October 17, 2001

M-02-01

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Mitchell E. Daniels, Jr.
Director

SUBJECT: Guidance for Preparing and Submitting Security Plans of Action and Milestones

On June 22, 2001, I issued a memorandum on "Reporting Instructions for the Government Information Security Reform Act" (OMB M-01-24). In the memorandum, OMB asked each agency to submit, with its September budget request, a set of program reviews and evaluations of both unclassified and classified systems, along with an executive summary. In addition, OMB asked each agency to submit to OMB by October 31, 2001, (with brief quarterly updates thereafter) "a plan of action with milestones" to address all weaknesses identified by program reviews and evaluations.

In response to the June 22nd memorandum, several agencies have asked OMB to issue more detailed guidance that further describes, and provides a standard format for, the information that agencies should include in their plans of action and milestones (POA&M). Working with representatives of agency program offices and Inspector General offices, OMB has developed the attached POA&M guidance, which provides specific instructions and examples for the POA&Ms. The first POA&M is due by October 31st, but please notify us if you will need more time. At a minimum, POA&Ms must address the reporting elements found in the attached guidance. Agency Chief Information Officers, working with program officials, budget officers, Inspectors General, and other appropriate agency officials, are responsible for developing a POA&M for each program and system for which a weakness was identified during the annual program review and independent evaluations required by the Government Information Security Reform Act.

Additionally, 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. Thus, the submission of these POA&Ms includes, but does not necessarily replace, all security remediation plans that an agency might have. By reflecting the enterprise security needs of an agency, a consolidated POA&M provides a roadmap for continuous agency security improvement, assists with prioritizing corrective action and resource allocation, and is a valuable management and oversight tool for agency officials, Inspectors General, and OMB.

The attachments provide specific instructions and examples for the POA&Ms.

POA&Ms should be sent to:

Office of Management and Budget
New Executive Office Building, Rm 10236
725 17th St, NW
Washington, DC 20503

Questions and comments should be directed to Kamela White at kgwhite@omb.eop.gov or 202-395-3630.

Preparing and Submitting Security Plans of Action and Milestones

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 this 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 31, 2001. Please notify Kamela White in OMB to request more time based on agency need. Thereafter, brief status updates must be submitted on a quarterly basis. The first quarterly update is due to OMB on January 31, 2002.

How many POA&Ms should an agency prepare?

An agency should develop a separate POA&M for every program and system for which weaknesses 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, including GAO audits, financial system audits, and critical infrastructure vulnerability assessments.

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 (1) 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 (2) (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. Also, for each POA&M for which there is an associated capital asset plan, agencies must also provide the security costs reported on the Exhibit 53 (3).

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 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 should use the attached spreadsheet-type format for the initial 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.

Because the information in these plans will likely be sensitive, agencies should submit POA&Ms to

OMB on diskette as a Microsoft Excel spreadsheet. Please notify Kamela White in OMB if you would like to use a different submission mechanism.

What format should be used for the quarterly status updates?

OMB is not prescribing a specific format for the status updates only that the agency CIO provide the following information: 1) The total number of weaknesses identified on the original POA&Ms; 2) the number of weaknesses for which corrective action was completed on time (including testing); 3) the number of weaknesses for which corrective action is ongoing and is on track to complete as originally scheduled; 4) the number of weaknesses for which corrective action has been delayed including a brief explanation for the delay; 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.

What level of detail and sensitivity should the POA&Ms include?

Sensitive 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 General Accounting Office and Inspectors General 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 sensitive data, the POA&M should note the fact of its special sensitivity.

What security precautions is OMB taking to adequately protect the POA&Ms?

Aggregated unclassified POA&Ms in electronic form will be maintained on a stand alone desktop PC with password controlled access. Access to aggregated data will be available to the appropriate OMB employees.

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 should 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 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.

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	Minimal	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	Minimal	1/30/02	Review and update all program exhibits 300 & 53			Ongoing

Sample 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	Program office, contracting	None	1/30/02	Identify specific security requirements, including for		No	Ongoing

security and privacy clause nor are contractor practices evaluated by agency	officer, and agency CIO			contractor personnel, and revise contract accordingly -- 1/30/02			
5 -- System vulnerabilities have not been periodically tested as specified in OMB policy and Security Act	Program office and agency CIO	Moderate	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			

[1] Please see OMB M-01-24 of June 22, 2001, "Reporting Instructions for the Government Information Security Reform Act."

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

[3] OMB Circular A-11 requires that agencies report via an exhibit 53, an estimated percentage of the total investment for associated IT security costs.

[4] 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 both major and significant 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.