Federal Communications Commission
Office of Inspector General

Report on Government Information Security Reform Act Evaluation - Findings and Recommendations

Report No. 01-AUD-11-43
November 29, 2001

Executive Summary

The Government Information Security Reform Act (Security Act), passed as part of the FY 2001 Defense Authorization Act (P.L. 106-398), focuses on the program management, implementation, and evaluation aspects of agency security systems. A key provision of the Security Act requires that the Inspector General (IG) perform an annual independent evaluation of the information security program of the Federal Communications Commission (FCC). The Security Act also permits the IG to select an independent evaluator to perform this evaluation. The IG contracted with KPMG, LLP to perform the independent evaluation.

The objective of this independent evaluation was to examine the Commission's security program and practices. The examination included testing the effectiveness of security controls for an appropriate subset of the Commission's applications. As part of the examination, we selected the Consolidated Database System (CDBS) application for review. CDBS is a major application operated by the Commission's Mass Media Bureau (MMB). We also used the Security Act assessment tool to evaluate the effectiveness of the Commission's information security program and assess risk for each component of the program.

On September 5, 2001, we issued a report, entitled "FY 2001 Government Information Security Reform Act Evaluation," summarizing the results of our independent evaluation. On September 10, 2001, our report, comprised of an executive summary and an independent evaluation, was included in a package of information provided by the Commission to the Office of Management and Budget (OMB). As a result of the independent evaluation, we concluded that the Commission has a generally effective information security program with acceptable practices for managing and safeguarding the Federal Communications Commission's (FCC's) information technology assets.

The purpose of this report is to communicate these findings and recommendations to FCC management. A byproduct of our Security Act evaluation, this report details the findings and provides recommendations that, when implemented, will strengthen the Commission's information security program.

During the independent evaluation, we identified areas for improvement in the Commission's information security program. Specifically, we identified sixteen (16) findings in the areas of management, operational, and technical controls. Three (3) of the findings were determined to be high-risk[1] and thirteen (13) were determined to be medium risk. We recommend that the problems we identified be corrected to strengthen the agency's security program and practices. Our recommendations will correct present problems and minimize the risk that future security problems will occur.

[1] Each finding was evaluated to determine its degree of exposure based on the following risk ratings. **High:** Security risk can cause a business disruption, if exploited. **Medium:** Security risk in conjunction with other events can cause a business disruption, if exploited. **Low:** Security risk may cause operational annoyances, if exploited.

On October 10, 2001, we issued a draft report summarizing the results of our audit. In that draft document, we requested that the Office of the Managing Director (OMD) and the Mass Media Bureau (MMB) respond to the findings and recommendations presented in our report.

In a response dated November 9, 2001, OMD indicated concurrence with each with each of the findings and recommendations. OMD also attached a Program-Level Plan of Action and Milestones, prepared by the Information Technology Center, which resolves each finding and recommendation and identifies corrective action that has been or will be taken. We have included a copy of the response from ITC in its entirety as Appendix C to this report.

In a response dated November 19, 2001, MMB agreed with each with the findings and recommendations. We have included a copy of the response from MMB in its entirety as Appendix D to this report.

Because of the sensitive nature of the information contained in the appendices, we have marked them all "Non-Public – For Internal Use Only" and have limited distribution. Those persons receiving this report are requested not to photocopy or otherwise distribute this material.

Background

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 Office of Management and Budget (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.

A key provision of the Security Act requires that the Inspector General (IG) perform an annual independent evaluation of the information security program of the Federal Communications Commission (FCC). The Security Act also permits the IG to select an independent evaluator to perform this evaluation. The IG contracted with KPMG, LLP to perform the independent evaluation as required by the Security Act.

The purpose of this review was to perform the independent evaluation of FCC's information security program and practices to ensure proper management and security for the information resources supporting the agency's operations and assets as required by the act.

To perform this independent evaluation, we followed the guidance as described in OMB Memorandum M-01-08, entitled "Guidance on Implementing the Government Information Security Reform Act" and dated January 16, 2001. Also relevant to this evaluation was guidance from OMB Memorandum M-01-24, entitled "Reporting on the Government Information Security Reform Act" and dated June 22, 2001. OMB M-01-24 provided the topics/questions that were required to be addressed in the IG's independent evaluation of the FCC's information security program and practices.

The independent evaluation, which includes the responses to topics/questions 2 through 13, was issued as an OIG report on September 5, 2001. This document transmits the specific findings that were developed during the independent evaluation.

Evaluation Objective

The objective of the independent evaluation was to examine the Commission's security program and practices. The examination included testing the effectiveness of security controls for an appropriate subset of the Commission's systems. The evaluation objective also included a review of the Commission's security policies, security architecture, business continuity, security capital planning, critical infrastructure, and security program planning and management.

This review was part of the Government Information Security Reform Act (Security Act) effort. The Security Act required the Inspector General (IG) to perform an annual independent evaluation of the information security program of the Federal Communications Commission (FCC). The IG contracted with KPMG, LLP to perform the independent evaluation. This report transmits the findings that were developed during the Security Act evaluation.

The specific objectives of the evaluation were to:

- Obtain an understanding of the Commission's Information Technology (IT) infrastructure;

- Obtain an understanding of the Commission's information security program and practices;

- Use the Security Act assessment tool to evaluate the effectiveness of the Commission's information security program and assess risk for each component of the program. At a minimum, the assessment should include an identification and ranking of the critical information security threats to the FCC IT infrastructure on a risk vulnerability basis; and

- Prepare the annual submission in accordance with the reporting requirements mandated under the Security Act for Fiscal Year 2001. This was completed as a separate review on September 5, 2001.

- Provide a detailed report that will (1) identify and rank the critical security risk factors and (2) contain observations and recommendations for improvements, if any.

Evaluation Scope

The evaluation approach consisted of reviewing documentation that included previous special reviews and audits, by conducting interviews, attending meetings, and by observations.

Our procedures were designed to comply with applicable auditing standards and guidelines. These included AICPA Professional Standards, Generally Accepted Government Auditing Standards (GAGAS) as well as GAO's Federal Information Systems Control Audit Methodology (FISCAM); however, this review was intended to be a risk assessment and not a general controls review; FISCAM was used as appropriate to assess management, operational and technical controls.

The scope of the evaluation included the security infrastructure managed by the Office of Managing Director's Information Technology Center (ITC) and the Auctions Automation Branch of the Wireless Telecommunications Bureau (WTB). In addition, the scope included selecting an appropriate subset of the Commission's business applications. As part of our evaluation of the FCC's Computer Security Program, we selected the Consolidated Database System (CDBS) application for review. CDBS is a major application operated by the Commission's Mass Media Bureau.

The evaluation methodology used was the NIST Self-Assessment Guide questionnaire (National Institute of Standards and Technology Systems (NIST) Self-Assessment Guide for Information Technology Systems). The final NIST Self-Assessment Guide was not available until September, 2001, therefore, the draft Self-Assessment Guide was used.

Our observations are organized according to NIST control areas: management controls, operational controls, technical controls. Within each control area, specific control objectives are addressed.

Management Controls - Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management. The specific management control objectives addressed are:

- Risk Management
- Review of Security Controls
- Life Cycle
- Authorize Processing (Certification & Accreditation)
- System Security Plan

Operational Controls - The operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems).

These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls. The specific operational control objectives addressed are:

- Personnel Security
- Physical and Environmental Protection
- Production, Input/Output Controls
- Contingency Planning
- Hardware and System Software Maintenance
- Data Integrity
- Documentation
- Security Awareness, Training and Education
- Incident Response Capability

Technical Controls - Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The specific technical control objectives addressed are:

- Identification and Authentication
- Audit Trails
- Logical Access Controls

Observations

Our review found that the FCC has a generally effective information security program with acceptable practices for managing and safeguarding the FCC's information technology assets.

Although the Commission has implemented numerous controls, we identified sixteen (16) findings that impact the effectiveness of the Commission's program. These findings occurred in the areas of management, operational, and technical controls. We recommend that the problems we identified be corrected to strengthen the agency's security program and practices. Our recommendations will correct present problems and minimize the risk that future security problems will occur.

Appendix A of the report, entitled Summary of Findings, provides a summary of the findings from this review and Appendix B, entitled Detailed Findings and Recommendations, provides detailed information on the conditions identified, criteria used to evaluate the condition, effect, and recommendation(s).

On October 10, 2001, we issued a draft report summarizing the results of our audit. In that draft document, we requested that the Office of the Managing Director (OMD) and the Mass Media Bureau (MMB) respond to the findings and recommendations presented in our report.

In a response dated November 9, 2001, OMD indicated concurrence with each with each of the findings and recommendations. OMD also attached a Program-Level Plan of Action and Milestones, prepared by the Information Technology Center, which resolves each finding and recommendation and identifies corrective action that has been or will be taken. We have included a copy of the response from ITC in its entirety as Appendix C to this report.

MMB also responded to these findings. In a response dated November 19, 2001, MMB indicated concurrence with each with each of the findings and recommendations. We have included a copy of the response from MMB in its entirety as Appendix D to this report.

In accordance with the Commission's directive on the management of non-public information, we have classified all appendices as "Non-Public – For Internal Use Only." Those persons receiving this report are expected to follow the established policies and procedures for managing and safeguarding this report in accordance with Commission directive.