in Clinger-Cohen (whether or not they process classified national security information) and any system that does process classified national security information (whether or not it is listed in Clinger-Cohen).

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 and the Government Information Security Reform Act of 2000, section 3534 (b)(2)(A-F))

A program review, in the context of the work required under the Government Information Security Reform Act, 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.

Project Matrix (defined by CIAO, www.ciao.gov/federal/index.html)

CIAO developed " Project Matrix," a program designed to identify and characterize accurately the assets and associated infrastructure dependencies and interdependencies that the U.S. Government requires to fulfill its most critical responsibilities to the nation. These are deemed "critical" because their incapacitation could jeopardize the nation's security, seriously disrupt the functioning of the national economy, or adversely affect the health or safety of large segments of the American public.

Project Matrix involves a three-step process in which each civilian Federal department and agency identifies (1) its critical assets; (2) other Federal government assets, systems, and networks on which those critical assets depend to operate; and (3) all associated dependencies on privately owned and operated critical infrastructures.

Security Costs (defined in FY04 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 much 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 the National Institute of Standards and Technology (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 the Office of Management and Budget, 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.