June 22, 2001

M-01-24

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Mitchell E. Daniels, Jr.
Director

SUBJECT: Reporting Instructions for the Government Information Security Reform Act

The Government Information Security Reform Act (Security Act), passed last year as part of the FY 2001 Defense Authorization Act (P.L. 106-398), amended the Paperwork Reduction Act of 1995 (PRA) by adding a new subchapter on information security. The Security Act focuses on the program management, implementation, and evaluation aspects of the security of unclassified and national security systems. Generally, the Security Act codifies existing OMB security policies, Circular A-130, Appendix III, and reiterates security responsibilities outlined in the Computer Security Act of 1987, the PRA, and the Clinger-Cohen Act of 1996. In addition, the Security Act requires annual agency program reviews and annual independent evaluations for both unclassified and national security programs.

On January 16, 2001, OMB issued memorandum 01-08, guidance to agencies on implementing the Security Act. The guidance directs agency heads to transmit to OMB in September, contemporaneous with their FY 2003 budget materials, copies of the annual agency program reviews, independent evaluations, and for national security systems, audits of the independent evaluations. In addition to the program reviews and evaluations, agency heads should also provide a brief executive summary, not to exceed 15 pages, developed by the agency Chief Information Officer, agency program officials, and the Inspector General that is based on the results of their work. These executive summaries will serve as the primary basis for OMB's summary report to Congress. Instructions for completing the executive summary are detailed in the attachment.

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

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

The program reviews, independent evaluations, and executive summaries along with any other appropriate information should be sent electronically in Microsoft Word or Word Perfect to Kamela White at kgwhite@omb.eop.gov.

Attachment

Reporting on the Government Information Security Reform Act

OMB Memorandum, 01-08, "Guidance on Implementing the Government Information Security Reform Act", directs agencies to provide to OMB the following information: 1) copies of annual program reviews; 2) copies of independent evaluations; and 3) for national security systems, copies of audits of the independent evaluations. Additionally, the OMB guidance referenced follow-on instructions to be issued to agencies on reporting the results of the program reviews and independent evaluations in an executive summary. The reporting instructions below provide a consistent form and format for agencies to report back to OMB. Each topic in the reporting instructions relates to a specific agency responsibility outlined in the Security Act or OMB Circular A-11.

I. Reporting Instructions for the Executive Summary

For non-national security programs, each agency head shall transmit to the OMB Director the results of an annual security review that includes: 1) an executive summary on how the agency is implementing the requirements of the Security Act and 2) copies of the annual program reviews[1] and independent evaluations. For national security programs, the agency head shall transmit to the OMB Director an annual report that includes: 1) an executive summary on how the agency is implementing the requirements of the Security Act and 2) the audits of independent evaluations of national security systems.

The executive summary shall consist of two separate components, one prepared by the Inspector General (IG) characterizing the results of the independent evaluation and the other prepared by the Chief Information Officer (CIO), working with program officials, that is based on the results of the annual program reviews. These summaries will be the primary basis of OMB's summary report to Congress. The executive summary, consisting of both the IG and CIO components, should not exceed 15 pages.

Each agency shall submit their executive summary and additional required materials to OMB September 10th when their budget submission is due. Please note that this information should be sent to OMB under separate cover from the agency's budget materials according to the directions in the memorandum attached to these reporting instructions.

---

[1]Agencies should provide sufficient documentation for each of the reporting areas that supports the findings and assessments in their annual program reviews as reported in the executive summary. They should not submit copies of actual program reviews. For example, for system reviews (which are essential elements of each program review), the submission should include the number and types of systems in place for that program, the number of systems tested, and the specific types of tests conducted to determine whether appropriate management, operational, and technical controls were in place and functioning properly. The submission should include a characterization of problems found (e.g., types of vulnerabilities), but specific problems should not be associated with any specific system.

A. Instructions for Agency CIOs and Program Officials

CIOs working with program officials should respond to the 14 topics listed below. All responses should be based on the results of the annual program reviews. Unless otherwise noted, all responses to the statements below should be organized by major agency component, e.g. operating division or bureau, and be separated into each of the 13 topic areas. Please note that most of the topic areas below require that the agency first describe how it measures performance[2] for the requirements of the Security Act and second describe the actual level of performance based on the results of the annual program reviews.

Topic 14 requires the agency to develop a plan of action with milestones to correct any security weaknesses identified by the annual program reviews and independent evaluations. This plan is due to OMB by October 31, 2001. Additional instructions on the plan of action will be issued by OMB this summer.

B. Instructions for Agency IGs

The Security Act directs IGs or their designee, to perform annual independent evaluations of the information security program and practices of the agency. OMB requests that IGs respond to topics 2-13. All responses should be based on the results of the independent evaluations. IGs are not required to describe or evaluate how an agency measures performance with respect to its annual program reviews or evaluate the review itself. Instead, IG responses should focus on the actual performance of the agency's security program and practices. For national security systems, IGs should respond to topics 2-13 as appropriate based on the information in the audits of the independent evaluations.

II. Specific Questions

A. General Overview

In this section, the agency shall provide the following information:

1. Identify the agency's total security funding as found in the agency's FY01 budget request, FY01 budget enacted, and the FY02 budget request. 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

[2] In this context, performance measures are not those required by the Government Performance and Results Act. However, agencies, in consultation with the CIO, should begin incorporating into their performance plans (as required under section 1115 of title 31) this summer a description of the time periods and the resources, to include budget, staffing and training, that are necessary to implement an agencywide information security program. (Section 3534(d)(1)-(2) of the Security Act).

operations and assets.[3] Do not include funding for critical infrastructure protection pertaining to lead agency responsibilities such as outreach to industry and the public[4].

2. Identify the total number of programs included in the program reviews or independent evaluations.

3. Describe the methodology used in the program reviews and the methodology used in the independent evaluations.

4. Report any 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).

B. Security Program Performance

In this section, the agency shall succinctly describe:

5. The specific measures of performance used by the agency to ensure that agency program officials have: 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. Include information on the actual performance for each of the four categories. (Section 3534(a)(2) of the Security Act).

6. The specific measures of performance used by the agency to ensure that the agency CIO: 1) adequately maintains an agency-wide security program; 2) ensures the effective implementation of the program and evaluates the performance of major agency components; and 3) ensures the training of agency employees with significant security responsibilities. Include information on the actual performance for each of the three categories. (Section 3534(a)(3)-(5) of the Security Act).

7. How the agency ensures that employees are sufficiently trained in their security responsibilities. Identify the total number of agency employees and briefly describe what types of security training was available during the reporting period, the number of agency employees that received each type of training, and the total costs of providing such training. (Section 3534(a)(3)(D), (a)(4), (b)(2)(C)(i)-(ii) of the Security Act).

---

[3]Agencies should report security costs which agree with those reported on their FY02 Exhibit 53. 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.

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

8. The agency's documented procedures for reporting security incidents and sharing information regarding common vulnerabilities. Include a description of procedures for external reporting to law enforcement authorities and to the General Services Administration's FedCIRC. Include information on the actual performance and the number of incidents reported. (Section 3534(b)(2)(F)(i)-(iii) of the Security Act).

9. How the agency integrates security into its capital planning and investment control process. Were security requirements and costs reported on every FY02 capital asset plan (as well as exhibit 53) submitted by the agency to OMB? If no, why not? (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act).

10. The specific methodology (e.g., Project Matrix review) used by the agency to identify, prioritize, and protect critical assets within its enterprise architecture, including links with key external systems. Describe how the methodology has been implemented. (Sections 3535(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act).

11. The measures of performance used by the head of the agency to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system. Include information on the actual performance. (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act).

12. How the agency has integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., physical and operational). (Sections 3534 (a)(1)(B) and (b)(1) of the Security Act).

13. The specific methods (e.g., audits or inspections) used by the agency 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. (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Security Act).

C. Next Steps

14. Each agency head, working with the CIO and program officials, must provide the following information to OMB by October 31, 2001. Provide a strategy to correct security weaknesses identified through the annual program reviews, independent evaluations, other reviews or audits performed throughout the reporting period, and uncompleted actions identified prior to the reporting period. Include a plan of action with milestones that include completion dates that: 1) describes how the agency plans to address any issues/weaknesses; and 2) identifies obstacles to address known weaknesses.