OFFICE OF INSPECTOR GENERAL

MEMORANDUM

DATE: September 5, 2001

TO: Chairman

FROM: Inspector General

SUBJECT: Government Information Security Reform Act Report

The Office of Inspector General (OIG) has completed an evaluation of the Commission's Information Security program in accordance with the Government Information Security Reform Act (Security Act). The Security Act requires that Inspectors General, or independent evaluators they choose, perform an annual evaluation of each agency's information security program and practices. I have attached a copy of out report, entitled FY 2001 Government Information Security Reform Act Evaluation," summarizing the results of our evaluation of the Commission's Information Security program.

In accordance with guidelines published by the Office of Management and Budget (OMB), the OIG report consists of two sections: (1) an executive summary, and (2) the independent evaluation. The executive summary section provides a brief background of the Security Act and the purpose of the evaluation, evaluation objectives and scope, and the results of the evaluation. The independent evaluation section provides a brief summary of the evaluation and provides OIG responses to specific questions required by OMB reporting instructions[1]. Our report has been developed for incorporation into one document with the Security Act report produced by the Chief Information Officer (CIO). This combined report is required to be submitted to OMB by September 10, 2001.

As a result of the independent evaluation, we have 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

[1] Office of Management and Budget (OMB) Memorandum for the Heads of Executive Department and Agencies (Memorandum No. M-01-24) entitled "Reporting Instructions for the Government Information Security Reform Act" and dated June 22, 2001.

assets. However, during the evaluation, we identified areas for improvement in the FCC's information security management, operational and technical controls. We are addressing these issues with FCC management in a separate Special Review Report.

If you have any questions, please contact me at (202) 418-0476.

H. Walker Feaster III

Attachment

cc: Chief of Staff
Managing Director
Chief Information Officer
AMD-PERM

Federal Communications Commission
Office of Inspector General

FY 2001 Government Information Security Reform Act Evaluation

September 5, 2001

Prepared by KPMG, LLP

EXECUTIVE SUMMARY

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 quite 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 – 13, is attached

The fundamental mission of the Federal Communications Commission (FCC) is to implement the Communications Act of 1934, as amended, in a manner that promotes competition, innovation, and deregulation in the communications industry and the availability of high quality communications services for all Americans. In order to achieve these objectives, the Commission must strive to stay on the cutting edge of changes in technology, economics and law.

As stated in the Commission's FY 2002 Budget Estimate to Congress, the advent of Internet-based and other new technology driven communications services will continue to erode the traditional regulatory distinctions between different sectors of the communications industry. The FCC recognizes that their most immediate challenge is to integrate the changing character of the industry into its core functions of 1) licensing; 2) consumer protection; 3) enforcement; 4) promotion of competitive markets; and 5) spectrum management.

In the past few years, the FCC has streamlined its licensing procedures and implemented electronic filing capability in 78 services, 72% of all licensing systems. At the end of Fiscal Year 2000, 62% of all license applications were filed electronically. Additionally, 93% of all applications were acted on within the FCC's speed of disposal goals. Implementation of these electronic licensing systems has led to improved processing time and to a significant decrease in the number of backlogged applications.

In Fiscal Year 2000, the FCC made its website more accessible to their Internet users. The FCC received 320 million "hits," making the FCC one of the most popular government online sites. The FCC's consumer information centers received more than 789,000 consumer inquiries on such hot topics as cramming, slamming and spamming.

To this end, supporting specific information technology initiatives requires an effective information security program that will safeguard FCC's computer-based assets from technological vulnerabilities, or from disruption of services. To support today's information technology infrastructure, effective management, operational and technical controls are essential. The FCC's method of implementing the requirements of the Security Act is focused on ensuring that programs and policies are in compliance with OMB A-130 requirements and in association with National Institute of Standards and Technology (NIST).

Evaluation Objective

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 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. 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 security 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. In addition to preparing the annual submission, 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, 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

Results of the Independent Evaluation

As a result of the independent evaluation, we have concluded that the Commission has a generally effective information security program with acceptable practices for managing and safeguarding the FCC's information technology assets.

During the evaluation, we identified in-place controls in key areas such as a current computer security program policy. An update to the current policy is already in circulation for approval and it is planned that this policy will replace the current policy by November 2001. The revised computer security program policy, which is in draft, is indicative of how proactive the FCC is with keeping pace with technological challenges, changes, demands, and innovations.

The FCC is diligent about synchronizing their procedures with OMB A-130 guidance. The security plan templates that have been created for general support systems and major applications are designed in accordance with NIST guidance for developing security plans. The FCC has begun development of their security plans; however, an area for improvement is to complete the security plans for all of the major applications.

On a monthly basis, the Computer Security Officer conducts Security Awareness Training for all new users who are granted access to the FCC Network general support system. Also in place is a recently developed system development life cycle methodology that was developed jointly with the Information Technology Center (ITC) and the Office of Inspector General (OIG).

An initiative demonstrated by the ITC was a site visit to J.P. Morgan/Chase Bank prior to allowing the processing of FCC data. The ITC group made an unannounced visit to the J.P. Morgan office in New York to review the effectiveness of the bank's security posture. The visit proved successful and authorization for J.P. Morgan to handle processing for the FCC was awarded.

Last year, the FCC conducted numerous computer security assessments. The assessments identified potential risks and provided countermeasures and safeguards to mitigate the risks identified. In addition, a risk assessment of the FCC Net and Auctions LAN general support systems was conducted.

Although the FCC has several controls in place, areas for improvement in the management, operational and technical control areas exist. To strengthen the agency's security program and practices, a strategy and plan of action as prescribed by OMB M-01-24, Reporting Instructions for the Government Information Security Reform Act, topic/question #14, should be developed with milestones that include completion dates, how the agency plans to address control areas that need to be strengthened as identified through the independent evaluation, and should identify a strategy to overcome any obstacles that would affect addressing known weaknesses.

Independent Evaluation of the FCC's Information Security Program

The Government Information Security Reform Act (Security Act) was passed last year as part of the FY 2001 Defense Authorization Act (P.L. 106-398). The Security Act focuses on the program management, implementation, and evaluation aspects of the security of agency computer systems. 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. An important provision of the Security Act requires 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 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.

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 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

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 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, therefore, the draft Self-Assessment Guide was used.

The Office of Management and Budget, Memorandum 01-24 (OMB M-01-24) provides the topics/questions for response by the Chief Information Officers (CIO) and Inspector Generals (OIG) of federal agencies. OMB-01-24 provides 14 questions that require response. OMB requests that OIG's respond to questions 2-13. All responses were based on the results of the OIG's independent evaluation.

The Commission's Office of Inspector General contracted for the professional services firm of KPMG, LLP to prepare the independent evaluation and respond to questions 2-13 as requested by OMB. KPMG's approach to responding to questions 2-13 was to perform an independent evaluation as required by the Government Information Security Reform Act. The evaluation methodology used was the National Institute of Standards and Technology (NIST) Self-Assessment Guide for Information Technology Systems questionnaire While performing the independent evaluation, numerous interviews were conducted and a number of documents provided by FCC were reviewed.

As a result of the independent evaluation, we have concluded that the Commission has a generally effective information security program with acceptable practices for managing and safeguarding the FCC's information technology assets. During the evaluation, we identified in-place controls in essential areas such as a current computer security program policy. An update to the current policy is already in circulation for approval and it is planned that this policy will replace the current policy by November 2001. The revised computer security program policy, which is in draft, is indicative of how proactive the FCC is with keeping pace with technological challenges, changes, demands, and innovations.

Although the FCC has several controls in place, areas for improvement in the management, operational and technical control areas exist. To strengthen the agency's security program and practices, a strategy and plan of action as prescribed by OMB M-01-24, Reporting Instructions for the Government Information Security Reform Act, topic/question #14, should be developed with milestones that include completion dates, how the agency plans to address control areas that need to be strengthened as identified through the independent evaluation, and should identify a strategy to overcome any obstacles that would affect addressing known weaknesses.

OIG Responses to OMB M-01-24 Security Act Reporting Topics/Questions

Question #1 - In this section, the agency shall provide the following information:

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

OIG response to Question #1 - This question is not applicable to the OIG per OMB reporting instructions.

Question #2 - Identify the total number of programs included in the program review or independent evaluations.

OIG response to Question #2 - In accordance with the guidelines contained in the OMB guidance, we selected an application from among the Commission's major applications for detailed review. Based on revenue generation, the Wireless Telecommunications Bureau (WTB) and the Mass Media Bureau head the list. Due to initiatives currently underway for WTB, we did not focus on WTB's major applications and general support system in the program review.

For the Fiscal Year 2001 review, the Mass Media Bureau (MMB) was selected. The MMB is second in revenue generation to WTB. MMB ensures that consumers have access to interference-free radio and television services that are in the public interests. To achieve this, MMB issues licenses for radio and television stations and establishes regulations to make certain that these stations serve their local communities through programming and advertising.

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. CDBS is the Mass Media Bureau's Internet based system that permits electronic filing of broadcast radio and television application forms with the FCC. The CDBS provides a Public Access System and an Electronic Filing System for internal use and external use.

CDBS is ranked high in the amount of revenue generated by the system as well as high in the OMB A-130 criteria of availability, integrity, and confidentiality. When appropriate, the FCC's general support system, FCC Net, is included in the program review as we moved through the assessment of control areas.

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

OIG response to Question #3 - The independent evaluation was performed using the draft version of the NIST Self-Assessment Guide. The independent evaluation consisted of reviewing Management Controls, Operational Controls and Technical Controls with the NIST Self-Assessment Guide framework. Within each control area, specific control objectives were addressed. A description of the NIST Self-Assessment Guide control areas is as follows:

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

Question #4 - Report any material weakness in policies, procedures, or practices as identified and required to be reported under existing law.

OIG response to Question #4 - The Commission's Fiscal Year 2000 Financial Statement audit, June 27, 2001, reported material weaknesses regarding information security policies, procedures or practices. The following deficiencies in security controls were reported:

- FCC is not in compliance with OMB Circular No. A-130 Requirement for a Comprehensive Security Plan (modified repeat condition from FY 1999's financial statement audit).

- FCC lacks a comprehensive and integrated security management structure. In such an environment, responsibilities could be unclear leading to the possibility of applying security controls inconsistently throughout the agency. As a result, certain vulnerabilities may be overlooked. In addition, monitoring the effectiveness of procedures for security controls throughout the agency will be ineffective.

- FCC has not performed risk assessments for its major application systems and its mission-critical general support system. FCC did perform vulnerability assessments for several of its major applications and general support systems in fiscal year 2000, but has not completed risk assessments as prescribed by OMB Circular No. A-123, Management Accountability and Control.

- There is no periodic review of security controls over FCC's systems. In addition, FCC has not performed any formal certification and accreditation of its systems. FCC plans to conduct initial security reviews over a two-year period ending in fiscal year 2002. FCC plans to make these reviews part of its internal control review process.

During the fiscal year 2001 independent evaluation for GISRA, an organizational pattern was observed with regards to management operating from draft policy guidelines. The policies that are in draft are significant in the area of information security:

- FCC Personnel Security/Suitability Manual (draft policy)
- Management of Non-Public Information, Form 1139 (draft policy)
- Physical Security (policy not available)
- Information Security Manual, Form 1131 (expired policy)
- IT Strategic Plan (draft)

Question #5 - Describe 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.

NOTE: Include information on the actual performance for each of the four categories.

OIG response to Question #5 - The Commission's "Strategic Plan: A New FCC for the 21St Century", August 1999, provides specific implementation plans for years 2000 – 2004. Section III, identifies specific policy initiatives and performance measures as a roadmap for the Commission to follow over the next five years and to measure progress toward the Commission's objectives. In 1999, the specific performance measures used by FCC to ensure that the Commission's strategic plan was carried out, consisted of identifying the performance measure, then measuring progress against two-year goals, five-year goals, or timeframes such as by year 2003.

The critical tasks that must be achieved in order to make progress include the following initiatives:

Create a Model Agency for the Digital Age

1) Lead the Way in the Information Age
2) Reorganize to Create an Agency Infrastructure Conducive to Convergence
3) Create a Faster, Flatter, More Functional Agency
4) Preserve and Increase the Wealth of Knowledge and Expertise of FCC Staff

Promote Competition in All Communication Markets

1) Eliminate Barriers to Entry in Domestic Markets
2) Deregulate As Competition Develops
3) Enforce the Rules so that Businesses Compete Fairly
4) Promote Competition in International Communications Markets

Promote Opportunities for All Americans to Benefit from the Communications Revolution

1) Ensure Access For All Americans To Existing And Future Communications Services
2) Promote Opportunities to Expand Direct Participation In Existing And Future Communications Businesses
3) Foster a More Consumer Friendly Marketplace

Manage The Electromagnetic Spectrum (the Nation's Airwaves) In The Public Interest

1) Create More Efficient Spectrum Markets
2) Increase the Amount of Spectrum Available, Particularly for New Services

(1) <u>Risk Assessments (assess the risk to operations and assets under their control)</u>

In evaluating FCC's assets, the Commission determines which of their business applications are considered major in accordance with guidance from OMB A-130, Appendix III. The FCC's Information Technology Center (ITC) uses evaluation worksheets as a tool to determine FCC's major applications. In the assessment, the ITC group uses the following categories to determine whether the applications should be categorized as major:

- **Importance (revenue)**
  Dollar amounts generated by the system, by the collection of regulatory and application fees, which is returned to the Federal government.
  (Low = $0-$500K; Moderate +>$500K - <$1M; High =>$1M)

- **System Investment**
  The dollar amount spent to date to develop and maintain the system, and any associated databases.
  (Low = $30 - $750K; Moderate = >$750K - <$2M; High = >$2M)

- **Administrative Significance**
  The impact of not having the system, or its associated data, available for use by the Bureau/Office or the FCC. *Important Note: Administrative Significance is a subjective ranking versus categories that are based on fixed costs.*

- **Risk/Harm**
  The amount of risk/harm that could be caused if the system, or its associated data, were compromised (i.e., the potential damage that might be caused by a person who gained unauthorized access to the data processed by a specific system. Risk/ Harm is a subjective ranking versus categories that are based on fixed costs.

Any application rated "HIGH" in any of the four categories noted above is considered a major application within the FCC infrastructure. However, the specific performance measures for assessing the risk to assets under the Commission's control needs to be identified and included in the agency's ITC Strategic Plan or the ITC Computer Security Strategic Plan.

In determining the risk to operations, the Commission currently has a statement of work in process to plan the development of a Continuity of Operations Plan (COOP). In addition, the majority of the Commission's business continuity plans represent Y2K as the triggered event and does not reflect the current operating environment. The specific measures of performance for COOP and BCP (Business Continuity Plan) programs need to be identified by the appropriate program officials.

The Commission has a draft IT Strategic Plan, however, to line up with the agency's overall strategic plan, performance measures need to be identified and included in the plan.

The actual performance of managing the risks associated with the operations and assets under the Commission's control could be enhanced by providing documented management approval of final risk determinations of systems under the system owner's control.

(2) <u>Appropriate level of security to protect such operations and assets</u>

The Commission has performed security assessments on several of its major applications. Potential risks, safeguards and countermeasures are identified in the security assessment. The specific measures of performance for measuring the level of security to protect the Commission's IT assets need to be identified and included in the draft ITC Strategic Plan or the ITC Computer Security Strategic Plan.

The level of security appropriate to protect operations consist of physical security apparatus such as turnstiles for electronic badging of people entering and exiting the FCC headquarters facility located at 445 12th Street, SW, Washington, DC. Also in place is access control to sensitive areas such as the Commission's data centers, wire closets, fire suppression closets, and the telecommunication room which houses the Commission's telephone system.

The specific measures of performance for measuring the level of security to protect the Commission's operational assets need to be identified and included in the draft IT Strategic plan.

The actual performance of determining the level of security appropriate to protect the operations and assets under the Commission's control could be enhanced by:

- Providing a more timely correction of deficiencies identified in the security assessments of the Commission's major applications.

- Developing a formally documented policy for Physical Security.

(3) <u>Up-to-date security plan (that is practiced throughout the life cycle)</u>

The Commission's business applications were developed before a formal system development life cycle (SDLC) for the agency was implemented. As a result, security plans are being developed in the maintenance phase of the Commission's SDLC.

The Commission is also in the beginning stages of developing security plans for its major applications and general support systems. A timeline for creating security plans has been developed and is being monitored by the ITC group. The Commission has up-to-date security plans developed for the following:

General Support Systems

- FCC Net
- Auctions Net

Major Applications:

- Consolidated Database System
- Universal Licensing System
- Automated Auctions System
- Experimental Licensing System
- Equipment Authorization System

The specific measures of performance for maintaining up-to-date security plans for each system supporting the operations and assets under the Commission's control needs to be identified and included in the draft ITC Strategic plan.

The actual performance of maintaining an up-to-date security plan (that is practiced through the life cycle) could be enhanced by:

- Including as part of the SDLC process, FCC's prescribed method for determining the sensitivity of its applications.

- Developing a security plan for each of the Commission's major applications.

- Developing rules of behavior that are specific to the major application.

Providing a summary of all security plans in the IT Strategic Plan or the ITC Computer Security Strategic Plan.

(4) Tested and evaluated security controls and techniques

In Fiscal Year 2000 and 2001, the Commission performed Certification and Accreditation on several of its major applications. In this process, security assessments were conducted which tested and evaluated the security controls and techniques of several major applications.

The specific measures of performance for testing and evaluating security controls and techniques for each major application supporting the operations and assets under the Commission's control needs to be identified and included in the draft ITC Strategic plan or the ITC Computer Security Strategic Plan.

The actual performance of testing and evaluating security controls and techniques could be enhanced by providing a more timely correction of deficiencies identified in the security assessments of the Commission's major applications.

Question #6 - Describe 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.

OIG response to Question #6

(1) Adequately maintaining an agency-wide security program

The FCC has designated a senior agency information security official who is referred to as the CSO (Computer Security Officer) and who reports to the Deputy Chief Information Officer (CIO). The agency-wide security program is developed and maintained in accordance with subsection (b) of the Security Act as follows:

- The FCC has developed a system development life cycle that incorporates information security principles and practices, but it is formally being carried out from the maintenance phase onward in the life cycle.

- The FCC has developed security plans that is formally being practiced from the maintenance phase onward in the life cycle.

- The CSO is involved in overseeing the development and implementation of standards and guidelines relating to security controls for FCC's applications and systems, however, performance measures need to be prescribed to determine how well the IT support for the FCC's programs are being met.

The specific measures of performance used by the agency to ensure that the agency CIO adequately maintain an agency-wide security program needs to be established and included in the draft IT Strategic Plan and the ITC's draft Computer Security Strategic Plan.

(2) Ensuring the effective implementation of the program and evaluating the performance of major agency components

The FCC has developed security policies, procedures, and control techniques that are implemented and that are being maintained by the CSO with support from other elements of the Information Technology Center. An enhancement to make the program more effective would be to:

- Improve information sharing techniques with the agency's Bureaus and Offices.

- Better integrate communication, roles and responsibilities pertaining to implementing a more effective information security program with Bureaus and Offices relevant to the agency-wide security program.

- Develop a method to evaluate the performance of the FCC's major components.

The specific measures of performance used by the agency to ensure that the agency CIO ensures the effective implementation of the program and evaluates the performance of major agency components needs to be established and included in the draft IT Strategic Plan.

(3) Ensuring the training of agency employees with significant security responsibilities.

The Commission provides Security Awareness training for all of its employees, contractors, interns and co-ops. To ensure the training of agency employees with significant security responsibilities, the ITC has identified positions designated as high risk and complies with guidance from the Office of Personnel Management regarding personnel suitability.

The Commission's training program does not require Offices and Bureaus to track and monitor the training issued to employees. Any tracking and monitoring that is being done is based on the initiative of the Offices and Bureaus. And as a result, the training of agency employees with significant security responsibility is not currently a reporting requirement for the agency's CIO.

The specific measures of performance used by the agency to ensure that the agency CIO ensures the training of agency employees with significant security responsibilities needs to be established and included in the draft IT Strategic Plan and the ITC draft Strategic Plan.

Question #7 - Describe 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.

OIG response to Question #7

- **Total number of agency employees** - The Fiscal Year 2000/2001 FTE's totaled 1,975 as presented in the President's Budget for the FCC.

- **Type(s) of security training available during the reporting period** - The reporting period consists of the Fiscal Year 2001. Security Awareness training briefings are provided around the middle of each month.

- **Number of agency employees that received each type of training -** During Fiscal Year 2001, approximately 700 FCC staff attended Security Awareness training.

- **Total costs of providing such training -** Total costs of providing Security Awareness Orientation training was not available from the FCC's Training Program Director.

For additional types of security training provided to FCC staff, refer to the CIO's annual program evaluation for the Security Act.

Question #8 - Describe 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.

OIG response to Question #8 - According to the FCC Computer Network (general support system) security plan, the FCC's Computer Incident Response Team (CIRT) has been charged to act as the Commission's focal point for mitigating the impact of computer related incidents. The team is managed by the FCC Computer Security Officer and is comprised of technical experts in the fields of PC's, computer networks, telecommunications, application(s) management, virus management, and security. The team acts to prevent or minimize the impact of a threat against computer operations at the FCC.

Planned controls consist of updating written policies and procedures for the incident response capability. The plan is to have a documented program for recognizing and handling incidents (e.g., viruses, intrusions, denial of service, etc.) by the third quarter of Fiscal Year 2001.

In addition, according to the FCC Auctions Network LAN (general support system) security plan, system anomalies or other potential security incidents are first reported to the Auctions' Technical Director. Incidents are then investigated and validated by FCC staff and contractors; the cause and nature of the event or incident is resolved before escalation. At the completion of the investigation, or during the course of the investigation if immediate resolution is not possible, the Technical Director follows appropriate FCC guidelines and reports the incident to designated FCC personnel. All security incidents are reported to the CSO within a reasonable time period.

Planned controls consist of having the tool, HP VPO (Hewlett Packard Vantage Point Operations) automatically page, e-mail, and/or display alerts on a message board notifying the responsible staff member of suspicious activity.

The documented procedures for reporting security incidents, in addition to the security plans for the general support systems, consist of the following:

- The ITC group has produced draft Incident Response Guidelines that contain procedures to monitor an incident and to ensure that is it resolved.

- The Auctions group has produced draft Incident Handling Procedures that provide steps to handle virus incidents and hacker/cracker attacks.

The current incident handling environment within FCC does not facilitate the sharing of information regarding common vulnerabilities. However, one of the planned controls is to have a documented program for recognizing and handling incidents (e.g., viruses, intrusions, denial of service, etc.) by the third quarter of Fiscal Year 2001. Another planned control is to have automatic paging, e-mailing, and/or displaying of alerts on a message board to notify the responsible staff member(s) of suspicious activity.

- Description of procedures for external reporting to law enforcement authorities and to the General Services Administration's FedCIRC.

The current procedures for external reporting to law enforcement authorities and to the General Services Administration's FedCIRC consist of the following:

> The FCC's Computer Incident Response Guidelines (draft, June 8, 2001), section 6.6.2, states that if the incident involves criminal activity or possible criminal activity notify the OIG, the FBI and NIPC.

- Include information on the actual performance and the number of incidents reported.

  The ITC identified and managed four incidents during FY'01, which included:

  - the Chinese attack on U.S. government and military sites;
  - one internal user who misused FCC resources for self gain; and
  - Code Red and Code Red II.

<u>Question #9</u> - Describe 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?

OIG response to Question #9 - The FCC integrates security into its capital planning and investment control process by incorporating funds for security into the information technology expenditures.

In the Fiscal Year 2002 Budget Estimates submitted to Congress in April 2001, the FCC requested $10.997 million in required, additional, funding for life cycle replacement of the Commission's information technology infrastructure hardware and software, for mandatory enhancements to twelve mission critical electronic filing systems and funding to implement mandatory requirements for the Commission's disability accessibility, information security, and asset management programs. The funding will be distributed among all five FCC activities: licensing, competition, enforcement, consumer information and spectrum management. The additional funding would be expended in the following areas:

Application System Maintenance and Development - The FCC requested $3.03 million for critical refreshments to twelve (12) mission critical systems. Mandatory adjustments are needed to the Commission's International, Cable Services, Mass Media and Consumer Information systems, as well as to the FCC's Office of Engineering and Technology's electronic filing systems. These applications were implemented several years ago and require web/sql replacements or upgrades to include more robust JAVA modules.

An additional $270K is required to implement an improved property management inventory system. The FCC's first financial audit revealed deficiencies in the FCC's information technology hardware/software inventory process. The additional funding will be used to design and implement a system to improve the FCC's data collection processes.

Internet, Telecommunications, Security, and Network Support - The FCC requested approximately $3.67 million for upgrades to the FCC's network infrastructure hardware and software which supports among other things, the FCC's telecommuting program. The FCC must replace many of the aging network servers, routers, switches, and local printers as well as upgrade the network operating system and firewalls. Of the amount requested, $331K is needed to ensure that all FCC applications fully meet federal government *security requirements* as called for in OMB Circular A-130.

Desktop Computer Support - The FCC requested $2.7 million for life cycle replacement of the FCC's office automation software and hardware including replacement of 900 personal computer and 200 laptops. In Fiscal Year 2002, the FCC plans to migrate to the Microsoft Office suite and Windows 2000 as the Commission's desktop operating software.

A breakout of FCC's *information technology expenditures,* including funding available in the base is shown in the following chart.

FCC IT Budget Expenditures by Fiscal Year

Information Technology Budget Initiatives ($ in millions)	FY 1999 (actual)	FY 2000 (actual)	FY 2001 (revised)	FY 2002 (request)	FY 2002 Increase Above FY 2001 Level
(1) Application System Maintenance and Development	$3.1	$6.3	$6.5	$10.8	$4.300
(2) Internet and Network Support	$3.0	$3.8	$3.5	$7.5	$4.00
(3) Telecommunications	$3.5	$3.3	$3.6	$3.6	-
(4) Desktop Computer Support	$1.8	$2.5	$2.5	$5.2	$2.697
(5) Y2K Supplemental Funding	$4.2	$2.4	-	-	-
TOTAL IT Expenditures by Fiscal Year		**$18.3**	**$16.1**	**$27.1**	**$10.997**

A description of what information technologies are included in each category from the chart on FCC IT Budget Expenditures is provided below.

(1) Application System Maintenance and Development -This expenditure would cover 30 data base systems of which 18 incorporate electronic filing or offer public access to data. The databases supported include licensing, enforcement, rulemaking and internal administration. It would also provide for routine upgrades, bug fixes and day-to-day system maintenance functions.

(2) Internet and Network Support - This expenditure would support electronic filing of license applications and other data. It would provide for an array of public information on Commission actions, proceedings and related telecommunications matters. It would also include maintenance of local area network, Internet and Intranet facilities, remote access system, and computer/network security.

(3) Telecommunications - This expenditure would provide for ISDN desktop telephone with voice mail and FTS 2001 services, automated call distribution and other specialized systems for the help desk and the Gettysburg call center. It would also provide for telephone and cellular phone services, voice mail, video and audio conferences, automated call distribution and other specialized systems, data circuits, consulting and PBX support.

(4) Desktop Computer Support - This expenditure would provide for desktop computers, peripherals and comprehensive software suite. It would include access to the Internet and agency and commercial databases. Additionally, it would provide for a Computer Resources Center helpdesk and training facility. It would provide file, print and email services supported by the local and wide area networks. It would also provide support for remote access system connectivity for telecommuters and travelers.

(5) Y2K Expenditures - This category represents the expenditures in 1999 and 2000 to provide for the Year 2000 Bug remediation project. The expenditures for this category were completed by March 31, 2000.

Question #10 - Describe 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.

OIG IG response to Question #10 - The specific methodology being used by the agency to:

Identify critical assets:

- The FCC used guidance from OMB Circular A-130, Appendix, III to identify its major applications and general support systems. In addition, the FCC used guidance from NIST SP 800-18, to determine confidentiality, integrity, and availability considerations to identify its critical assets. The assets were ranked High, Medium, or Low.

  To ensure that each FCC application experienced a consistent evaluation, the ITC group used a "yard stick" approach to evaluate each of the automated systems managed within the FCC network. The ITC group developed a methodology that allowed the group to provide a consistent criteria against which each of the automated applications, and its associated data, resident on the FCC network were evaluated. Any application rated "High" in any of the four categories in the table below were considered to be major within the FCC infrastructure.

ITC "Yard Stick"	

Importance (Revenue)	Dollar amounts generated by the system, by the collection of regulatory and application fees, which is returned to the Federal government.
	Low = $0 - $500K
	Moderate =>$500K - < $1M
	High = >$1M

System Investment	The dollar amount spent to date to develop and maintain the system, and any associated databases.
	Low = $0 - $750K
	Moderate =>$750 K - <$2M
	High = >$2M

Administrative Significance	The impact of not having the system or its associated data available for use by the Bureau/Office or the FCC *Important Note: Administrative Significance is a subjective ranking versus categories that are based on fixed costs.*

Risk/Harm	The amount of risk/harm that could be caused if the system, or its associated data were compromised (i.e., the potential damage that might be caused by a person who gained unauthorized access to the data processed by a specific system.) *Important Note: Risk/Harm is a subjective ranking versus categories that are based on fixed costs.*

Prioritize critical assets:

- The FCC used the "yard stick" methodology that was developed by the ITC group to identify prioritization. The amount of revenue generated by the system determined its level of importance. However, this importance rating is not the criteria used in operations while servicing and maintaining the system in the client/server environment. Service level prioritization still needs to be determined.

[NOTE: The *importance* rating is based on revenue generated by the system; *investment* amount is based on cost of developing the system; *administrative significance* is based on the reliability level of the system; and *risk/harm* of the system is based on whether the system supports sensitive data and whether the data is proprietary.]

Protect critical assets:

- The FCC's ITC group has begun development of security plans in accordance with NIST Special Publication 800-18 to protect critical assets. The ITC group also coordinates security assessments to identify potential risks to the FCC applications. Business continuity plans have also been developed, however, to better protect critical assets, the plans should be updated.

Links with key external systems:

- FCC's key external systems are identified through Memorandum of Agreement, Memorandum of Understanding, or Interagency Agreements. These agreements outline cross-servicing to be provided by the FCC and the corresponding responsibilities of the external organization.

System Interconnection and Information Sharing is defined in the template for FCC's security plans for general support systems and major applications in accordance with guidelines from OMB A-130, Appendix III. Section l.9 of FCC's security plans provides descriptions for any system interconnection or direct connections to the application as well as links with key external systems. Information in this section includes the following:

  - List of interconnected systems or major applications and their system identifiers.
  - Description of interconnections with external systems not covered by a security plan and any security concerns.

- Description of any required written authorizations (e.g., MOUs or MOAs) that are in place for connection with other systems and/or sharing of sensitive information.
- Detail of the rules of behavior that have been established with the interconnected site.

Question # 11 - Describe 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.

OIG response to Question #11 - The measures of performance used by the head of the agency to ensure that the Commission's information security plans are practiced through the life cycle of each of FCC's systems consist of carrying out the goals of the Information Technology Strategic Plan (ITSP) as well as correcting deficiencies found in prior years. Satisfying the functional, technical and business needs of the bureaus and offices is the primary focus of the (draft) ITSP. The planning process addresses these needs by involving internal stakeholders in individual and small group interviews and group workshops where problems were defined and strategic vision and proactive procedures were identified.

In addition, developing comprehensive security plans was identified as a material weakness finding in the "Report on the Federal Communications Commission, Fiscal Year 2000, Financial Statements", dated June 27, 2001. The correction of this deficiency will be tracked for timely response as well as how effectively developed the security plans are for FCC's major applications.

FCC is in the beginning stages of developing security plans. It is recommended that in a subsequent review year, the status of security plan development be assessed.

Question #12 - Describe 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).

OIG response to Question #12 - The FCC's security program environment is governed by the Computer Security Program Directive 1479.1. The provisions of the directive apply to all FCC employees and contractors who use a computer system or access computer generated data to conduct business on behalf of the FCC. The directive discusses safeguard measures to be taken for computer related information systems processing or containing sensitive and Commission critical data. The directive should also be used as a minimum standard for safeguarding other non-sensitive information processed or stored on FCC computer equipment.

It is the policy of the FCC that computer systems, sensitive and mission critical information, and facilities that promote the process of such information shall be used for official agency/government business only, and shall be secured to at least the minimum level of security defined in directive 1479.1 and other related FCC directives. FCC users must not store national security classified information on FCC computer systems, unless specifically authorized by the Associate Managing Director – Operations, Personnel Security Office. A copy of each authorization must be forwarded to the Computer Security Officer.

The FCC also maintains an "Information Security Manual" for classified information. In Chapter 1, Section 4, Purpose and Applicability, it is stated that the regulations establish uniform Commission policies, standards, criteria and procedures for the classification, safeguarding, downgrading and declassification of National Security Information, and provide for oversight and administrative sanctions for violations. The regulations are applicable to all Commission headquarters and field activities. It further states in Chapter 2, Section 1, Security Classification Designations, that information or material that requires protection against unauthorized disclosure in the interest of national security shall be classified in one of three designations, namely: "Top Secret," "Secret," or "Confidential." The markings "For Official Use Only," and "Limited Official Use" shall not be used to identify classified information. Moreover, no other term such as "Sensitive," "Conference," "Agency" or "Commission" shall be used in conjunction with the authorized classification designations to identify national security information. Classification cannot be used to conceal violations of law, inefficiency, or administrative error, to prevent embarrassment, nor to restrain competition.

The Commission's policy on the handling of non-public information is stated in FCC (draft) Directive 1139. The purpose of (draft) directive 1139 is to establish policies and procedures for managing and safeguarding non-public information. These procedures are necessary to protect the integrity of the Commission's decision-making process and to ensure public confidence in the agency's ability to protect proprietary and other similar material. Unauthorized disclosure of non-public information is prohibited by the Commission's rules and unauthorized disclosure of non-public information may result in disciplinary action. In the case of contractors, unauthorized disclosure may result in termination of the contract, replacement of a contract employee, or other appropriate measures.

The above topics are introduced to users of FCC's computers in the Security Awareness Orientation that is provided monthly to all new users of the general support system. A User Access Acknowledgement form is required to be signed at the completion of training to provide assurance that users are aware of their information security responsibility. The policy for use of computer resources as stated on the User Acknowledge Form is:

As an employee or contractor of the Federal Communications Commission (FCC), you are required to be aware of, and comply with, the FCC's policy on all usage and security of computer resources.

The specific topics covered on the form are:

- Responsibility for all actions performed with a users personal user ID

- Policy, Standards and Procedures that must be followed.
- Advising the user to control the information they access
- Proper use of the FCC computer resource is the user's responsibility

Physical Security Program

The FCC Directive 1479.1, Section 14, provides a topic on Physical Security and Computer Equipment Handling. The policy states that the offices and work areas where FCC computer systems are located must be physically secured when unattended. The policy further states that adequate controls should be employed consistent with the value, exposure and sensitivity of the information and equipment that is to be protected. The policy advised that although the value of a computer can be significant, the value or importance of the information, can be far greater.

The Commission houses two data centers that are located on separate floors within the 445 12th Street, SW, Washington, DC, headquarters facility. The data centers are designated as sensitive areas, therefore, the access is controlled by issuing access to those personnel who must have access to the data centers.

Card keys must be used upon entry and exit to the FCC headquarters facility. All visitors must sign in, receive a visitor badge, and must also pass through the metal detector apparatus to complete the screening process. The elevator lobbies on each floor have access control points that restrict visitors from using their badge to enter the FCC work area. To enter an FCC work area, the visitor must be escorted by a holder of an FCC employee badge or contractor badge. A formally documented physical security policy needs to be developed.

Operational Security Program

The Commission's operational security program safeguards the critical infrastructure through its personnel security and suitability manual policy; through the logical access controls to FCC's general support systems and major applications, and through having contingency plans for continuity of FCC's business operations.

Personnel Security/Suitability Manual (draft)

The purpose of the FCC Personnel Security/Suitability Manual (Manual) is to provide guidance and a basic understanding of the responsibilities, duties, and assignments for the FCC's Personnel Security and Suitability Program. The FCC's practice and policy is to employ and retain individuals who are found suitable for Federal employment in order for the FCC to complete its operations, goals, and missions. Every appointment, including contractor positions, shall be made subject to investigative processing.

The FCC's Security Operations Center (SOC) maintains a personnel/suitability file on each individual. The SOC is the main repository for all security information and the SOC maintains a Personnel Security database/file. Privacy Act and Freedom of Information act requests for security information is referred to the SOC for direct response to the requestor. The personnel security/suitability file consists of the individual's completed Standard Form 85, or 86 that is applicable to the designated position risk/sensitivity level. These forms may be destroyed after completion of the OPM report of investigation and after the Security Officer certifies and dates the Certification of Investigation (CIN). The file also consists of a copy of the Position Risk Designation Record with the OF 8, Position Description.

Initially, the Commission's Human Resources Management Office designates all FCC positions as to the position's risk/sensitivity level using the Office of Personnel Management's Position Risk Designation System upon receiving a position description from the Bureaus/Offices. The SOC reevaluates HRM's initial designation determination to ensure accuracy and consistency in the FCC's Personnel Security and Suitability Program. The SOC has the final decision on all position risk/sensitivity level designations.

Contingency Planning

The security plans for major applications and general support systems contains a section on contingency planning. The objective is to provide procedures that will permit the organization to continue essential functions if information technology support is interrupted. The procedures (contingency plans, business continuity plans, and continuity of operations plans) should be coordinated with the backup contingency, and recovery plans of any major application. The contingency plans should ensure that interfacing systems are identified and contingency/disaster planning coordinated.

Also in place as an operational control is the "TechFest" meeting, which is held every day at 8:30 AM. The TechFest meeting is a forum to discuss the issues of the day or the problems that may have come up over night. The attendees are from the Information Technology Center with a representative from each area of support.

Question #13 - Describe how 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.

OIG response to Question #13

Private Sector Agreements

The Commission's Office of the Managing Director, Information Technology Center, made a computer security facility site visit inspection to J.P. Morgan/Chase Bank in New York City, NY. The purpose of the site visit was to perform a cursory review of the facility to ensure that an adequate baseline security posture was in place prior to the transfer of FCC information to the contract facility. A second objective of the site visit was to verify that the FCC was about to engage in a bona-fide professional business versus a type of business where adherence to security policy might not be a business priority.

FCC computer security policies have no exclusionary provision, but are applicable to computer systems and information/applications containing FCC information for which the FCC is the legal custodian. The boundaries of responsibility apply whether the processing services are performed at a FCC facility or by a contracted vendor. More and more Federal government work is being performed by contractors. When these organizations are under contract with the FCC, the contract must specify adherence to the FCC Computer Security Program Directives. In addition, before entering into an agreement to process or handle sensitive information at a contractor facility, a security assessment of the facility should be conducted, or should have been completed within the previous three years. The results of the analysis will be made available to the Contracting Officer and the Computer Security Officer for review.

The contract should specify that FCC reserves the right to perform on-site inspections (announced/unannounced) of the site where FCC information is being processed. The inspections are used as a tool to ensure adherence to FCC's computer security directive and policies, and other applicable Federal regulations and mandates.

The target facility for the site visit inspection was J.P. Morgan/Chase Bank, Capital Market Fiduciary Services, 450 West 33rd Street, New York, NY. The following represents a list of the security controls that were in place at the target facility:

- Physical Safeguards at the facility
    - Picture ID assigned to each person working for J.P. Morgan/Chase Bank;
    - Guests are required to sign in/out when visiting J.P. Morgan/Chase Bank facilities;
    - 24/7 guard services are provided at the facility
    - Guard monitoring station in place with displaced cameras throughout the building with centralized monitoring;
    - Fire alarms installed throughout the building, which alarm locally; and
    - Sprinkler fire suppression system installed throughout the building.

- Storage Vault Safeguards
    - Diebold card access with picture ID assigned to each person who is granted permission to access the document storage vault;
    - Magnetic locking systems installed on all doors accessible to the vault;
    - Slab-to-slab walls installed in the vault;
    - No raised floors installed in the vault; and
    - Motion detection system installed in the vault with alarming to guard station.

- Computer-based Loan Processing System (Mortgage Collateral System (MCS))
    - NT v.4.0 platform;
    - Appropriate use banner displayed at each user login session;

  - Running Norton Anti-Virus software (updated routinely);
  - Screen saver use mandatory;
  - 10 minute automatic timeout feature when connected to MCS; and
  - Internet System Security (ISS) is used to provide system level intrusion detection capabilities.

- Other in-place safeguards consisted of:
  - System Development Life Cycle;
  - Policy on computer security and system usage;
  - Encryption use policy, includes the use of connect direct, MQ Security and DES;
  - Computer Security Awareness Training is provided to all J. P. Morgan/Chase Bank employees (e.g., user level awareness, technical level, system custodian and local user level);
  - Hot site contingency planning facility located at 4 New York Plaza. Site can be occupied within 24 hours and is equipped with similar physical and environment security controls as in place at the 450 West 33rd Street facility; and
  - System level backup are performed routinely (e.g., intro-day, nightly and weekly) and stored on DLTs using a centrally located disk farm.

The cursory review of the site visit inspection provided verification that security controls that are physical, logical, and computer-based, appear to be in place. Although the security controls were not tested for reliability, discussions with respective program managers were held.

Agreements with Federal Agencies

The Commission has entered into Memorandum of Understanding, Memorandum of Agreement and Interagency Agreement with agencies that provide service to the FCC. However, the Commission has not performed an audit or inspection of these contracted servicing agencies. The following cross-servicing agreements have been developed:

- The Federal Communications Commission and the US Department of Interior, Bureau of Reclamation, Administrative Services Center (ASC) have entered into a Memorandum of Understanding. The ASC provides processing services and operations support to the FCC on the Federal Financial System (FFS).

- The Federal Communications Commission and the National Business Center/Products and Services (NBC/PS), Office of the Secretary, have entered into a Memorandum of Understanding. The NBC/PS provides detail database conversion of the Nortridge Loan System (NLS) from Sybase to Oracle, configuration setup, implementation, ongoing database administration and security administration services and support to the FCC.

- The Federal Communications Commission and the US Department of Agriculture have entered into a Memorandum of Agreement. The USDA provides payroll and personnel data processing services and telecommunications access to the USDA mainframe to the FCC.

- The Federal Communications Commission and the Department of Interior Franchise Fund, National Business Center (DOI/NBC) have entered into an Interagency Agreement. The DOI/NBC provides software maintenance and NBC Help Desk support for the FCC implementation of the Interior Department Electronic Acquisition System – Procurement Desktop (IDEAS-PD) to the FCC.

The agreements mentioned above (MOU, MOA, IA) are with Federal government agency service centers. Some of these agreements were entered into as early as June 1989. Although an implied trust relationship exists between agencies who provide cross-servicing, a review of the audits and/or inspections performed on the contracted servicing agency needs to be enforced.

Question #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.

OIG response to Question #14 - This question is not applicable to the OIG per OMB reporting instructions.