Office of Inspector General

Independent Evaluation Report

Review of Federal Trade Commission Implementation of the Federal Information Security Management Act For Fiscal Year 2005

September 29, 2005

OFFICE OF
INSPECTOR GENERAL

FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

September 29, 2005

Chairman Majoras:

The Office of Inspector General (OIG) recently completed its Independent Evaluation of information security pursuant to requirements contained in the Federal Information Security Management Act (FISMA) of 2002. This is the fifth annual evaluation completed by the OIG in the area of information and computer security.

This year's review objectives were to assess compliance with FISMA and related information security policies, procedures, standards and guidelines, and to test their effectiveness on a representative subset of the agency's information systems. Specifically, this review (i) evaluated the implementation of the Federal Trade Commission (FTC) information security program; (ii) assessed agency progress towards correcting weaknesses addressed within the FY 2005 Plan of Action and Milestones (POA&M); (iii) verified and tested information security and access controls for the FTC Network and modem pool; (iv) verified staff compliance with the agency's wireless network policy; and (v) evaluated the implementation of IT security policies and procedures at one FTC regional office.

The FTC continues to make progress in developing a mature information security program, and has implemented or addressed many of the OIG-identified security vulnerabilities discussed in the prior year evaluation. For example, the FTC (i) tested its Major Applications and General Support Systems for security vulnerabilities; (ii) addressed 51 of 111 issues identified on its POA&M and developed time frames to address the remaining 60 issues; (iii) developed new policies and procedures to keep abreast of emerging security vulnerabilities; (iv) implemented a scanning and remediation program for identifying and correcting system vulnerabilities; and (v) modified the inventory to include interconnections to other systems.

The FTC has also taken steps to ensure privacy in accordance with M-99-05, *Instructions for Complying with the President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records."* The FTC established a Privacy Steering Committee to address and monitor security issues. The FTC posted its privacy policy on its website and runs scans to identify and correct privacy related vulnerabilities associated with its website. The FTC has also taken steps to ensure the security and privacy of data located on contractor-owned and/or managed systems.

The agency's firewall did not permit the OIG's team of "ethical hackers" to penetrate the network, and the OIG, using sophisticated electronic tracking and detection instruments, did not identify any wireless networks at the headquarters or 601 NJ buildings.

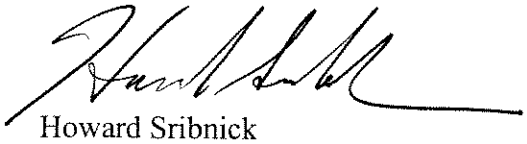
At the FTC's Southwest Regional Office the OIG observed physical and operational controls in place to safeguard data. Guards are posted in the lobby around the clock, closed-circuit cameras monitor internal and external activity and smoke detectors are prevalent. All full-time staff interviewed attended the FTC Security Awareness training and our interviews revealed that staff is aware of and follow FTC policies and procedures.

While the agency has made many needed changes and improvements in its IT security program, the OIG has identified some new vulnerabilities that could impact the overall effectiveness of the IT security program. The OIG identified a vulnerability in the agency's modem pool that enabled the OIG to breach the modem's security controls. Although the OIG did not attempt to exploit this breach to determine the extent or seriousness of the vulnerability, the breach would enable a hacker to execute additional attacks on the FTC network that would have been impossible without the breach. Additional details were provided to ITM managers, who took immediate steps to correct the vulnerability. This and other technical vulnerabilities discovered by the OIG that could compromise FTC IT security were provided to ITM in a separate (nonpublic) report.

The OIG also identified weaknesses in the agency's background check process for IT employees. Approximately 30 percent of ITM full-time staff had outdated or no background investigation. Half of these individuals have significant data access responsibilities and/or security responsibilities. We also identified a weaknesses in the assignment of "roles" to ITM personnel working with the agency's personnel database. This allowed liberal access to privacy data even though such access was not needed for job performance responsibilities.

The OIG review was conducted from June 14, 2005 to September 26, 2005, and followed National Institute of Science and Technology guidance for information systems, OMB Memorandum M-05-15, *FY2005 Reporting Instructions for the Federal Information Security Management Act* (June 13, 2005) and best practices used in the industry. The OIG wishes to thank ITM management for the cooperation and assistance it provided to the OIG during the period of our review.

Respectfully submitted,



Howard Sribnick
Inspector General

EVALUATION SUMMARY

INTRODUCTION

The Federal Trade Commission's (FTC) Office of Inspector General (OIG) completed this Independent Evaluation Report along with the IG's portion of the Office of Management and Budget (OMB) mandated Executive Summary for FY 2005. This OIG Independent Evaluation Report, unlike the Executive Summary which focuses on performance measures, provides specific findings and, when applicable, recommendations for resolution.

On December 17, 2002, the President signed into law the E-Government Act of 2002 (Public Law 107-347), which includes Title III, the Federal Information Security Management Act (FISMA) of 2002. The FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act (GISRA) of 2000, which expired in November 2002. The FISMA outlines the information security management requirements for agencies, including the requirement for annual review and independent assessment by agency inspectors general. In addition, FISMA includes new provisions aimed at further strengthening the security of the federal government's information and information systems, such as the development of minimum standards for agency systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs and to develop strategies and best practices for improving information security.

OBJECTIVES

The objectives of the independent evaluation of the FTC information security program were to:

1. Assess compliance with FISMA and related information security policies, procedures, standards and guidelines;

2. Determine the effectiveness of information security policies, procedures and practices as implemented at headquarters and the SWRO in Dallas, TX

3. Perform an external penetration test to identify vulnerabilities in the agency's external security controls, and

4. Assess privacy protection controls.

The results of these various evaluations are presented in this Independent Evaluation Report along with a number of recommendations to address vulnerabilities identified during the evaluation.

RESULTS IN BRIEF

FISMA defines information security as "... protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide (i) integrity -- guarding against improper information modification or destruction, and ensuring information nonrepudiation and authenticity; (ii) confidentiality -- preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (iii) availability -- ensuring timely and reliable access to and use of information."

The OIG found that FTC's Office of Information and Technology Management (ITM) continues to make progress in developing a mature information security program, and has implemented or addressed OIG-

identified security vulnerabilities discussed in previous independent evaluation reports and other security reviews. For example the FTC:

- Certified and accredited (C&A) six of its nine Major Applications and General Support Systems (GSS). (One of the of FTC's major applications is owned and managed by the Department of Interior (DOI) and is not included in the nine.) One system has an Interim Authority to Operate (IATO), and ITM is planning to give the two remaining systems IATO. ITM plans full C&A's on the three IATO's by CY 2005 end.
- Addressed 51 of the 111 issues identified in the Plan of Action & Milestones (POA&M), with plans to address the remaining 60 issues.
- Continued to improve the POA&M management process
- Instituted a scanning and remediation process
- Modified inventory management to include interconnections to other systems.

The OIG also conducted a penetration test of the FTC network and ran tests to determine if any wireless networks were set up within the FTC environment. The test detected no wireless signals emanating from within the FTC facilities located at 600 Pennsylvania Ave. or 601 New Jersey Ave. However, the penetration test and vulnerability assessment identified six vulnerabilities within the FTC network environment. These findings as well as the wireless network test findings are discussed in a non-public report entitled *Penetration Testing Report and Vulnerability Assessment for the Federal Trade Commission,* September 2005, that was provided to ITM managers for immediate action.

TheOIG found that the agency has enhanced IT security controls in a number of important areas. However, the OIG also identified control weaknesses and vulnerabilities that merit management's attention. These various conditions are discussed in the body of the report.

TABLE OF CONTENTS

1 Background

On December 17, 2002, the President signed into law the E-Government Act of 2002 (Public Law 107-347), which includes Title III, the Federal Information Security Management Act (FISMA) of 2002. FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act (GISRA) of 2000, which expired in November 2002, and outlines information security management requirements for agencies, including the requirement for annual review and independent assessment by agency inspectors general. In addition, FISMA includes new provisions aimed at further strengthening the security of the federal government's information and information systems, such as the development of minimum standards for agency systems. The annual assessments provide agencies with the information needed to determine the effectiveness of overall security programs and to develop strategies and best practices for improving information security.

2 Purpose

The objectives of the independent evaluation of the FTC information security program were to:

1. Assess compliance with FISMA and related information security policies, procedures, standards and guidelines;

2. Determine the effectiveness of information security policies, procedures and practices as implemented at headquarters and the Southwest Regional Office (SWRO) in Dallas, TX

3. Perform an external penetration test to identify vulnerabilities in the agency's external security controls, and

4. Assess privacy protection controls.

3 Scope and Methodology

The scope of this independent evaluation of the FTC FY 2005 information security program included:

- Review of FTC major applications and general support systems security documentation
- POA&M review for completeness and accuracy
- Implementation of privacy controls
- Self-assessment review
- Exhibit 53 review focusing on IT security budget reporting
- E-Gov analysis
- Review of least privilege access to IT systems and resources
- Privacy management controls
- FTC scan process review
- Penetration testing
- Background investigations
- Regional Office visit

To accomplish the review objectives, the OIG conducted interviews with Information and Technology Management (ITM) staff including the Chief Information Officer (CIO), the Senior Information Security Officer, other members of the CIO staff and FTC SWRO personnel. The team reviewed documentation

provided by the FTC including security plans, risk assessments, the disaster recovery plan (DRP), C&A packages, privacy impact assessments, self-assessments, information security budgets and other security related policies. The OIG reviewed ITM's vulnerability scanning and remediation process to determine if the process could be streamlined or improved. Additionally, the OIG performed a penetration test of the FTC's IT network and applications and determined whether wireless networks were in use at the agency. OIG reviewed physical security controls at the SWRO. Finally, the review included a site survey, documentation reviews, and interviews with FTC personnel.

All analyses were performed in accordance with guidance from the following:

- Office of Management and Budget (OMB) Memorandum M-05-15, *Reporting Instructions for the Federal Information Security Management Act*, June 13, 2005.
- FTC policies and procedures.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998.
- Small Agency Council Memorandum SACCIO-05-1.
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26, *Self-Assessment Guide for Information Technology Systems*, August 2001.
- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, July 2004.
- NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, June 2002.
- NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, May 2004.
- Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.
- *Quality Standards for Inspection* issued by the President's Council on Integrity and Efficiency.
- GAO, *Federal Information System Controls Audit Manual*, Volume I: Financial Statement Audits, January 1999.
- FTC/OIG audit guidance.
- OMB Memorandum M-03-22 *Guidance for Implementing Privacy Provisions of the E-Government Act of 2002.*
- OMB Guidance M-04-15 *Guidance Development of Homeland Security Directive (HSPD) – 7 Critical Infrastructure Protection Plans to Protect Federal Infrastructure and Key Resources.*

Fieldwork was conducted between June 14 and August 15, 2005.

4 General Overview

ITM continued to progress in developing a mature information security program and has implemented or addressed OIG-identified security vulnerabilities discussed in the fiscal year (FY) 2004 Independent Evaluation report and in other security reviews and vulnerability scans. For example the FTC:

- Certified and accredited six of its Major Applications (MA) and General Support Systems (GSS) and has made substantial progress in completing C&A's in the two newly identified systems.
- Addressed 51 of 111 issues identified on the POA&M, with plans to address the remaining 60 issues.
- Made improvements in its POA&M tracking and reporting process.
- Continued to develop policies and procedures that addressed various security issues.
- Developed a scanning and remediation program for identifying and correcting system vulnerabilities.
- Modified the inventory to include interconnections to other systems.

In addition to these improvements, the OIG noted that self-assessments were prepared for many of the FTC's GSS's and MA's. At the time of the review, the FTC had completed self-assessments for Infrastructure, Hart-Scott-Rodino Electronic Filing System (e-Premerger), the Consumer Information System (CIS), CommentWorks, and Documentum. There are also plans to complete a self-assessment for the Matter Management System (MMS).

Exhibit 53's are being completed and security costs are listed as separate line items. Additionally, the FTC is preparing Exhibit 53 supplementary information forms in accordance with the Small Agency Council Memorandum SACCIO-05-01.

FTC has also taken steps to ensure privacy in accordance with M-99-05, *Instructions for Complying with the President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records."* The FTC set up a Privacy Steering Committee to address and monitor security issues. FTC posted its privacy policy on its website and runs scans to identify and correct privacy-related vulnerabilities associated with its website. FTC has also taken steps to ensure the security and privacy of data located on contractor-owned and/or managed systems. For example, the FTC certified and accredited Do-Not-Call (DNC) in September 2004 (systems owned and operated by AT&T) and is in the process of conducting a System Test & Evaluation (ST&E) on the system. A Certification & Accreditation (C&A) is also being performed on CommentWorks, and other contractor-owned and operated systems.

At the FTC's SWRO, the OIG observed physical and operational controls in place to safeguard data. Guards are posted in the lobby around the clock, closed-circuit cameras monitor internal and external activity and smoke detectors are prevalent. All full-time staff interviewed attended the FTC Security Awareness training and our interviews revealed that staff is aware of and follow FTC policies and procedures.

Notwithstanding the security controls in place at FTC Headquarters and the SWRO, the OIG found other areas where improvements are still needed. While no significant deficiencies were found according to the FY2005 definition provided by OMB, the OIG did identify the following reportable conditions.[1]

5 Self-Assessment Review

FISMA requires that Federal agencies conduct annual reviews of their MA's and GSS's. Self-assessments provide a method for agency officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. The *Security Self-Assessment Guide for Information Technology Systems,* NIST SP 800-26, utilizes an extensive questionnaire containing specific control objectives and techniques against which an unclassified system or group of interconnected systems can be tested and measured. The control objectives and techniques are abstracted directly from long-standing requirements found in statute, policy, and guidance on security.

[1] FY 2005 OMB guidance no longer requires that significant deficiencies be reported in the annual FISMA evaluation, although they are still required to be tracked on POA&Ms. A significant deficiency, according to OMB guidance, is a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information. A reportable condition exists when a security or management control weakness does not rise to the level of a significant deficiency, yet is still important enough to be reported to internal management.

The review confirmed that ITM prepared self-assessments for the following systems:

- Infrastructure (June 20, 2005)
- Hart-Scott-Rodino Electronic Filing System (e-Premerger) (not dated)
- Consumer Information System (CIS) (June 21, 2005)
- CommentWorks (performed by ICF Corporation) (April 20, 2005)
- Documentum (March 15, 2005)

A contract was in place to conduct a self-assessment for the MMS at the time fieldwork was conducted.

Analysis of the documents revealed that, in general, the self-assessments:

- Were typed and easy to read;
- Listed the system name;
- Indicated the system's level of sensitivity/criticality;
- Listed connections to other systems;
- Indicated whether the systems were major applications or general support systems;
- Matched the NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* criteria with the corresponding SP 800-26 question set, when possible. SP 800-53 identifies the security controls that must be in place for systems based on their confidentiality, integrity, and availability (CIA) levels. Future self-assessments and security documentation will be based upon this guidance;
- Listed documentation that was associated with each section at the beginning of each section; and
- Were color coded to indicate whether Operations Assurance (OA), Operations, or Administrative Services would be the source of the information.

Several vulnerabilities were identified during the review of the self-assessments. The vulnerabilities that applied across all of the self-assessments are listed below.

Finding: The questionnaire cover sheet for the self-assessments are either incomplete or are not included with the self-assessment.

SP 800-26, *Self-Assessment Security Guide For IT Systems,* provides specific guidance on what should be included in the sections that make up the questionnaire cover sheet. The guidance states:

- All completed questionnaires should be marked, handled and controlled at the level of sensitivity determined by organizational policy;
- The cover page of the questionnaire should begin with the name and title of the system to be evaluated;
- The system category should be marked and any specific agency system types or system categories should be included;
- The purpose and objectives of the assessment should be identified;
- The start and completion date of the evaluation should be listed; and
- The level of sensitivity of information as determined by the program official or system owner should be documented using the table on the questionnaire cover sheet.

Review of the self-assessments found that the cover sheets were either not completed properly or not included with the self-assessments. Weaknesses that applied across most of the self-assessments were:

- Self-assessments were not labeled to indicate their level of sensitivity;
- Self-assessments did not list the start and completion date of the review;

- Security-control effectiveness levels were not completed per NIST instructions;[2]
- Purpose/objective section was not completed; and
- The names of the assessors were not always included on the cover sheet

Without such detail included in the self-assessments, critical information about the system may be missed when reviewing the self-assessments, and the self-assessments may be mishandled because the security level of the document is not identified.

Recommendation 1. System owners should complete the coversheets in accordance with NIST SP 800-26 guidance and include them with the self-assessment.

In addition to the general self-assessment findings, system specific self-assessment findings were identified. These findings are discussed below.

Finding: CommentWorks - The self-assessment did not respond to critical evaluation questions and did not include a cover sheet.

SP 800-26 provides a specific form and format to be used for self-assessments. The guidance states that the questionnaire section may be customized by the organization by adding additional questions and requiring more descriptive information, and may even include pre-marked questions. The guidance goes on to say that critical element levels should be determined based on the answers to the subordinate questions.[3] Finally, SP 800-26 also states that questionnaires should not have questions removed or questions modified to reduce the effectiveness of the control.

The self-assessment form prepared by Commentworks-ICF did not include the critical element questions. Further, the form did not include the self-assessment coversheet. In addition to not complying with NIST standards, this weakness makes it more difficult to assess the overall security of the system because all of the relevant information is not included in the self-assessment.

Recommendation 2. System owners should use the most current self-assessment form found in SP 800-26 when completing the next self-assessment. The cover sheet should be completed and included with the questionnaire, and no questions should be removed from the questionnaire.

Finding: ePremerger - Some critical elements on the self-assessment were marked at higher levels than control objectives under that category.

According to SP 800-26 certain conditions must be implemented before the next level of effectiveness can be achieved on the self-assessment. Therefore, the level assigned to the critical element can be no higher than the lowest level assigned to the control objective under that critical element. Critical element

[2] SP 800-26 identifies five levels of effectiveness for security controls. These levels are:
Level 1 – Control objective documented in a security policy
Level 2 – Security controls documented as procedures
Level 3 – Procedures have been implemented
Level 4 – Procedures and security controls are tested and reviewed
Level 5 – Procedures and security controls are fully integrated into a comprehensive program
SP 800-26 states that if a topic area is documented at a high level in policy, the level 1 box should be checked in the questionnaire. If a specific control is described in detail in procedures, and implemented, the level 2 and level 3 boxes should be checked in the questionnaire. An example of how the self-assessment should be completed can be found in Appendix C of the SP 800-26 document.

[3] Critical elements are used to develop a hierarchy within the self-assessment for assessing a system. These critical elements are derived from OMB A-130. The critical element level of effectiveness is based on the answers provided to the subordinate questions associated with the critical element.

7.1 was marked at Level 2 "procedures" compliance; while, some of the control objectives in that category are marked at Level 1 "policy" compliance. The effect of improperly completing the self-assessment is that the management may make improper security decisions based upon inaccurate information.

Recommendation 3. Complete the e-Premerger self-assessment in accordance with NIST SP 800-26. Specifically, do not mark critical elements higher than the lowest level assigned to any of the control objectives in that category.

Finding: Infrastructure - The self-assessment does not identify systems connected to Infrastructure.
SP 800-26 states that a system's connection to other systems should be listed, and once the assessment is complete, a determination should be made and noted on the cover sheet as to whether the boundary controls are effective. The systems that connect to Infrastructure GSS are not listed on the self-assessment cover page. As a result, connections to other systems may be overlooked leading to possible access-control vulnerabilities going undetected.

Recommendation 4. ITM should list the systems connected to the Infrastructure GSS on the cover sheet of the self-assessment. Then, determine and report whether boundary controls are effective.

Finding: Documentum - The sensitivity/criticality levels in the self-assessment do not match the level assigned in the security plan.
SP 800-26 requires that the sensitivity/criticality of the system be listed on the self-assessment cover sheet. The information process should be related to each of the three basic protection requirements of confidentiality, integrity, and availability. The self-assessment gave Documentum a confidentiality score of Medium, an integrity score of High, and an availability score of Medium. The Documentum system security plan stated a confidentiality-integrity-availability (CIA) rating of Medium.

Having different organizations develop the self-assessment and the system security plan may have caused this vulnerability. Having sensitivity/criticality ratings that do not match leads to confusion as to the actual CIA levels of the system. The wrong security controls may be applied.

Recommendation 5. Correct the confidentiality, integrity, and availability levels on the Documentum self-assessment so that it reconciles to the security plan's confidentiality, integrity, and availability levels. These levels should be determined using FIPS 199.

6 Exhibit 53 Review

As part of this year's FISMA review, OIG reviewed FTC's Exhibit 53 documents to determine if the FTC is reporting its IT security investments in accordance with OMB Circular A-11, Part 7 *Planning, Budgeting, and Management of Capital Assets* (OMB A-11). According to OMB A-11, all major IT investments must be reported on each agency's Exhibit 53. The Exhibit 53's are used in the agency's capital planning process. The OIG reviewed the FTC FY 2005 Exhibit 53 submission to confirm that it meets OMB requirements.

A draft Small Agency Council Memorandum SACCIO-05-1 to the CIO's of all small and independent federal agencies stated that, for the IT budget reporting for FY 2007, OMB and Small Agency CIO Council are placing particular emphasis on completion of the Exhibit 53. OMB will notify the agency if any of the IT investments listed on their Exhibit 53 will require a more detailed Exhibit 300 for a

particular investment.[4] The memorandum also stated that each small agency should include an Exhibit 53 Supplementary Information Form with their Exhibit 53.

The OIG confirmed, based upon review of the draft FY 2007 Exhibit 53 submission, that security is being identified as a separate line item and that the FTC is preparing Exhibit 53 supplementary information forms for the FY 2007 submission in accordance with SACCIO-05-1. The forms are being completed for:

- Consumer Protection Mission
- Maintaining Competition Mission
- Federal Financial System
- General Support System
- IT Infrastructure and Office Automation and Telecommunications

No weaknesses were identified.

7 E-Gov Systems

Federal agencies are required to conduct reviews of how information about individuals is handled within their agency when they use information technology (IT) to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information. Agencies are also directed to describe how the government handles information that individuals provide electronically, so that the American public has assurances that personal information is protected.

Based upon discussion with ITM personnel and the OIG's review of Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, September 26, 2003, the FTC has no E-Gov systems.

8 System Certification & Accreditation Review

Review of the C&A packages for FTC systems confirmed that six of the nine FTC systems identified as major applications and general support systems are certified and accredited. The systems were certified and accredited between June 2004 and September 2004, and include the following:

- Infrastructure (GSS)
- Documentum (MA)
- E-premerger (MA)
- Do Not Call (MA)
- Consumer Information System (CIS)
- Matters Management System II (MMS 2)

CommentWorks has an interim certification and accreditation

Vulnerabilities associated with these C&A packages are:

[4] In prior reviews, the OIG reviewed Exhibit 300's as part of our overall IT security investment audit plan. The Exhibit 300 is a planning document and a performance tracking document. Although it was originally designed to assess IT investments, it later expanded to cover non-IT capital assets. ITM confirmed with the OIG that small agencies were not required to prepare or submit Exhibit 300s this year.

***Finding:* The Do Not Call (DNC) C&A package is incomplete.**
SP 800-37 defines security certification as a comprehensive assessment of management, operational, and technical security controls in an information system, made in support of security accreditation. The guidance also states that the security certification package should contain a:

- Security plan (based on a risk assessment)
- Security assessment report
- POA&M

The guidance states that all C&A's initiated after finalization of NIST SP 800-37 must be consistent with SP 800-37. SP 800-37 was finalized in May 2004.

Additionally, ITM-2004-02, *System Security Certification & Accreditation Policy,* states that the C&A package should contain:

1. System security plan
2. Risk assessment
3. Security testing & evaluation (ST&E) report
4. Privacy impact assessment (if required)
5. System POA&M
6. Certifier's statement

The C&A package that ITM provided to the OIG for the DNC did not have a POA&M or an ST&E, although ITM was performing an ST&E (scheduled for completion 10/15/05) at the time of our fieldwork. DNC was originally certified and accredited before an ST&E was a required part of the C&A package. Regardless, the OIG believes that by not performing an ST&E prior to placing the system into production, there could be unknown vulnerabilities that could impact operation of the system and the security of the data. As stated, ITM has already initiated steps to address this issue.

***Finding:* Not all of FTC's GSS's are certified and accredited.**
OMB A-130, Appendix III, requires that major applications and general support systems undergo a security C&A once every three years, or sooner, if the system has undergone major modifications. At the close of fieldwork, the Internet Lab and the Litigation Support Lab were not certified and accredited. The OIG was concerned since these systems are in production and operating potentially with unknown vulnerabilities.

ITM explained that these systems were identified as GSS's only within the past year, and that it has taken steps to complete a C&A for each system.

***Finding:* Documents in the CommentWorks C&A package do not follow NIST guidance.**
FIPS PUB 199 defines three levels of potential impact (high, moderate, or low) on organizations and individuals should there be a breach of security. FIPS 199 states that these standards shall apply to all information within the federal government other than classified information and national security systems. SP 800-30 identifies vulnerabilities as part of the risk assessment process. The sample risk assessment outline found in Appendix B of the document includes a section for reporting vulnerabilities. OMB A-130 requires that systems undergo a ST&E as part of the C&A process.

Review of the C&A package found that (1) sensitivity/criticality of the system was not determined in accordance with FIPS 199 in either the risk assessment or security plan, (2) the risk assessment did not identify any management, operational, or technical vulnerabilities associated with the system, and

(3) CommentWorks did not have a finalized ST&E. ITM told the OIG that a CommentWorks ST&E is scheduled to be completed in October 2005.

Until the ST&E is complete, ITM may not have a clear understanding of the vulnerabilities associated with operating CommentWorks. Additionally, without assessing the sensitivity/criticality using FIPS 199 guidance, ICF may not have a clear understanding of the sensitivity/criticality requirements of the data collected.

Recommendation 6. Report system vulnerabilities and related information in the risk assessment as described in SP 800-30.

Recommendation 7. Assess the sensitivity/criticality of the system and data using FIPS 199 and include the findings in the security plan.

9 Least Privilege

Least privilege is a basic underlying principle for securing computer systems and data. Applying least privilege means that users are granted only those access rights and permissions they need to perform their official duties. Organizations establish access rights and permissions to restrict the access of legitimate users to only the specific programs and files that they need to do their work.

The OIG reviewed access controls over the agency's personnel and financial databases. The FTC relies on the Department of Interior's National Business Center (NBC) to provide these support services to the FTC. The systems housing this sensitive data are located in Denver CO, although FTC personnel in Washington DC have a direct link to the data. The OIG reviewed both staff and ITM access.

FTC timekeepers have direct access to the Federal Personnel and Payroll System (FPPS) at NBC in order to enter biweekly time and attendance data. Conversely, few FTC staff outside the Financial Management Office (FMO) have access to the Federal Financial System (FFS), the agency's automated accounting system.

While access to the mainframe is limited, many staff have direct and indirect access to the same data via the FTC's "data warehouse." Each night, updated data is transferred from NBC to the FTC. The information is then available to managers as a means to manage programs and operations. The application used to prepare and organize the data into usable reports is Business Objects.

Both FPPS and FFS house sensitive data. The data warehouse, by virtue of the fact that it is a copy of real data, is as sensitive as the data at NBC. Hence controls over both need to be commensurate with the risk and outcome of exposing the data.

The OIG found that controls are generally in place to limit access to only those individuals who need NBC real time and FTC warehouse access. On the other hand, the OIG also found vulnerabilities associated with access by ITM staff to select information in the data warehouse.

9.1 Payroll Data Access Controls

To obtain FPPS access, employees must submit a FTC DOI Mainframe Computer and Federal Personnel/Payroll System FPPS Access Request Form, which identifies the requested role.[5] The employee's supervisor signs the form and submits it to the Director of Human Resources, who is the HR

[5] Roles define what data sets the user can access.

Data Custodian, for approval. The HR Security Point of Contact (SPOC) notifies the NBC to open a new account.

To remove accounts, HR staff generate bi-weekly separation reports to identify individuals who left the agency and compares this report to a list of FPPS access holders. Individuals (accounts) appearing on both lists are removed from the FPPS system.

9.2 Federal Financial System Controls

According to the FTC SPOC for FFS, the system has two layers of security. The first layer is the front end ID that allows users to access the DOI mainframe where the FFS applications reside. The second level of security is a separate FFS user ID that controls access to the FFS. The FFS user ID enables users to view and work with FFS data including to add, modify, and delete data within the FFS.

9.2.1 Access To FFS

The Assistant CFO for Finance is the Data Custodian for the FFS. The Data Custodian reviews access requests for the FFS and provides the SPOC with a list of approved personnel. The SPOC then completes and sends an electronic ASC-14 form to DOI. DOI creates the accounts and assigns a front-end ID. The SPOC can request accounts from DOI but cannot grant the access.

To remove accounts, the FFS SPOC reviews user lists provided by ITM on a quarterly basis to identify any unneeded user accounts.

9.3 FTC Data Warehouse

The data warehouse (warehouse) is an FTC Oracle database where authorized users can view data. While all FTC employees are assigned an Oracle ID, a user must first submit a request for access to a particular data universe (see below). The universe owner then approves or denies the request. If the request is approved, the business object supervisor is notified and grants the requestor access to the data universe.

9.3.1 Oracle Database Security

There are two layers of security that protect the Oracle database:

1. Users must first have access to the database itself. This provides access to the Oracle database. ITM provides the Oracle access.

2. Users must then have access to the universes of data or data objects. These universes include but are not limited to Personnel, FFS, STAR, FFS Detail, and FTC BUY. Business objects reside under Oracle and are used to set up the data universes.

Finding: IT Personnel Are Provided Unneeded Privileges in FPPS/FFS

The FTC uses FPPS and FFS personnel, payroll and financial transaction data to plan, implement and monitor agency programs and operations. To assist staff when technical glitches arise in the viewing of downloaded data, ITM has appointed a "data advocate" to assist FFS/FPPS SPOC's. The advocate works primarily on problems arising due to software malfunction when manipulating data in the warehouse and data processing errors. The prior ITM advocate had access to the DOI mainframe computer, which the current advocate does not have. The expanded privileges enabled the former advocate to perform downloads to compare mainframe data with warehouse data when glitches occurred. The new advocate does not perform this function.

The current ITM advocate has the following roles in the data warehouse: COMPRIZONBUY_RO, FFSDETL_RO_BO, FFS_RO, FFS_RO_BO, AND FTCDOWNLOADS role. These roles effectively provide him access to all finance, procurement, budget and personnel information in the warehouse. The

FTCDOWNLOADS role provides INSERT, UPDATE, DELETE and SELECT privileges on the HR combine file, HR payroll file, and the daily financial download file. The roles FFSDETL_RO_BO, FFS_RO, FFS_RO_BO are redundant in that collectively they provide SELECT access to HR payroll and daily financial download information. However, if the FTCDOWNLOADS role were revoked, the advocate would still have considerable access to information.

In our discussions with the SPOC for FFS and FPPS data, the OIG learned that the advocate was provided these roles to perform research into the cause and solution for unusual data processing errors. However, the research referred to is generally the responsibility of the application owner, not the ITM advocate. For example, occasionally a glitch may occur when data is (automatically) downloaded in to the warehouse from DOI. When this happens, program staff, not the advocate, manually download (or "insert") the file into the data warehouse. On the rare occasions that the files have been downloaded but the reconciliation still indicates that the files are not in sync, then further research is performed – again by FMO staff. These steps require access to both the FFS mainframe data and the warehouse via the FTCDOWNLOADS role. But as stated above, the advocate does not have access to mainframe data. Hence, giving the advocate access to personnel data via the FTCDOWNLOADS role, for example, unnecessarily gives the advocate access to privacy data. He does not need this access to perform his advocate responsibilities.

Another role of concern is the STAR_SA role. This role is the STAR system administrator role and provides the advocate complete access control of the STAR application. Again, only the STAR Administrator and a designated back up (not the advocate) should be assigned this role. The rationale provided was again to perform research.

The OIG believes that the advocate was provided these roles because the prior advocate had them – along with mainframe access. However, the current advocate does not have access to the mainframe data, and thus cannot do the research (and fix the glitches) for which he was provided the roles.

OMB A-130 requires that organizations incorporate personnel security controls such as separation of duties and least privilege. Additionally, SP 800-33, Underlying Technical Models for Information Technology Security, identifies least privilege as an example of system protections. The effect of this condition is that personnel may be able to access and manipulate data they should not be able to view or modify.

Recommendation 8. The FMO SPOC for FFS review user access privileges and assign only the roles and privileges needed to perform the advocate's duties and responsibilities.

10 FTC Scan Review

OIG evaluated FTC's scanning policy and procedures to determine how effectively ITM's Operations Assurance Branch (OA) is scanning, tracking, and correcting vulnerabilities. At the time of the review, OIG found that ITM is running full scans of the FTC network on a nightly basis. ITM utilizes a variety of spreadsheets and tools to track the testing, approval, and implementing of patches on FTC systems. These tools include:

FTCPatchTracker.xls: This is a spreadsheet that tracks the status of patch testing and its implementation. The spreadsheet tracks the status of patch testing for Windows servers, Call Manager servers, Unity servers, Windows workstations, Oracle, network devices, Unix servers, and printers.

Windows Server Patch Report.pdf: ITM uses this tool to track and report on the patches implemented on Windows servers.

Windows Workstation Patch Status.xls: This spreadsheet lists the status of patches applied to FTC workstations.

To apply patches OA submits a request to apply baseline patches after a scan is run and vulnerabilities are identified. OA monitors the remediation process to make sure the remediation process is on track. After the patches are applied (which is generally before the time has expired), OA scans for compliance. If any devices are out of compliance, OA notifies Operations and it has until the next maintenance window (every Thursday evening or monthly maintenance weekend which ever is sooner) to apply the patch. OA then rescans. If the patch is not applied, a POA&M entry is created.

ITM modified its POA&M reporting process for tracking scan-related vulnerabilities. Scan-related vulnerabilities are not posted to the POA&M until they are out of baseline (when the vulnerability is not patched within the time period allotted to correct the vulnerability).

ITM has documented scanning and patch management policies. The scanning policy requires that assets with the highest exposure be scanned more frequently and more intensely than other less exposed assets. It also states that assets in the Demilitarized Zone (DMZ), routers and switches inside the firewall, and FTC-owned computers are to be scanned monthly. The policy also discusses denial of service activities, investigation authorities, and corrective actions.

The Patch Management Policy describes the patch management process. The policy identifies the patch groups that correspond to Infrastructure Operations functional groups; discusses the risk classifications to security and patch notifications and the response times associated with each risk classification category.

Finding: OA does not perform trend analysis reports to track when vulnerabilities are identified and corrected.
At this time OA has no easy way of tracking the progress of correcting vulnerabilities. The reason for this is that the scanning software does not have a trend analysis reporting capability. This means that OA has to use different methods for tracking progress of correcting vulnerabilities that may not be as informative. They may be overlooking serious vulnerabilities that need to be corrected. One possible solution, for instance, is to develop a trend analysis report that provides personnel with the capability to track how effectively vulnerabilities are being corrected.

Recommendation 9 ITM should develop a means to track and identify when scan vulnerabilities are detected and corrected.

Finding: Full vulnerability scans may be run too frequently.
Although there are documented scanning and patch management policies, ITM reported to the OIG in a March 16, 2005 meeting that it was having problems tracking and correcting vulnerabilities. ITM informed the OIG that it was modifying its reporting procedures for listing vulnerabilities on the POA&M. ITM runs full scans on a nightly basis. ITM is identifying vulnerabilities already identified by earlier scans and is experiencing difficulty trying to track and remediate vulnerabilities. ITM may need to adjust its scanning policy and schedule. One possible way to address this problem is for ITM to run full-scans on a regular, but less frequent, basis. Instead, ITM could run specialized scans, such as the FBI SANS Top 20 or custom scans with newly identified vulnerabilities, between full scans.

Recommendation 10. ITM should evaluate the type and frequency of scans to determine if there are more efficient ways to scan FTC IT resources.

11 POA&M Analysis

11.1 General Overview of FTC's POA&M Process

Based upon the findings of the fourth Quarter FY 2004 through second quarter FY 2005 POA&M review (OIG report AR 05-066) and the third quarter FY 2005 review conducted for this task, ITM's POA&M management program continues to mature. Overall POA&M tracking and reporting is being completed in accordance with FISMA guidance and the POA&M includes findings from other security studies. Additionally, the OIG is involved in the POA&M process. The OIG periodically reviews completed POA&Ms and provides guidance to ITM on how to improve the POA&M process. Since the submission of last year's FISMA independent evaluation, ITM reported and the OIG verified the completion of actions that corrected 51 weaknesses. FTC is also submitting its quarterly reports to OMB in a timely manner.

Finding: POA&M list does not prioritize IT security weaknesses.

FISMA guidance recommends that agencies prioritize the weaknesses on the POA&M to help ensure that significant IT weaknesses are addressed in a timely manner and receive appropriate resources. The OIG could not locate a column or code to indicate a priority level associated with correcting vulnerabilities. Not prioritizing weaknesses on the POA&M makes it difficult to identify critical weaknesses that should be addressed sooner than other less critical vulnerabilities.

Recommendation 11. Prioritize IT security weaknesses in the POA&M.

11.2 Third Quarter FY 2005 Quarterly Reporting

OIG confirmed, with two minor exceptions, that ITM is using the POA&M process to record, track, and clear corrective actions.

12 Privacy Review

Federal law requires agencies to protect data containing personally identifiable information and the systems containing this data. The OIG evaluated this area several ways. First, the OIG validated a sample of responses to the Privacy Officer OMB Questionnaire. Second, the OIG ran a Watchfire WebXACT test of the FTC website to identify possible privacy vulnerability issues. Finally, the OIG evaluated how effectively FTC is monitoring the privacy for their CommentWorks system. The results of the review are discussed below.

12.1 Privacy Officer Questionnaire Review

OIG reviewed the Privacy Officer Questionnaire (See Section D of the OMB FISMA Report) to validate the FTC Privacy Steering Committee's responses to these questions. ITM was able to provide references to documentation that validated its answers.

12.2 FTC Website Scan

According to the Privacy Steering Committee's meeting write-up of July 21, 2005, a web scan was conducted in May. According to the meeting minutes, identified errors were corrected. Scans are run on a quarterly basis.

12.3 CommentWorks Privacy Review

The OIG evaluated the privacy controls for CommentWorks because the system collects personally identifiable information on individuals and organizations that provide comments on pending legislation.

This information includes names, addresses and phone numbers. Review of the scan reports validated that ICF Corporation (ICF) is conducting vulnerability scans on CommentWorks servers and that FTC has access to the reports so it can review the security of the servers.

The OIG also reviewed the Blanket Purchase Agreement (BPA) that was prepared for FTC and ICF. The BPA describes the roles and responsibilities of the FTC and ICF with regard to the performance and availability of CommentWorks. The BPA states that all personally identifying information (PII) for individuals must be redacted. No redaction is required if the comments come from a business or organization. The BPA identifies deliverable and data access schedules and timeframes established by the FTC, by which ICF must have paper and electronic comments available for review and web posting. ICF and FTC contact information is also provided.

The BPA addresses security requirements for CommentWorks on a high level. For example, the BPA requires that FTC data not be divulged to any unauthorized person for any purpose. The contractor is required to obtain approval from the FTC Contracting Officer's Technical Representative (COTR) prior to the public release of information on orders under the BPA. ICF employees who work with FTC data must sign non-disclosure agreements.

In terms of physical security, the BPA states that data systems developed and operated by the contractor must be designed to protect data from unauthorized access. The contractor is responsible for creating, maintaining, and disposing of only those records that are specifically listed in the Statement of Work (SOW). Upon request of the COTR, the contractor is required to provide the original record, or a reproducible copy of such record, within three working days of receipt of the request.

The BPA also requires that the system meet the requirements of Section 508 of the Rehabilitation Act of 1973 and related amendments to the extent possible. Section 508 requires that the agency ensure that technology developed, procured, maintained, or used by the agency allows individuals with disabilities to have access to and use of information and data that is comparable to the access and use provided to members of the public who are not individuals with disabilities, unless an undue burden would be imposed on the agency; in such cases, individuals with disabilities must be provided alternative means of access that allows them to use the information and data.

The BPA also states that the government may request, and the contractor shall provide upon request, full and immediate access to and custody of all public comments or other information or data compiled for or generated on behalf of the government by the contractor and any of its employee, agents, or subcontractors under the BPA. Finally, the BPA discusses breach of contract and applicable Federal Acquisition Regulation (FAR) clauses.

Since FTC is purchasing a service from ICF, the BPA adequately addresses the areas of privacy protection, security, and Section 508 compliance.

13 E-Authentication

In December 2003, OMB issued E-Authentication guidance to all Federal agencies, addressing those Federal government services accomplished using the Internet . To make sure that online transactions are secure and protect privacy, some type of identity verification or authentication is needed. OMB requires federal agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurances. OMB also directs agencies to conduct "e-authentication risk assessments" on electronic transactions to ensure that there is a consistent approach across government. The OIG met with ITM to determine if an e-authentication risk assessment was conducted for the agency.

Finding: The agency has not conducted system e-authentication risk assessments.
OMB Memorandum M-4-04, *E-Authentication Guidance for Federal Agencies*, December 16, 2003 states that agencies should determine assurance levels using the following steps:

1. Conduct a risk assessment of the e-government system
2. Map and identify risks to the applicable assurance level
3. Select technology based on e-authentication technical guidance
4. Validate that the implemented system has achieved required assurance level
5. Periodically reassess the system to determine technology refresh requirements

ITM reported that it plans to include e-authentication risk assessments when it updates system risk assessments. Without e-authentication risk assessments, the FTC is not able to map identified risks to the applicable assurance level and, therefore, is unable to select technology based upon e-authentication guidance.

14 Background Investigations

FTC Administrative Manual, Chapter 4, Section 820 establishes general policies and procedures for administration of the Personnel Security and Suitability Program for the Agency. These policies and procedures apply to employees in all permanent positions, as well as applicants for employment, contractors and individuals employed for 180 days or more.

With few exceptions, all FTC appointments are subject to a background investigation. The scope of the investigation depends on the sensitivity/risk level of the position as determined by the degree of risk to the public trust. Individuals selected for IT positions are subject to investigations commensurate with the sensitivity of the data to be handled and the risk and magnitude of loss or harm that could be caused.

ITM staff generally undergo National Agency Checks with Inquiries Investigations (NACI) or a Minimum Background Check (MBI). A NACI is conducted for low-risk positions. These investigations include a National Agency Check, written inquiries, and record searches covering specific areas of a subject's background during the past five years (60 months). An MBI, on the on the other hand, is somewhat of a misnomer in that the background check is more in depth than a NACI, as it includes a personal interview with the subject. MBI's are to be updated at least every seven years (84 months).

The Office of Personnel Management (OPM) performs the investigations for the FTC. Investigative results are provided to the FTC security office. The FTC Security Officer considers all the information of record, both favorable and unfavorable, and assesses its relevance, recency, and seriousness and makes an adjudication based on OPM adjudication guidelines, applicable laws, and regulations. Final adjudicative

determination is based on considerations of whether the conduct of the person either would, or would not, promote the efficiency of the Federal service and/or the National Security.

The OIG reviewed background checks for all ITM employees to assess compliance with FTC background investigation policy – specifically whether employees have received investigations within the timeframes required by the OPM.

Finding: Background Checks for some ITM employees are outdated.
The OIG found that many ITM employees, some with significant data access responsibilities, have not undergone updated background checks for months and sometimes years beyond federally recommended intervals. As of August 23, 2005, 32 of 45 ITM employees 71 percent had completed background investigations that were less than five years old. Twelve employees (27 percent) had completed investigations that were completed between 71 months and 360 months ago.[6] The OIG identified six of the 12 employees as having significant data access privileges and responsibilities. One ITM employee refused to submit to a background investigation.

Requiring investigations every five years helps to identify conditions that could lead ITM to limit access to certain data, or may even make the employee unsuitable for continued employment. Some conditions or occurrences that could go undetected in the absence of an up-to-date investigation include the following:

- Criminal or dishonest conduct
- Intentional false statement or deception or fraud in examination or appointment
- Misconduct or negligence in prior employment
- Alcohol abuse
- Illegal use of narcotics, drugs, or other controlled substances
- Statutory and regulatory bar
- Knowing and willful engagement in acts or activities designed to overthrow the United States Government by force

The OIG provided the names of the twelve employees to the FTC information security officer to determine whether access privileges should be curtailed pending an updated background check.

Recommendation 12. The OIG recommends that Administrative Services Office schedule background investigations for the 13 IT employees lacking up-to-date investigations. The OIG further recommends that the six individuals with significant data access be performed first.

15 Southwest Regional Office Review

As part of this year's FISMA evaluation, the OIG performed an on-site review of the FTC's SWRO in Dallas, TX, during the week of June 20, 2005. The objectives of this review were to assess how well FTC policies and procedures are being implemented and to evaluate security observations and conditions against industry and NIST best practices.

The SWRO is located in the Harwood Center, a 26-story building constructed of steel and concrete. The building was built in 1982. The SWRO is located on the 21st floor of the building. The firm Taylor &

[6] The distribution, in months of the age of the most current background investigation for the 12 ITM employees follows: 71, 103, 113, 122, 144, 146, 147, 148, 152, 175, 183, and 360 months.

Mathias is responsible for facilities management. FTC leases approximately 10,000 square feet of commercial space that was obtained through GSA.

15.1 1999 Bryan Street Building Security

Residents of the building include commercial and government organizations. The building is open to the public between 6:30 AM and 6:00 PM. A card key is required to gain access to the building and to use the elevators during non-business hours. The lobby has a guard desk staffed around the clock. During business hours, guards at the guard desk will generally notify the FTC when someone is visiting the suite. There is also a visitor sign-in sheet at the guard desk. Closed circuit cameras are positioned outside and inside the facility to detect suspicious activity. The building contains standpipes to aid in fire control. Fire inspections are conducted by the fire department annually and fire drills are conducted quarterly. Smoke detectors are located in air ducts, common areas, freight elevators and electrical rooms.

Heating, Ventilation and Air Conditioning (HVAC) systems are maintained regularly. The coil and filter are replaced annually. Chillers are maintained annually per manufacturer's specifications. Thermo imaging is performed annually on the building's main electrical system. There is a backup generator for limited building components. This does not support the computer room. Taylor & Mathis reported that an Emergency Response Plan was developed in June 2004. However, the SWRO did not maintain a copy of this document.

The OIG identified other physical security vulnerabilities that were outside the scope of the IT security evaluation. We provided these observations to the FTC's physical security officer in preparation for his September 2005 site visit to the SWRO.

15.2 FTC Southwest Region Suite

The FTC SWRO resides in suite 2150. An electronic cipher lock on the main door and mechanical cipher locks on the other exterior doors control access to the suite. The room where visitors enter the suite restricts access to the rest of the suite. Two fire alarm switches are located in the public hallway area of the floor. Two small fire extinguishers capable of extinguishing A (paper), B (combustible or flammable liquids), and C (electrical) type fires are located in the stairwells. An additional Halon fire extinguisher is located in the suite. The doors to the stairwells cannot be opened from inside the stairway. One vulnerability was identified.

Finding: There is no contingency plan for the SWRO.

Title III of the E-Government Act (FISMA) states that "an organization's information security program should include plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency." National Institute of Standards and Technology Special Publication 800-37 (SP 800-37) *Contingency Planning Guide for Certification and Accreditation of Federal Information Systems* provides guidance for developing contingency plans. Not having a current contingency plan that has been tested could delay and hinder recovery operations.

The headquarters' contingency plan discusses offsite backup storage for tapes and shipment schedules. It also identifies the regional offices by name and address and describes the effects on regional offices should a catastrophic failure occur at the headquarters data center. The OIG found no guidance or plans regarding what needs to be done in the event of catastrophic failure at regional offices. For example, existing guidance does not identify (i) procedures for replacing hardware and software at the region should the equipment be destroyed by an event that occurs at the region, (ii) who to contact if the computer room or hardware are destroyed or damaged, (iii) procedures for procuring, building and shipping replacement equipment, (iv) how to create and deploy a recovery team to go to the region to restore operations, and (v) references to instructions or guidance for working from an offsite location (like home).

Recommendation 13. ITM should assist the SWRO in developing a contingency plan for that office. ITM should also ascertain whether contingency plans are in place at other FTC regional offices. If they are not, then plans should be developed.

15.3 Computer Room

The computer room is located in the FTC suite and is inaccessible to the public. The computer room contains two Windows servers, a CISCO Systems switch, ROLM 9200 Phone Mail SP system and an APS SmartUPS and battery. One of the Windows servers is an Exchange server and the other is a Domain Controller. Other hardware in the computer room includes:

- Snap server storage device
- Tape Backup Unit
- PBX
- Routers
- Printer

Vulnerabilities associated with the computer room are:

Finding: Cooling and ventilation for the computer room is inadequate.
Failures of electric power, heating and air-conditioning systems, water, sewage, and other utilities will usually cause a service interruption and may damage hardware. NIST SP 800-18 states that organizations should ensure that these utilities, including their many elements, function properly. The OIG noted that the door to the computer room must remain open because the HVAC system does not properly cool the room. Additionally, there is no backup HVAC system to maintain a safe operating temperature for the equipment in the event the primary HVAC system fails. As a result, the computer room cannot be secured because the door cannot be closed and locked.

Recommendation 14. ASO should work with GSA to evaluate the practicality of improving cooling and ventilation in the computer room. ASO and GSA will first need to determine if the recommendation is cost effective and develop requirements for maintaining a safe operating environment for the computer room.

Finding: Plumbing lines may affect computer room operations should they rupture.
NIST SP 800-17 states that organizations should know the location of plumbing lines that might endanger system hardware and that steps should be taken to reduce the risk associated with this vulnerability. Taylor & Mathis officials reported that they are aware of the location of the plumbing lines and agreed that they could potentially disrupt computer room operations and disable the network should the lines rupture.

Recommendation 15. ASO should identify ways to protect equipment in the server room from water damage. One option would be to place plastic covers in the computer room. Another option would be to install moisture detectors that would shut-off power to the hardware when water is detected.

Recommendation 16. The SWRO should maintain an updated list of emergency numbers, that include building management, to speed the response to water leakage and other emergencies.

***Finding:* There is no emergency power shut-off switch for the computer room.**
NIST SP 800-18 states that systems and the people who operate them need to have a reasonably well-controlled operating environment. Not having an emergency power shut-off switch for the computer room may lead to hardware damage and personal injury in the event of an emergency situation such as a fire or water release.

Recommendation 17. ASO should evaluate the feasibility of installing an emergency power shut-off switch in the computer room.

***Finding:* The computer room is not secured.**
NIST SP 800-18 states that physical access controls should address not only the area containing system hardware, but also locations of wiring used to connect elements of the system, supporting services (such as electric power), backup media, and any other elements required for the system's operation. It is important to review the effectiveness of physical access controls in each area, both during normal business hours and at other times -- particularly when an area may be unoccupied. At this time the door to the computer room must remain open at all times in order to maintain a safe operating temperature for the equipment located in the computer room. The effect of this condition is that the computer room is accessible to personnel who do not have a need to access the area.

Recommendation 18 ASO should secure the computer room if the HVAC climate control issue can be resolved.

***Finding:* The computer room does not have a fire extinguisher.**
SP 800-18 states that it is important for organizations to evaluate the fire safety of the buildings that house computer systems. There is no fire extinguisher capable of extinguishing A, B, or C type fires in the computer room. The room is equipped with a sprinkler system. Fires may get severe enough to activate the floor-wide sprinkler system, and thus cause more property damage and extend business interruption. A portable extinguisher would delay or prevent such an occurrence.

Recommendation 19 The SWRO should install a fire extinguisher capable of extinguishing, at a minimum, A and C type fires in the computer room.

15.4 Regional Office IT Operations

According to IT Operations personnel, administration of the servers is handled remotely. There are three Remote Insight Boards (RIBs) connected to the servers that system administrators in Washington can use to access the servers. These boards are directly connected to a power source so the servers can be completely shutdown and rebooted remotely. Each regional office has a technical liaison that is responsible for assisting ITM to physically access the system. The technical liaison is also responsible for switching backup tapes. Differential backups are conducted nightly and full backups are conducted weekly. Backups are taken offsite on a regular basis.

Configuration Management for regional office devices is centralized through ITM. Servers are built at headquarters and shipped to the regions. There are no maintenance schedules or logs for the specific servers. ITM Operations designates a maintenance weekend and "pushes out" global upgrades to all same-type devices. (e.g., Windows 2000 servers). In the event of an IT security incident at a regional office, the Headquarters Computer Incident Response Team (HQ CIRT) would be notified. If an incident

were reported, the response team would assemble and analyze the problem, perform remote diagnostics, and then respond to the incident.

15.5 Summary Of Findings From Interviews With The SWRO User Community

As part of the site visit to the SWRO, the OIG interviewed the regional office's user community. Generally, the interviews revealed that the user community is aware of and follows FTC policies and procedures. This includes logging off and rebooting workstations, taking steps to properly handle sensitive data, and knowing who to contact in the event of IT security incidents. Additionally, personnel backup important data stored on local hard drives. Several vulnerabilities or areas that need improvement were identified.

Finding: New files, diskettes, and downloaded files are not always scanned and checked for viruses prior to use

NIST SP 800-18 requires documented procedures for automatic and manual scans. ITM policy ITM-2004-15, *Anti-Virus Policy,* states that all ITM-issued workstations and ITM-managed servers, whether connected to the FTC network or standalone, must use virus protection software configured and approved by ITM. ITM-2005-09, *Litigation Anti-Virus Policy* requires that any litigation data from external sources be cleansed per the requirements identified in the policy document.

The review found that a number of users do not scan new files or diskettes prior to loading them on their systems. Some individuals reported that they send electronic storage media to the Litigation Support or the regional office technical liaison so the media can be scanned for viruses, but these individuals tended to be the exception. Not scanning files or electronic media for viruses could cause new viruses or malicious code to be introduced to the FTC computing environment. Data may be destroyed or damaged and system performance may be hindered.

Recommendation 20. ITM should remind all FTC staff of the policies requiring testing of all newly received media. One approach would be to use the FTC Daily to communicate the requirement.

Finding: Law clerks (law students interning at the FTC) do not receive annual security awareness training.

Office and Management and Budget (OMB) Circular A-130, *Management of Information Resources, Appendix III,* states that organizations need to "ensure that all individuals are appropriately trained in how to fulfill their security responsibilities before allowing them access to the system." ITM-2004-04, *Information Security Training & Awareness Policy,* states that the FTC "will implement and maintain an IT security training and awareness program that ensures that all staff and contractors receive information technology security training appropriate to their level of responsibility for the protection of FTC information and information resources." The law clerks interviewed during the SWRO site visit reported that they have not received information security awareness training. These law clerks have access to FTC IT resources. This raises the possibility that clerks may be unaware of and do not follow FTC policies and procedures. This could put FTC IT resources at risk for viruses, loss or disclosure of data, or misuse.

Recommendation 21. The SWRO should ensure that all FTC personnel including full- and part-time employees, volunteers, and interns receive security awareness training before granting them access to the FTC IT resources.

15.6 Logical Access Controls for the Regional Office

Access control was evaluated during the visit. Users are given user IDs and passwords and are instructed not to share passwords with others. Interviews with personnel indicated that they either log off their

computers or rely on the 15-minute inactivity timeout to lock their workstations when they leave their workstations. Users also change their passwords every 90 days. One vulnerability was identified.

Finding: The access control list is not up to date.
According to OMB A-130, management controls such as individual accountability requirements, separation of duties enforced by access controls, or limitations on the processing privileges of individuals, are generally more cost-effective personnel security controls than background screening. Such controls should be implemented as both technical controls and as application rules. SP 800-18 states User IDs that are inactive on the system for a specific period of time (e.g., three months) should be disabled. According to ITM-2004-07, *Inactive Accounts Policy,* FTC system administrators are required to regularly identify, disable, and purge inactive accounts in a timely, coordinated manner.

Comparison of the SWRO employee list with the Access Control List (ACL) provided by ITM found that the ACL was not up to date and contained errors. Three individuals on the ACL are no longer with the organization. Of the three, two individuals recently retired, and the third was a volunteer who left the organization on May 6, 2005. The OIG also identified two individuals listed on the ACL who never worked at the SWRO. The names of these staff were reported to ITM for appropriate action.

The Helpdesk is responsible for notifying Infrastructure Operations (Operations) when an account is to be deactivated. After disabling the account, Operations then sends an e-mail to Administrative Officers, COTRs, Helpdesk, and CICOM staff identifying the disabled accounts, the planned purge date, and the procedure to reactivate the account in the event the account was incorrectly disabled. Additionally, the Operations staff identifies and immediately disables inactive Windows LAN accounts on a monthly basis. Failure to timely inactivate accounts provides potentially malicious individuals with an unauthorized portal to the FTC network environment.

Recommendation 22. ITM should send copies of ACLs to Regional Office management on a quarterly basis to ensure that the ACL is accurate and updated in a timely manner.

16 Penetration Testing and Wireless Network Detection

The OIG performed a penetration testing and vulnerability assessment of the FTC external computer network, dial-in phone line, and internal wireless network in support of the Federal Information Security Management Act (FISMA) FY 2005 Independent Evaluation. The OIG performed the testing activities from a remote location in Bethesda, MD and at the FTC facilities in Washington DC. The findings identified in the report were found during the period of September 13, 2005 through September 23, 2005.

The objective of the testing was to document the security risk posture associated with the FTC's Internet presence, dial-in, and wireless networks The testing did not detect any wireless networks in operation within the FTC environment, consistent with FTC's ban on such networks. On the other hand, the penetration test identified two medium risk and four low risk vulnerabilities. These vulnerabilities are discussed in detail in a non-public report to management. Results were shared with the FTC's Information Security Officer when they were detected. Management took immediate steps to address the vulnerabilities.