Office of Inspector General

Independent Evaluation Report

Review of Federal Trade Commission Implementation of the Federal Information Security Management Act For Fiscal Year 2004

October 6, 2004

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 2004. 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 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.

The OIG independent evaluation (i) reviewed the implementation of the Federal Trade Commission (FTC) information security program; (ii) assessed agency progress towards correcting weaknesses addressed within the 2004 Plan of Action and Milestones (POA&M); (iii) verified and tested information security and access controls for the General Support System, the Federal Financial System and the Premerger System, and (iv) evaluated FTC's vulnerability assessment scanning and remediation program.

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.

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; and
2. Test the effectiveness of information security policies, procedures and practices on a representative subset of the agency's information systems.

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) made extensive progress in developing a mature information security program, and has implemented or addressed OIG-

identified security vulnerabilities discussed in the fiscal year (FY) 2003 Independent Evaluation report. For example the FTC:

- Certified and accredited three of its Major Applications and General Support Systems (GSS).
- Completed 25 of the 91 issues identified in the POA&M, with plans to address the remaining 66 issues.
- Made improvements in its POA&M tracking and reporting process.
- Developed policies and procedures that addressed various security issues.
- Developed a scanning and remediation program for system vulnerabilities.
- Modified the inventory to include interconnections to other systems.

As a result of these actions, the OIG believes that the FTC continues to make steady progress in the development of a mature security program in accordance with FISMA requirements.

In a memorandum to agencies and inspectors general, the OMB-provided guidance on FISMA implementation and reporting. As part of this guidance, OMB requires agencies to identify and report on "significant deficiencies" in their information security programs. OMB defines a significant deficiency as 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, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate corrective action must be taken. A significant deficiency under FISMA is to be reported as a material weakness under the Federal Managers Financial Integrity Act (FMFIA).

Unlike in prior years the OIG found no significant deficiencies this year. However, the OIG identified several findings that merit management's attention. These various conditions are discussed in the body of the report.

TABLE OF CONTENTS

Evaluation Summary i

1 Background 1

2 Purpose 1

3 Scope and Methodology 1

4 Certification and Accreditation Findings 2

4.1 Certification and Accreditation (C&A) 3
4.2 C&A Package Review 4
4.3 Security Plans 5
4.4 Risk Assessments 7
4.5 Privacy Impact Assessments 8

5 Independence 9

6 Security Policies and Procedures 10

6.1 Policy Development 10
6.2 Review of the FTC Administrative Manual Chapter 1 11
6.3 Media Handling Policy 12

7 Security Awareness Training 13

8 Security Incident Response 13

9 Continuity of Operations Planning 14

9.1 Disaster Recovery Plan 14
9.2 Memorandums of Agreement (MOA) and Memorandums of Understanding (MOU) 15

10 Plan of Action and Milestones (POA&M) 16

11 Miscellaneous Findings 17

11.1 Separation of Duties 17

12 Testing 17

12.1 Internal and External Vulnerability Assessment 17
12.2 Logical Access Controls 18
12.3 Managerial Access Controls 19
12.4 Controlling Access for Interagency Transfers 20
12.5 Access to Test Data 21

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 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.

The Office of Inspector General (OIG) independent evaluation (i) reviewed the implementation of the Federal Trade Commission (FTC) information security program; (ii) assessed agency progress towards correcting weaknesses addressed within the 2004 Plan of Action and Milestones (POA&M); (iii) verified and tested information security and access controls for the General Support System (GSS), the Federal Financial System (FFS), and the Premerger System, and (iv) evaluated FTC's vulnerability assessment scanning and remediation program.

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; and
2. Test the effectiveness of information security policies, procedures and practices of a representative subset of the agency's information systems.

3 Scope and Methodology

The scope of this independent evaluation of the FTC FY 2004 information security program included:

- Review of FTC major applications and general support systems
- POA&M review for completeness and accuracy
- Security controls testing

The OIG reviewed the following FTC systems and/or system components in detail:

- GSS (FTC Enterprise System and E-mail)
- Hart Scott Rodino Premerger Tracking System Including Electronic Filing Process (Premerger)
- Federal Financial System (FFS) owned by Department of Interior. FTC OIG also relied on DOI OIG's *Review of Information System Security Over Systems & Applications used by the National business Center to Provide Services to Non-Department of Interior Clients* (Report No. A-EV-OSS-0094-2004) for this portion of the study.

The OIG did not review physical security controls in this evaluation.

To accomplish the review objectives, the OIG conducted interviews with Information and Technology Management (ITM) staff, including the Chief Information Officer (CIO), the Senior Agency Information Security Officer, other members of the CIO staff and FTC program officials. The team reviewed documentation provided by the FTC including security plans, risk assessments, the Disaster Recovery Plan (DRP), Certification and Accreditation (C&A) packages, Privacy Impact Assessments and other security related policies. The OIG also reviewed ITM's vulnerability scanning and remediation program.

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

- Office of Management and Budget (OMB) Memorandum M-04-25, *Reporting Instructions for the Federal Information Security Management Act* (8/23/04)
- National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18, *Guide for Developing Security Plans for Information Technology Systems*, December 1998
- NIST (SP) 800-26, *Self-Assessment Guide for Information Technology Systems,* August 2001
- NIST SP 800-30, *Risk Management Guide for Information Technology Systems*
- NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*
- 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
- The 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 May 27 and September 20, 2004.

4 Certification and Accreditation Findings

The OIG found that ITM made extensive progress in developing a mature information security program, and has implemented or addressed OIG-identified security vulnerabilities discussed in the fiscal year (FY) 2003 Independent Evaluation report. For example the FTC:

- Certified and accredited three of its Major Applications (MA) and General Support Systems (GSS), and has made substantial progress in completing C&A's in the remaining four systems.
- Completed 25 of the 91 issues identified in the POA&M, with plans to address the remaining 66 issues.
- Made improvements in its POA&M tracking and reporting process.
- Developed policies and procedures that addressed various security issues.
- Developed a scanning and remediation program for system vulnerabilities.
- Modified the inventory to include interconnections to other systems.

In addition to these improvements, FTC also made improvements in other areas as well. As of mid-June 2004, the ITM Operations Section assumed responsibility for all production systems. Prior to this, developers had substantial privileges on production applications and data. All default system passwords

have been changed and Change Management procedures are used to manage changes to the system. Hardware is located in the FTC Computer Room. Software is stored in a locked room. All new and revised hardware and software are authorized, tested, and approved prior to implementation.

FTC also made improvements in the area of data integrity. Review of a workstation, mail server and firewall server indicated that all three of the devices had virus-scanning software loaded on them. For intrusion detection, the FTC purchased three Proventia devices and installed them on the FTC Infrastructure network.

Audit logs are now being used to track activity involving access to and modification of sensitive information or critical files. Audit logs are flagged to an e-mail. Oracle and Solaris logs are reviewed daily and Windows logs are reviewed on an as-needed basis. Premerger's log files are used for tracking all activity on the *Transactions and Amount Paid* tables. FFS external security and System Management Facility (SMF) provides comprehensive audit and reporting capabilities and FFS internal security (security logging options) provides audit capabilities.

Based upon a review of an independent assessment performed by the Department of Interior's OIG, it was determined that DOI's National Business Center (NBC), the organization responsible for the Federal Financial System (FFS), has security measures and procedures in place to control and track installation of, and updates to, this application. There is an automated configuration management and tracking system in place in the Financial Systems Division, NBC, for the management of the baseline FFS software components and file conversion routines which are supplied by American Management Systems via the Reston National Business Center.

Notwithstanding progress made by ITM in the areas identified above, the OIG found other areas where improvements are still needed. While no significant deficiencies were found according to the FY2004 definition provided by OMB, the OIG did identify the following reportable conditions. [1]

4.1 Certification and Accreditation (C&A)

OMB A-130, Appendix III, requires that major applications and general support systems undergo a security certification and accreditation review every three years or sooner if major modifications are made to the system.

The National Institute of Standards and Technology (NIST) Special Publication 800-37, *Guide for Security Certification and Accreditation of Federal Information Systems* (SP 800-37), states that the security certification package should contain a security plan (based on a risk assessment), a vulnerability assessment report, and a POA&M. The accreditation letter itself should contain the accreditation decision, supporting rationale, and terms and conditions. Further, OMB guidance states that for non-national security systems, development of an IT security program is to be consistent with NIST documents and Federal Information Processing Standards (FIPS). Any evaluation of the agency IT security program implementation should evaluate the consistency with NIST.

[1] 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.

Finding: Not all of the FTC's major applications and general support systems are certified and accredited.

Table 4-1 identifies the six major applications (MA), one general support system (GSS) and the security-related documentation available for review at the time of this evaluation. Systems identified in bold were reviewed by OIG in this year's FISMA review.

Table 4-1 – C&A Security Documentation

System Name	System Type	Risk Assessment Report	Security Plan	ST&E or Vulnerability Assessment Report	POA&M	Privacy Impact Assessment	C&A Letters
Documentum	MA	Draft	Draft	No	N/A	No	No
FFS	MA	Yes	Yes	Yes	Yes	Yes	Yes
MMS	MA	Draft	Yes	No	N/A	No	No
CIS	MA	No	Yes	No	N/A	No	No
Pre-Merger	MA	Yes	Yes	Yes	No	Yes	Yes
Do Not Call	MA	Yes	Yes	No	No	No	Yes
Infrastructure	GSS	Yes	Yes	No	N/A	No	No

At the time fieldwork was completed, three of FTC's major applications were certified and accredited (DNC, Premerger and FFS). Do Not Call and Premerger are owned and operated by the FTC. FFS, a Department of Interior system used by the FTC is owned and operated by the Department of Interior's National Business Center (NBC). ITM reported to the OIG that the remaining four applications are scheduled to have their C&A's completed by September 30, 2004.

Not having systems certified and accredited could result in systems going into the production environment with undetected and uncorrected vulnerabilities. These vulnerabilities could be exploited and the data and systems could be compromised.

Recommendation:

As the four systems that have not yet received a C&A are scheduled to have their reviews completed by 9/30/04, and as these weaknesses have already been placed on a prior POA&M, no OIG recommendation is necessary.

4.2 C&A Package Review

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)
- A security assessment report
- A POA&M

Additionally, the guidance states that all certifications and accreditations initiated after finalization of NIST Special Publication 800-37 must be consistent with 800-37. SP 800-37 was only recently finalized in May 2004.

Finding: C&A Packages do not fully conform to NIST 800-37 or FTC Certification and Accreditation Policy guidance.

FTC's current C&A policy, which closely monitors NIST guidance, was implemented June 30, 2004. It states that the C&A package should contain a system security plan, risk assessment report, a security testing & evaluation report (or vulnerability assessment report), privacy impact assessment (if required), System Plan of Action & Milestones and a certifier's statement. The C&A package contents required by NIST and FTC are summarized in table 4.2.

Table 4-2 – C&A Package Requirements

NIST C&A Package Requirements	FTC C&A Package Requirements
System Security Plan including related documents	System Security Plan
System Security Assessment Report	System Risk Assessment
POA&M	POA&M
	Privacy Impact Assessment
	Security Test & Evaluation Report

FTC accredited the Do Not Call system on July 1, 2004, contrary to agency policy. Specifically, the Do Not Call C&A package does not contain a Security Test & Evaluation (ST&E). The result of certifying and accrediting a system without thorough testing increases the possibility that the system may have gone into production with unidentified problems.

However, the C&A package for Do Not Call did contain a security plan, a risk assessment and an unsigned Memorandum of Understanding for AT&T Government Solutions Inc. The OIG did not take issue with the accreditation despite the missing documentation for two reasons. First, we felt that the quality of the Risk Assessment and the Security Plan was high. Secondly, according to the DNC POA&M, a systems test and evaluation is scheduled for completion on January 30, 2005.

Recommendation:

As management has recorded the weakness on the DNC system POA&M and has scheduled to complete the ST&E by January 30, 2005, no OIG recommendation is necessary.

4.3 Security Plans

According to NIST SP 800-18, the security plan should address:

- System Identification
- Interconnections to Other Systems
- Rules of Behavior
- System Sensitivity
- Management Controls
- Operational Controls
- Technical Controls

SP 800-37 states that the security plan can also include other security-related documents as supporting appendices or references. These documents include:

- Risk Assessment
- Privacy Impact Assessment
- Contingency Plan
- Incident Response Plan
- Configuration Management Plan
- Security Configuration Checklists
- System Interconnection Agreements

Finding: The security plans lack selected pieces of the information required by NIST SP 800-18, Guide for Developing Security Plans for Information Technology.

Security plans are in place for all FTC major applications, Infrastructure, and FFS. FTC has updated four plans which are pending certification: Infrastructure, MMS, Documentum, and CIS. Although, the security plans address many of the major areas identified in SP 800-18, review of these documents found that selected sections were not fully addressed. For example, review of the security plan for Infrastructure (*Federal Trade Commission Enterprise Network Security Plan*), found:

- Rules of Behavior (ROB) are not clear about the consequences of behavior that is not consistent with the rules; ROB do not include a statement and signature and date line that the user acknowledges receipt, understands responsibilities, and will comply with the rules; ROB signatures are not kept on file for all users.
- Data integrity controls, identification and authentication, logical access controls, and auditing are not discussed in sufficient detail.
- The email portion of Infrastructure is not discussed in sufficient detail.

The Premerger security plan addresses all of the areas that NIST SP 800-18 says should be addressed in a security plan with the exceptions of Security Awareness Training and Incident Response Capability. However, many of the areas addressed in the security plan are not addressed in detail. Review of the Premerger security plan identified the following two weaknesses:

- Rules of Behavior are not clear about the consequences of behavior that is not consistent with the rules; Rules of Behavior do not include a statement and signature and date line that the user acknowledges receipt, understands responsibilities and will comply with the rule; Rules of Behavior are not kept on file for all users.
- The identification and authentication section needs to discuss password controls.

The security plans were finalized and approved but were not reviewed by ITM for compliance with NIST SP 800-18.

Not having sufficient detail in the security plans makes it difficult for agency C&A officials to efficiently determine if a system contains all the necessary security controls. Again, not including sufficient security documentation as part of the security plan makes it difficult to gather all the required information to certify and accredit systems.

Recommendation:

1. OIG recommends that ITM develop security plans that include Rules of Behavior and which provide sufficient documentation to allow for an efficient C&A process.

4.4 Risk Assessments

OMB A-130, Appendix III, requires that risk assessments be performed on systems at least every three years or whenever the system undergoes a C&A and/or significant modification. NIST SP 800-30, *Risk Management Guide for Information Technology Systems*, August 2001, provides guidance on conducting risk assessments.

The effect of not having up to date risk assessments on all systems is that the threats, vulnerabilities and risks associated with running a system may not be completely understood. For example security plans are supposed to be developed from the findings of the risk assessment process. Not having completed risk assessments could affect the quality of the security plan. This could have the ultimate effect of:

- Impacting the agency's ability to perform some of its mission responsibilities effectively
- Making it difficult for management to make well-informed risk management decisions to justify expenditures that are part of the IT budget
- Reducing the thoroughness of the certification and accreditation process

Finding: Not all systems have risk assessments or current risk assessments.

The OIG found that Premerger, Do Not Call (DNC) and Infrastructure General Support System (GSS) (Infrastructure) had finalized and documented risk assessments. FFS, the system owned by DOI, had a risk assessment that was four years old. The OIG also confirmed that draft risk assessments existed for Documentum and MMS. Plans were developed for conducting a risk assessment for the CIS.

Recommendation:

2. OIG recommends that ITM finalize risk assessments for all systems lacking up-to-date reviews.

NIST SP 800-30 recommends that risk assessments include an executive summary, and describe the risk assessment methodology used. The risk assessment should identify the threats associated with operating the system. The risk assessment should also contain system-related information to include:

- Hardware
- Software
- System Interfaces
- Data and information
- Persons who support the system
- System mission
- System and data criticality
- System and data sensitivity

Additional information that NIST recommends be included in the assessment includes, but is not limited to:

- Functional requirements of the system
- Users of the system
- System security policies (organizational policies, federal requirements, laws, and industry practices
- System security architecture

- Current network topology
- Physical/environmental security controls
- Management controls
- Operational controls
- Technical controls

A more extensive list can be found in NIST SP 800-30.

Finding: Some of the existing risk assessments do not address all required areas.

The Infrastructure risk assessment includes a vulnerability scan report generated from a vulnerability assessment scan conducted by Unisys on July 26, 2004. According to the risk assessment, Internet Security Systems (ISS) Internet Scanner and Nessus were used to conduct the scans for Windows and Unix devices respectively. Additionally, Foundstone Superscan and nmap were used to map and scan ports.

Review of this risk assessment found that it addressed most of the areas identified in SP 800-30. However, other areas were not addressed. For example:

- The risk assessment does not identify the value of the information and system assets falling within the scope of the risk assessment
- The physical and environmental security controls are not addressed
- The user community is not described

The Premerger risk assessment was originally prepared to address the e-filings portion of Premerger. It appears that the risk assessment methodology only used a scanning tool to assess the system. Review of the Premerger risk assessment also found that it does not:

- Define the scope of the risk assessment effort
- Address management and operational controls
- Identify threats that could affect the system

Recommendation:

3. OIG recommends that ITM Expand risk assessments to address all areas in NIST SP 800-30 when the next scheduled risk assessment is performed for the aforementioned systems.

4.5 Privacy Impact Assessments

According to OMB Memorandum M-03-22 *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, a Privacy Impact Assessment (PIA) must be conducted before developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public; or before initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the Federal government). A PIA is used to analyze how information is handled (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Finding: Not all FTC systems have a Privacy Impact Assessment.

At the completion of fieldwork only Premerger and FFS had PIAs. Review of the Exhibit 300's found that PIAs were not completed for the remaining systems. ITM reported that it plans to develop PIAs for CIS, Documentum, and a new system in development called Comment Works. ITM also reported that it plans to prepare memorandums for applications that do not require PIAs. These memorandums will state that the system does not contain or process personally identifiable information and does not require PIAs.

Not having completed PIAs puts FTC in noncompliance with OMB guidance. The potential exists that personally identifiable information could be mishandled or released.

Recommendation:

No recommendation is necessary as ITM has recognized the requirement to complete PIAs and is in the process of completing them.

5 Independence

SP 800-37 identifies the senior agency information security officer as the agency official responsible for (i) carrying out the Chief Information Officer responsibilities under FISMA; (ii) possessing professional qualifications, including training and experience, required to administer the information security program functions; (iii) having information security duties as that official's primary duty; and (iv) heading an office with the mission and resources to assist in ensuring agency compliance with FISMA. The senior agency information security officer (or supporting staff member) may also serve as the accrediting official's designated representative.

The certification agent is an individual, group, or organization responsible for conducting a security certification, or comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The certification agent also provides recommended corrective actions to reduce or eliminate vulnerabilities in the information system. Prior to initiating the security assessment activities that are part of the certification process, the certification agent provides an independent assessment of the system security plan to ensure the plan provides a set of security controls for the information system that is adequate to meet all applicable security requirements.

NIST guidance recommends that the certification agent be in a position that is independent from the persons directly responsible for the development of the information system, and the day-to-day operations of the system. The certification agent should also be independent of those individuals responsible for correcting security deficiencies identified during the security certification.

Finding: The Senior Agency Information Security Officer position may not be sufficiently independent to act as the Certification Agent.

Having the security officer serve as the certification agent creates a potential conflict of interest. The security officer represents the CIO who is also the accrediting official. SP 800-37 states that the certification agent should be in a position that is independent from the persons directly responsible for the development of the information system, and the day-to-day operations of the system.

This conflict stems from the fact that the FTC is a relatively small organization in which IT management is centralized through the Office of the CIO. Thus, likely alternatives to this review structure are few. However, the current structure has the potential, according to NIST guidance, to allow vulnerabilities to go uncorrected or systems to be put in production prior to needed testing because of pressures to accredit a system or put it in production before its ready.

ITM informed the OIG that it agrees with the finding and has taken steps to involve program staff in the certification process whereby program staff are held accountable for their system certifications. The ITM security officer reviews and signs the certification and forwards it to the accreditation official. The OIG cautions that, although a step in the right direction, program staff may not be technically skilled to identify all vulnerabilities. This responsibility falls to the Senior Systems Security Officer, who, as stated above, could succumb to pressure from the accreditation official. The OIG will monitor the extent to which program officials are involved in the C&A process and the results of the program staff-approved certifications to determine whether potential conflicts are observed.

Recommendation:

No recommendation is necessary as ITM has taken steps to include an independent group (system owners) in the certification process. It is our understanding that this separation of duties will be placed on the POA&M to assist the OIG in tracking and monitoring this outcome.

6 Security Policies and Procedures

6.1 Policy Development

NIST 800-37 defines security certification as a "comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system." Additionally, SP 800-37 states that "(t)he Security Certification Phase consists of two tasks: (i) security control assessment; and (ii) security certification documentation. The purpose of this phase is to determine the extent to which the controls in the information system are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system. SP 800-37 also identifies the following assessments as sources to use in the certification process:

- Commercial product testing and evaluation programs
- Privacy impact assessments
- Physical security assessments
- Self-assessments
- Internal and external audits

The C&A package should contain the following:

- Approved system security plan
- Security assessment report
- Plan of action and milestones

A memorandum from OMB's Office of E-Government and Information Technology to the CIO Council, *Guidance To Assist Agencies With Certification And Accreditation Efforts,* states that certification should

contain sufficient supporting documentation describing what has been tested and results of the tests. If the test results identify security controls requiring implementation or modification, a plan documenting the security controls to be implemented must be developed as well. Agencies may also use another certification review methodology provided the set of requirements covered in 800-26 are addressed.

Finding: FTC's C&A policy does not require extensive testing of security controls.

The FTC made significant progress in developing policies and procedures to enhance its IT security program. For example, FTC developed the following policies between 2003 and 2004:

- Computer incident response team policy
- Remote access
- Certification and accreditation policies
- Password policy
- Vulnerability scan policy
- Peer to peer policy
- Inactive account management
- E-mail management policy

Additionally, the FTC Administrative Manual, Section 550, Chapter 1, was updated in June 2004. It acts as an overarching guide for the agency's overall IT security. ITM also documented the formal and informal processes for identifying the need for and developing policies and procedures. However, the OIG identified other areas that require updates or do not conform to OMB or NIST guidance.

Specifically, FTC's Certification and Accreditation Policy states that for purposes of Security Testing and Evaluation a vulnerability scan using approved vulnerability scanning software is sufficient to meet the requirement for security testing. As agency policy excludes the need to test for management and operational controls it is not in keeping with NIST guidance.

Notwithstanding the shortfall in agency policy, ITM has contracted with SAIC to perform its ST&E's. These tests and evaluations, according to ITM will be based on analysis that will include document reviews, scans and interviews to better address management and operational controls. However, as no results were available at the conclusion of fieldwork, we could not validate the methodology or the results of the ST&E's.

Recommendation:

4. OIG recommends that ITM modify its C&A policy to include the testing of management and operational controls as required by NIST guidance.

6.2 Review of the FTC Administrative Manual Chapter 1

NIST SP 800-18 states "documentation should be coordinated with the GSS and/or network managers to ensure that adequate applications and installations documentation are maintained to provide continuity of operations." Additionally, security best practices recommend that administrative documentation be up to date.

Finding: Sections of the FTC Administrative Manual Chapter 1 – Information and Technology Services, are outdated.

Review of the FTC Administrative manual found that the Section 550, *Computer Security,* was updated in June 2004. It addresses the roles and responsibilities of key personnel, information system and application access controls, information security awareness training, and FTC's information technology usage policies and practices. Section 550 also addresses security requirements for GSS and MAs and identifies FTC's MAs and GSSs. The areas of desktop software management and safeguarding sensitive and mission critical data are also discussed.

Notwithstanding these positive steps, the OIG also found that a number of sections were outdated in FTC Administrative Manual Chapter 1 – *Information and Technology Services*. Specifically, Section 200, ITM Training Resources, describes the IT training options offered by ITM. Training subjects range from outdated to current topics, e.g., the Rolm telephone system, computer literacy, FTC core software packages and corporate databases residing on the agency's central computer. This section does not discuss the IT Security awareness course offered by ITM. Additionally, the document lists courses for systems that are no longer used at FTC. For instance Section 200 offers a course for the Office of the Secretary Control and Reporting System (OSCAR). OSCAR was merged with MMS in 2003 and is no longer separately identified.

Section 300, Computer Resources identifies the variety of computer resources available at the FTC. This section also discusses remote access and appropriate use of FTC IT assets. It does not include FTC's Virtual Private Network (VPN) as a means of remote access. Not all of the major applications identified in Section 550 appear on the list of major mission support systems identified in Section 450. For instance, Do Not Call and Documentum are listed as MAs in Section 550 but are not mentioned in the list of major support systems identified in Section 450. Additionally, OSCAR is listed as a major mission support system in Section 450.

With outdated policies, Administrative Manual readers risk wasting time and effort learning outdated processes and procedures.

Recommendation:

5. OIG recommends that ITM update FTC Administrative Manual sections 200, 300 and 450 to reflect the FTC's current training classes, VPN as a means of remote access, and to capture FTC's current operating environment.

6.3 Media Handling Policy

NIST Special Publication 800-18, *Guide for Developing Security Plans for Information Technology Systems*, requires that agencies address areas such as:

- Procedures for ensuring that only authorized users pick up, receive, or deliver input and output information and media
- Audit trails for receipt of sensitive inputs/outputs
- Procedures for restricting access to output products
- Procedures and controls used for transporting or mailing media or printed output
- Internal/external labeling for appropriate sensitivity (e.g., Privacy Act, Proprietary)
- External labeling with special handling instructions (e.g., log/inventory identifiers)
- Controlled access, special storage instructions, release or destruction dates

Finding: ITM does not have general procedures for handling media containing sensitive data or personally identifiable information for all its sensitive systems.

The FTC Administration Manual Chapter 1 Section 650 provides instructions on records management. Media handling procedures were developed specifically for DNC. Yet, the OIG found in its review of the Premerger security plan that the plan does not display the sensitivity or classification of the document. For example, aside from agency level guidance, there were no additional policies and procedures in place for the FTC systems reviewed. On the other hand, the FFS security plan (developed and implemented by DOI) provides guidelines for handling the transfer of data as well as internal and external labeling. Basically, all FFS-related data is transferred directly between mainframes via secure transmission mode. It also addresses storing, and destruction of media including hardcopy data when the media is spoiled or no longer needed.

Not having information identified in the security plan as sensitive could lead to documents and storage media not being handled properly. This could result in the inadvertent release of sensitive or personally identifiable information.

Recommendation:

6. OIG recommends that ITM create system security plans that identify the sensitivity of the information contained in the systems.

7 Security Awareness Training

FTC continues to show progress in training staff on IT security awareness. To date, 1,067 of FTC's 1424 personnel (F/T, P/T, students and consultants, all of whom were with the agency at some point in FY 2004) have received security awareness training. Additionally, 25 of 34 of FTC's personnel having significant IT security responsibilities received specialized training. ITM told the OIG that it has recently begun to identify staff who have not received training, and will provide the names of these individuals to their respective supervisors. Personnel without security awareness training are more likely to commit security violations or be involved in activity that could threaten the security of the system because they are unaware of security policy and procedures.

Recommendation:

There are no recommendations for this section.

8 Security Incident Response

OMB A-130 requires that agencies develop an incident response capability for their major applications and general support systems.

The FTC Computer Incident Response Team (CIRT) handles information security incidents. When an IT security incident occurs, employees are instructed to contact the Help Desk. The Senior Agency Information Security Officer is then notified. The CIRT then goes into action and tries to resolve the problem. The Federal Computer Incident Response Center (FedCIRC) is notified when the incident is new or drastically affects agency operations. If the event is of a criminal nature, the Office of the General Counsel is contacted for advice and to make a determination if law enforcement should be contacted. The

Incident response policy includes notifying the designated OIG representative for internal security incidents where criminal activity is suspected and reported to law enforcement.

The Incident Response Policy provides step-by-step instructions on how to respond to a computer security incident. This process includes instructions for documenting the incident, assigning the event to an incident and assigning a security level to the incident. The next step in the process is to assign a handler to the incident. The policy also addresses coordinating the incident response team, containing and eradicating the problem and conducting a forensic analysis of the event. The policy also provides instructions for follow-up with external organizations and creating technical and executive reports of the incident. There are also instructions on evidence handling.

The OIG also found that there are data integrity controls used to protect FFS data (a tested system) from accidental or malicious alteration or destruction. NBC uses a variety of controls including backups, background investigations, audit trail reviews, and the use of shrink wrapped COTS software or in-house development software on the server to protect its IT assets.

Recommendation:

There are no recommendations for this section.

9 Continuity of Operations Planning

NIST SP 800-34 *Contingency Planning Guide for Information Technology Systems* states that changes to the plan, strategies, and policies should be coordinated through the contingency plan coordinator, who should communicate changes to the representatives of associated plans or programs as necessary. The contingency plan coordinator should record plan modifications using a Record of Changes, which lists the page number, change comment and date of change. The Record Changes should be depicted in a table and should be integrated into the plan.

NIST SP 800-34 also states that the plan must be in a ready state that accurately reflects requirements, procedures, organizational structure, and policies. The contingency plan should be updated at least annually or whenever significant changes occur to any element of the plan. SP 800-34 states that Line of Succession planning should be included in Continuity of Operations Plans and may also be included in an IT contingency plan. The order of succession defines who assumes responsibility for contingency plan execution in the event that the highest authority (usually starting with the CIO) is unavailable or unable to do so.

9.1 Disaster Recovery Plan

Finding: The DRP needs to be updated and modified.

The OIG found that the FTC has a tested Disaster Recovery Plan (DRP). The methodology used to evaluate the DRP was tabletop testing. The DRP addresses the recovery of FTC systems. Additionally, the FTC responded to Homeland Security Presidential Directive (HSPD) –7 and submitted a memorandum to OMB stating that the FTC has no resources that qualify as either critical Infrastructure or Key Resources. Aside from these positive developments, the OIG identified a few areas that need to be strengthened.

The FFS security plan stated that a formal contingency plan has been completed, tested, and is in place for all supporting IT systems and networks. National Business Center, Products and Services (NBC/PS) Business Recovery Plan was completed in October 1999. A formal contingency plan, "NBC Computer Center Continuity of Operations Plan (COOP)" has been implemented for the mainframe platform where the production FFS application resides. A copy of the Business Recovery Plan is securely stored offsite. The COOP is tested annually in September. The contingency/disaster recovery plans are tested every six to twelve months. According the security plan, it was tested in March, August, September 2003, and March 2004.

The emergency management team contact list contained in the FTC's plan is outdated and the plan does not list a line of succession to assume authority for executing the plan. The DRP does not contain a record of changes, nor are the changes date stamped. This could create recovery problems and delays if team members begin the recovery process with an outdated DRP. Not having an up to date emergency contact list could lead to delays and problems in contacting team members when an emergency occurs. This could lead to recovery delays. Not having an updated DRP could lead to mismanagement during the recovery process as well as increased recovery costs.

Recommendation:

7. OIG recommends that ITM Include a Record of Changes in the DRP, update the emergency management contact list, and include a line of succession for leaderships in the DRP.

9.2 Memorandums of Agreement (MOA) and Memorandums of Understanding (MOU)

NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems* states that "…memorandums of understanding (MOU), memorandums of agreement (MOA), or a Service Level Agreement (SLA) for an alternate site should be developed specific to the organization's needs and the partner organization's capabilities."

Finding: FTC needs to establish whether MOUs and MOAs with subcontractors are in place.

The FTC made progress in obtaining MOAs and MOUs. FTC currently has MOUs with the Department of Justice (DOJ) and AT&T Government Solutions, Inc. (GSI). FTC also has an MOA with the DOI for FFS. The Department of Treasury does not enter into MOAs with other agencies but it did provide FTC with an Agency Guide to Access Control for Pay.Gov. However, ITM did not know if MOUs and MOAs were in place with subcontractors, or whether they were even required. ITM is currently working with AT&T to determine the status of these agreements.

Not having MOAs and MOUs in place with these subcontractors may lead to extended disruptions in service should a system failure occur.

Recommendation:

The OIG makes no recommendation as management has proceeded to check on selected subcontractor agreements.

10 Plan of Action and Milestones (POA&M)

A POA&M, also referred to as a corrective action plan, is a tool that identifies tasks that need to be accomplished. It details the resources to accomplish the elements of the plan, milestones in meeting the task and scheduled completion dates for the milestones. FISMA guidance states POA&Ms "*are the authoritative agency management mechanism to prioritize, track, and manage all agency efforts to close security performance gaps.*" The POA&M should include all security weaknesses resulting from all reviews done by, for, or on behalf of the agency, including Government Accountability Office (GAO) audits, financial system audits and critical infrastructure vulnerability assessments. POA&Ms are to be submitted on a quarterly basis to OMB.

ITM has made significant progress in improving its POA&M management program this past year. A review of the POA&M for fiscal year 2004 found that ITM is now tracking significant weaknesses from other security reviews and studies as well as from FISMA evaluations. Quarterly POA&M reports are being submitted to OMB on time. The FTC has improved its POA&M recording, tracking, correcting and reporting processes. The POA&M follows OMB format and includes performance measures. ITM also improved its methodology for recording changes to milestones and corrective actions.

The OIG and ITM are now working together to review completed corrective actions on a quarterly basis to confirm that remediation actions actually correct the problem. Over the three quarters of FY 2004, the OIG verified that the FTC completed 25 corrective actions.

Despite the progress ITM made in improving its POA&M management process and implementing effective corrective actions, there are still areas of the POA&M process that can be improved.

Finding: ITM is marking corrective actions as complete before they are actually completed.

OMB Guidance requires that agencies report the number of weaknesses for which corrective actions were completed on time (including testing) on December 15, March 15, June 15 and October 6. Over the past three quarters of fiscal year 2004, the OIG determined six corrective actions were identified in the POA&M as complete prior to their actual completion.

Premature reporting of completed corrective actions was occurring because ITM based some of its decisions to declare an action completed on the estimated completion dates of the tasks, and in some cases these dates were overly optimistic. As OMB requires that quarterly reports be submitted prior to the last day of the last month of the quarter (for three quarters), ITM incorrectly assumed (on six items) that the actions would be completed. Additionally, ITM is not testing corrective actions to determine if the corrective action is actually completed or is effective.

OMB also requires agencies to submit quarterly update reports on their progress in correcting POA&Ms. Unlike the POA&Ms themselves which contain narratives, these status reports provide a quantitative measure of agency progress in tracking and correcting weaknesses. Because of the way ITM interpreted FISMA guidance and the way ITM reported corrective actions as completed prior to their actual completion date, the totals on the quarterly update reports are not always accurate. Additionally, the POA&M sheet from the first quarter of the year did not contain all of the weaknesses identified from other security reviews and studies. This issue was addressed by the third quarter. ITM told the OIG that it would adjust its procedures accordingly.

This problem arose because FTC misinterpreted FISMA POA&M reporting guidance. This has the effect of FTC inaccurately reporting POA&M status to OMB.

Recommendation:

8. OIG recommends that ITM verify that projected corrective actions are indeed completed, and if not reflect any adjustments on the next quarterly POA&M.

11 Miscellaneous Findings

11.1 Separation of Duties

OMB A-130, appendix III requires that duties be separated to ensure that users only have access to those functions needed to do their job and individual accountability. Premerger, Infrastructure, and FFS all maintain a separation of duties among users. The NBC identified two divisions as being primarily responsible for the maintenance and support of FFS and the data center. The Finance Systems & Operations Division is responsible for the overall management of the FFS. The ADP Services Division is responsible for the support of the data center environment it resides in. There are formal reporting lines within NBC to maintain separation of duties between key functions. The ADP Services Division is responsible for security administration, planning and programs, computer operations, application development and maintenance, system software maintenance, and production control. The Finance Systems & Operations Division is responsible for application change management and production control. Premerger relies on Oracle roles to maintain separation of duties and control what users can do on the system. For Infrastructure, there is separation of duties between security personnel and system administrators. Security personnel have limited access to system resources and must notify Infrastructure Operations when they need unlimited access to the system.

Recommendation:

There are no recommendations for this section.

12 Testing

12.1 Internal and External Vulnerability Assessment

Scans and penetration tests were not conducted as part of the FISMA review this year due to the testing performed last year by the OIG and because the FTC has taken steps to implement regular scanning of their systems. The assessment team felt that it would be counterproductive to run a scan while their scanning and remediation program is underway. However, the OIG plans to conduct scans in the upcoming year and continue to monitor ITM's progress in identifying, tracking and correcting vulnerabilities. To date FTC has:

- Purchased and installed ISS Proventia scanning and Intrusion Detection System (IDS) tools
- Conducted NESSUS scans on various systems
- Developed and finalized a vulnerability scanning policy
- Contracted Science Applications International Corporation (SAIC) to conduct scans of the Demilitarized Zone (DMZ), Infrastructure network, and FTC applications
- Developed a means to track the status of corrective actions

Review of the vulnerability assessment scan indicated that scans were run on the following systems:

- Infrastructure, (July 26, 2004)
- Premerger (August 5, 2003, e-filing servers; May 6, 2004)
- Demilitarized Zone Information Systems, (March 5, 2004)

Finding: The Corrective Action Plan (CAP) does not always identify who was responsible for taking action or the planned and actual completion dates, (ii) is not standard across all of the systems, and (iii) is not being updated.

Review of the two Premerger scans found that the August 5, 2003 scan did not contain IP addresses and only addressed the e-filing module of Premerger. Therefore the later scan could not be compared with the earlier scan. In an attempt to determine if vulnerabilities are being corrected in a timely manner, the OIG evaluation team reviewed the CAP.

The CAP did not uniformly identify who was responsible for the corrective action or the planned and actual completion dates of the remediation. Therefore, it could not be confirmed if vulnerabilities identified by the scans are being corrected. Review of the latest CAP also revealed that the format of the CAP is not standard across all of the systems.

ITM personnel stated that vulnerabilities are being corrected but the CAP is not being updated regularly. Additional scan reports were requested but not provided by the close of fieldwork. The assessment team also reviewed the VANTIVE ticket log for 2004 and found only one ticket for the removal of unnecessary services on Unix systems. This ticket was marked as completed.

Recommendation:

9. OIG recommends that ITM modify the CAP to include the name of the person responsible for the corrective action as well as the planned and actual completion dates. In addition, the CAP should be standardized across all systems, and kept up to date.

12.2 Logical Access Controls

OIG reviewed the system logical and managerial access controls implemented by ITM. The findings are discussed below.

System Access Controls

NIST SP 800-18 requires that systems employ logical access controls to designate who or what is to have access to a specific system resource and the type of transactions and functions that are permitted. There are logical access controls over Infrastructure network access. By default, accounts are given access to areas within their organizational group. Additional access is provided by information system request (ISR) or Vantive ticket. The ISR requires approval by the person's supervisor and the Vantive ticket requires approval by the data owner before access can be granted. There are logical access controls over network access.

Logical access **c**ontrols for Premerger restrict the time of day, day of the week, and status of the transaction when data can be entered. Roles within the Oracle menu also restrict users to authorized transactions and functions. Network access is determined by what shares a person can access. Access to the network is granted by Network Operations. Personnel have default access to certain areas of the network. Other areas require need-based justification for access.

According to the FFS security plan, there are controls in place to authorize and restrict the activities of users and system personnel within the application. There are hardware and software features that are designed to permit only authorized access to or within the application. These features restrict users to authorized activities. Connectivity to the FFS application is provided through the DOI limited network: SNA, TCP/IP, dial-up and VPN. Rights are granted by designated Security Points of Contact (SPOC). Privileges are granted based on job function and job categories.

In conclusion, the OIG has determined that management has moved forward to gain control over system access, an improvement over the prior year.

Recommendation:

There are no recommendations for this section.

12.3 Managerial Access Controls

Managerial controls encompass decisions or actions by individuals to provide accounts to other individuals to perform their job responsibilities while restricting access to information that is not needed for that purpose.

Limiting access to FTC systems continues to be a vulnerability for ITM. While ITM has made some improvements in this area since the last FISMA review, e.g., ITM has revoked access privileges for developers for select systems while consolidating responsibility for all production systems, the OIG noted that departing staff are not always removed from access lists, and some reassigned IT staff can still access sensitive information they no longer need to access to perform their job-related responsibilities.

The OIG review covered two areas related to access controls. First, the OIG reviewed policies and procedures to remove separating (departing) employees from FTC system access. Any accounts left open provide another gateway into the system for hackers to use. To test these controls, we reviewed (i) LAN (GSS) and (ii) Premerger access controls.

The second area reviewed also involves deleting accounts, but for current staff. Oftentimes, staff is provided access to select databases and /or systems only to have their requirements change as they move from one position, office or bureau to another within the agency. This often occurs with IT staff who, in addition to having technical skills and experience needed to navigate various IT platforms, software and databases, is often assigned administrator-level privileges on select systems. The OIG reviewed policies and procedures to control access for interagency transfers on the FFS / FPPS systems.

(A) Removing Separating Employees - The FTC maintains a biweekly separation report detailing (full time, part time and consultant) staff that have left the agency. In addition, the agency has a check out process that requires staff (either departing staff or their administrative officers) to alert the FTC Help Desk to the departure so that their system accounts can be terminated. These redundant processes provide information to systems managers to delete accounts for these employees.

Notwithstanding the processes described above, the OIG observed internal control weaknesses that permitted individuals who have separated from the agency to maintain access privileges to one of the two systems reviewed. The OIG identified 21 active LAN accounts belonging to separated employees that should have been deleted.

LAN Access - The FTC relies on a common IT infrastructure to support its major programs. Consequently, the level of security over the applications operated by these programs is derived, to a large extent, from the security controls employed in conjunction with the general support system. A major component of the GSS is the LAN. If a LAN account is disabled, it is not possible to access other systems through that disabled account.

The OIG compared the LAN access list as of 9/10/04 with the agency's separation report for FY 2004. Ideally, employees leaving the agency would have their access revoked on their last day of work at the agency. There were approximately 1,300 employees at the agency on 9/10/04. The OIG identified 152 staff that left the FTC between 10/3/03 and 8/7/04. There were 21 names appearing on both lists - e.g., staff that left the agency but were not removed from LAN access. The OIG provided the names to the network administrator for removal.

The OIG was told by ITM that accounts that are not used for 30 days go dormant, and become inaccessible. If after an additional 30 days the accounts are still not accessed, then they are permanently deleted. As a result, the most that an account should exist is 60 days. However, the OIG determined that this control does not catch all departing employees as 20 of the 21 separated staff identified above had active accounts for between two and ten months.

The OIG compared the Premerger access list with the separation report and found no exceptions. For the Premerger access list, ITM sends the program manager a list of staff who currently have access as of the date of the list. The program manager then reviews the list and provides the names of staff who no longer need account access back to ITM for deletion. This effort by ITM and Premerger appears to be effective.

The OIG believes that procedures in place to limit Premerger access are generally effective. On the other hand, network personnel should determine how LAN accounts of 20 former staff remained active for as many as 10 months after these individuals left the agency.

Recommendation:

10. OIG recommends that ITM determine why the control to eliminate accounts over 60 days failed for the employees identified by the OIG as having active accounts over 60 days.

11. OIG recommends that ITM compare separation reports to a current list of staff with LAN accounts monthly. (This search can be performed electronically.) Staff appearing on both lists should be provided to the LAN manager for immediate deletion.

Note: Subsequent to the close of fieldwork, ITM informed the OIG that seven of the 21 accounts were speed dials for the former employees listed in a current employee's IP Phone address book, and one account belonged to an employee who was still at the agency, even though he was identified as separating on 12/31/03. The OIG did not validate this explanation.

12.4 Controlling Access for Interagency Transfers

The OIG performed limited tests of employee transfers within the FTC (and NBC)[2] to determine if access to the FFS or FPPS systems were still required, and whether individuals were removed when access was no longer required.

[2]The Federal Financial System (FFS) and Federal Personnel and Payroll System (FPPS) are Department of Interior systems used by the FTC through DOI's National Business Center (NBC). FFS houses the

The OIG found that ITM, FMO and HRMO have failed to implement a policy of reviewing information access to insure that FTC and NBC contractors and staff professionals do not have access to information once they have been assigned to other duties.

For purposes of this discussion, there are two levels of access within FFS/FPPS. The first level enables users to enter and change data. Users access the FFS mainframe directly to perform these transactions. On 6/29/04 there were 18 FTC staff and 38 NBC staff with such access. (The FTC staff is primarily located in the financial management program area.)

Level 2 access does not permit the user to alter the data, rather it enables the user to view or access downloaded data for the purpose of producing reports for management review (in effect, "read only"). Reports include "FFS Detail", Payroll, "PersBud" and "FTC Downloads." On 6/29/04, there were 72 FTC staff that were granted one or more role assignments to view or access downloaded data.

The OIG identified no FTC staff transfers requiring removal from level one access. This was expected, as ITM told the OIG at the entrance conference that it was in the process of reviewing access permissions on all systems. However, we did identify five staff at NBC with access to FTC data that no longer were assigned to FTC accounts. The OIG provided the names to the NBC program manager responsible for FTC accounts who promptly deleted the names of these five from access to these accounts.

The OIG discussed account deletion policies and procedures with FTC's security point of contact (SPOC), the person responsible for, among other things, granting and revoking access, and assigning different profiles to users depending on need. He told the OIG that he has no formal procedure to ensure that the accounts of staff no longer needing system access are deleted. The SPOC told the OIG that he has not deleted any names from FFS access in the two years he has performed these duties. Similarly, the SPOC for the FPPS database (timekeeper access and SF-50 processing) told the OIG that she relies on administrative officers informing her of staff separations, but admitted that transfers often go unreported.

Although we did not review transfers with Premerger, the program manger told the OIG that ePremerger (the new system that will replace Premerger for tracking HSR filings) will provide access to all within the Bureau of Competition. The OIG believes that this runs counter to sound security practices. Access should be limited to those employees with a demonstrated need.

Recommendation:

12. OIG recommends that FFS and FPPS SPOC's establish procedures to review access lists monthly to determine whether access lists are up to date. An email to the administrative officer for all staff with access rights could quickly confirm the need.

12.5 Access to Test Data

ITM has recently attempted to limit access to systems and databases only to those individuals who have a bonafide need to select systems. However, ITM has not removed access in select test databases (test),

---

FTC's accounting system for travel and vendor payment transactions, while FPPS provides payroll and other select personnel services.

which provide access to the same data as do the production databases (production). To understand the importance of this failure, it is first necessary to understand test and production. The latter contain data that is continually updated when transactions occur. Based on the production database for FFS, for example, select staff is able to access the personnel information (pay level, awards information, social security numbers) of FTC employees for the purpose of running reports for management. Test is used to make alterations in the software that enables analysts to use the production data or to fix "glitches." ITM will copy the production database, which then becomes the test database.

ITM recently removed some of its developers from access to the production data because of its sensitivity. ITM also told the OIG that it will continue to limit access to its staff. However, ITM failed to perform this same review for staff with access to the "test" database. Consequently, staff removed from production has access to identical data in test. While aged information is no longer sensitive in some databases, the same cannot be said for personnel information. The OIG believes that access between the two should be similarly controlled.

The OIG also noted that individuals with access to the test database also had special privileges that enabled them to view information freely. Specifically, any individual that has the Oracle role app_developer assigned has four important privileges that effectively make any individual that has this role assigned to them a DBA. The Alter user privilege allows the user to alter any user password including SYS and SYSTEM. Using a series of commands that have been common knowledge among Oracle users for many years, a user can change the SYS password, login as SYS and then change the SYS password back so that the DBA would not know that the account was compromised. The second privilege is SELECT ANY TABLE. This privilege allows the user to view information in any table or view in the database. GRANT ANY ROLE and GRANT ANY PRIVILEGE allow the user to grant any role or privilege to any other user in the database including themselves. Combining the create user and grant any role or privilege effectively provides the capability of creating a Trojan horse in the database for later use.

The OIG believes that there is no reason to assign a developer a "create user" privilege, yet this privilege is automatically given with the app_developer role. Just by virtue of needing access to one area in the FSS data warehouse, i.e., staff time & attendance (STAR) data, the user is given, by default, access to all FFS databases, to include personnel and payroll. For example, the privilege "select any table" allows the user to see any data from any table.

Recommendation:

13. OIG recommends that the account manager ensure that staff has access only to those systems it needs to perform work-related functions.

14. OIG recommends that the account manager limit privileges for those assigned the app_developer *role to areas of the database required for work-related performance.*