AR 03-056

Office of Inspector General

Independent Evaluation

Review of Federal Trade Commission Implementation of the Federal Information Security Management Act For Fiscal Year 2003

INTRODUCTION

Working with the Federal Trade Commission's (FTC) Office of Inspector General (OIG), Richard S. Carson & Associates, Inc. (the Assessment Team) completed this Independent Evaluation Report along with the IG's portion of the Executive Summary that management submitted to the Office of Management and Budget (OMB) on September 29, 2003. The Independent Evaluation Report 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.

The independent evaluation comprises four elements — evaluation of the implementation of the FTC information security program, evaluation of FTC progress towards completing weaknesses addressed within the 2002 Plan of Action and Milestones (POA&Ms), evaluation of the FTC system self-assessments, and verification and testing of information security controls for four representative information systems. The results of the independent evaluation are presented in a separate Independent Evaluation Report that presents a number of recommendations to address the problems identified during the evaluation. The major findings from the report are summarized in the Results In Brief.

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

The Federal Information Security Management Act defines information security as "… protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide – (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means 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 the FY 2002 Independent Evaluation report. For example the FTC:

- Developed security plans for its general support system and major applications.
- Addressed nine of the 16 issues identified in the POA&M list and expects to complete the remaining ones by the March 31, 2004.
- Developed policies and procedures that addressed various security issues, such as password management, incident response reporting, remote access, and certification and accreditation.
- Developed a Disaster Recovery Plan (DRP).
- Developed a new IT security awareness program.

As a result of these actions, the OIG believes that the FTC is more secure today (from an information security perspective) than it was just one year ago.

In a memorandum to agencies and inspectors general, dated August 6, 2003, the Office of Management and Budget (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 interprets a significant deficiency to include a "failure to meet FISMA's delineated requirements for an agency security program including the failure to substantially comply with related policies, guidance and standards." In the IT *security program* context, examples of significant deficiencies include the failure to (i) perform adequate annual program and system reviews, (ii) maintain comprehensive POA&Ms, and (iii) adequately train agency employees and contractors. In the context of *individual systems*, OMB A-130 details three specific examples of significant deficiencies: (i) the failure to assign responsibility for security of the system or application, (ii) the lack of a system security plan, and (iii) the absence of authorizations to process (certification and accreditation).

Notwithstanding progress made by ITM in the areas identified above, the OIG found two significant deficiencies along with other areas of security concern that need to be addressed. The significant deficiencies are:

- **FTC Systems are Not Certified and Accredited**. OMB A-130, Appendix III, requires that major applications and general support systems undergo a security certification and accreditation once every three years, or sooner if the system has undergone major modifications. The OIG found that the ITM certified and accredited only one of seven systems. This was an interim certification valid for one year. Further, ITM policy does not require system tests and evaluations before certifying and accrediting its major applications and support systems. Without testing, ITM lacks assurances that modifications made to address security vulnerabilities are working.

- **POA&M Tracking does not Meet OMB Requirements.** Both OMB and GISRA/FISMA guidance requires agencies to identify vulnerabilities from all audits, studies and evaluations performed on IT systems. This requirement was reiterated in the new FISMA guidance provided to executive departments and agencies by OMB in August 2003. A review of the quarterly POA&Ms submitted to OMB found that weaknesses from the last GISRA evaluation were being tracked by ITM. However, the OIG found no evidence that vulnerabilities from C&A reviews, risk assessments or annual self-assessments were either documented or tracked in the POA&M. By not documenting vulnerabilities in the POA&M, ITM is not in compliance with OMB.

Based on these significant deficiencies and other security concerns (identified in the body of the report), the OIG made a number of recommendations to strengthen FTC's security program.

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. The FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000 (GISRA), 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 independent evaluation comprises four elements — evaluation of the implementation of the FTC information security program, evaluation of FTC progress towards completing weaknesses addressed within the 2002 Plan of Action and Milestones (POA&Ms), evaluation of the FTC system self-assessments, and verification and testing of information security controls for four representative information systems.

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 information security program included:

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

The computer security review did not include controls related to the management of safeguards or classified information or physical security controls. The OIG reviewed the following FTC systems and/or system components in detail:

- CND
- Infrastructure (E-mail)
- OSCAR
- Infrastructure (FTC Enterprise Systems)

To accomplish the review objectives, the OIG conducted interviews with the Chief Information Officer (CIO), Deputy CIO, Acting Senior IT Security Officer, other members of the CIO staff, Director of Administrative Services, and FTC program officials. The team reviewed documentation provided by the FTC including security plans, risk assessments, the disaster recovery plan, the continuity of operations plan, the Occupant Emergency Plan, certification and accreditation reports, and other security related policies. The OIG also conducted an external penetration test, a social engineering test, and an internal vulnerability scan.

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

- OMB Memorandum M-03-19, *Reporting Instructions for the Federal Information Security Management Act and Updated Guidance on Quarterly IT Security Reporting* (8/6/03)
- National Institute of Standards and Technology (NIST) Special Publication 800-26, *Self-Assessment Guide for Information Technology Systems*, August 2001
- U.S. General Accounting Office (GAO), *Government Auditing Standards*, 1994 Revision
- GAO, *Federal Information System Controls Audit Manual*, Volume I: Financial Statement Audits, January 1999
- The FTC/OIG Audit Guidance

This work was conducted during several site visits to the FTC offices between July 9 and September 5, 2003.

4 Significant Deficiencies

OMB defines significant deficiencies as "failure to meet FISMA's delineated requirements for an agency security program including the failure to substantially comply with related policies, guidance and standards."

In the context of the IT *security program*, a significant deficiency would, according to OMB, include the failure to perform adequate annual program and system reviews, failure to maintain comprehensive POA&Ms, and failure to adequately train agency employees and contractors.

In the context of *individual systems*, OMB A-130 details three specific examples of significant deficiencies: the failure to assign responsibility for security of the system or application, the lack of a system security plan, and the absence of authorizations to process (certification and accreditation). Depending on the level of risk and magnitude of harm to the system other weaknesses may also rise to the level of significant deficiency.

The OIG found two significant deficiencies in the FTC agency-wide IT *security program*. These deficiencies are discussed below.

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), currently in draft, states that the security certification package should contain a security plan (based on a risk assessment), a security test and evaluation report, and a POA&M list. The accreditation letter itself should contain the accreditation decision, supporting rationale, and terms and conditions. Further FISMA 2003 guidance states "agencies [*sic*] certification and accreditation processes must conform to NIST guidance."

FTC's C&A policy, dated March 28, 2002, states that the C&A package should contain a risk assessment report, a system security plan, a certifier's statement and the accreditation decision. The FTC's C&A policy does not require a security test and evaluation report nor a POA&M list as part of its C&A package.

Table 4-1 below identifies the major applications (MA) and general support system (GSS), to include email and FTC enterprise systems, and the security-related documentation available for review at the time of this evaluation.

Table 4-1 – C&A Security Documentation

System Name	System Type	Risk Assessment Report	Security Plan	Security T & E Report	C & A Letters
Documentum	**MA**	**No**	**Yes**	**No**	**No**
FMO	**MA**	**N/A**	**N/A**	**N/A**	**N/A**
OSCAR	**MA**	**No**	**Yes**	**No**	**No**
MMS	**MA**	**No**	**Yes**	**No**	**No**
CIS	**MA**	**No**	**Yes**	**No**	**No**
Pre-Merger	**MA**	**No**	**Yes**	**No**	**No**
CND	**MA**	**Yes**	**Yes**	**No**	**Yes**
Infrastructure	**GSS**	**No**	**Yes**	**No**	**No**

Risk Assessment Report - The OIG found that only the CND system had a documented risk assessment. However, vulnerabilities identified in this report were not listed on the POA&M for monitoring and ultimate disposition. For all remaining systems, the OIG identified no documented vulnerabilities and/or recommendations resulting from any system reviews.

ITM management told the OIG that, due to staffing constraints, it could not prepare security plans and perform risk assessments in the same year. Based on prior OIG security recommendations, it laid out a plan to prepare security plans in FY 2003 (see below), and perform risk assessments in FY 2004.

Security Plan - The agency made significant progress in the development of security plans. Seven systems requiring a plan have one. An eighth system, FMO, belongs to the Department of Interior (DOI), where responsibility for the development of the security plan lies.

The FTC is in the process of redefining its major applications and general support systems. In the previous year the FTC identified five general support systems: FTC Network, Web Servers, Firewalls, Unix Servers, and Internet/Intranet. These systems have now been rolled up into one general support system called Infrastructure.

The OIG reviewed the Infrastructure security plan and found that the security controls did not address the E-mail component in sufficient detail. This finding was verified in interviews with program officials, who stated that the infrastructure security plan focused primarily on the network. Not having sufficient detail for individual Infrastructure components may mean that the agency does not have a clear picture of the system's security posture.

Security T& E Report – While testing and evaluation is not yet a mandatory part of the C&A process (per NIST), it is required to be conducted annually on all major systems, pursuant to FISMA {Sec. 3544(b)(5)}. The OIG found no testing and evaluation material for any major system or component. Without T&E, it is difficult to identify select vulnerabilities and assure that vulnerabilities that were known have been addressed. ITM told the OIG that it recognizes the importance of testing its systems, and will incorporate the NIST guidance on T&E into its C&A policy once this guidance is finalized.

C&A Letters - The OIG found that the CND System was the only system requiring a C&A that had one. This was an interim C&A, e.g., good for one year. ITM officials told the OIG that the C&As were not accomplished in FY 2003 because the C&A process requires a risk assessment to be performed on the systems prior to certification. As stated, risk assessments are planned for FY 2004, at which time, according to ITM officials, the remaining systems will be certified and accredited.

RECOMMENDATIONS

OIG recommends that ITM:

1. Certify and accredit its seven major systems.
2. Document all risk assessments.
3. Revise the C&A policy to include testing and evaluation.
4. Modify the FTC Enterprise Network security plan to address security for major system components.

4.2 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 General Accounting Office (GAO) audits, financial system audits, and critical infrastructure vulnerability assessments. POA&Ms are to be submitted on a quarterly basis to OMB.

A review of the POA&M's for fiscal years 2002 and 2003 found that only weaknesses from the FY 2002 GISRA evaluation were identified and were being tracked.

Regarding the prior year vulnerabilities identified by the OIG, and placed on the POA&M, the OIG found that the agency has made some progress in addressing them. The OIG verified that the FTC completed nine of the sixteen corrective actions, and most of the remaining recommendations are scheduled for completion by March 31, 2004. The FTC uses the POA&M as one management tool to track security weaknesses. ITM told the OIG that it also uses the change management process meetings (see Section 5.5) as another tool to identify and address vulnerabilities. As mentioned above, these vulnerabilities are not reported on the POA&M.

Without a single, comprehensive list of its security vulnerabilities, it is difficult for ITM to have a clear understanding of its security posture. Further, the current POA&M without such vulnerabilities added is not FISMA compliant.

For FY 2004, the OIG plans to review POA&M's quarterly to more closely follow the agency's progress in addressing security vulnerabilities.

RECOMMENDATIONS

OIG recommends that ITM:

5. Record vulnerabilities and recommendations from other security studies and include them in the POA&M.
6. Rely on the key features of the agency's security program (C&A testing and evaluation) to identify, record and dispose of all significant vulnerabilities.

5 Other Security Concerns

5.1 Security Policies and Procedures

The FTC made headway in developing policies and procedures to enhance its IT security program. The FTC developed incident response, remote access, as well as certification and accreditation policies. The agency also updated its password policy. The FTC revised the Administrative Manual, Section 550, Chapter 1, to act as an overarching guide for the agency's overall IT security. However, the OIG identified other areas that do not meet OMB guidance and NIST standards.

5.1.1 The FTC's Agency-Wide IT Security Program Continues to Evolve

The FTC made progress in developing policies and procedures to enhance its security. The agency developed security requirements that were driven by the Gramm-Leach-Bliley legislation. ITM developed policies that address certification and accreditation, incident handling, remote access, and passwords. The FTC developed a Disaster Recovery Plan (DRP) for its IT assets. The FTC recently revised the Administrative Manual, Section 550, Chapter 1, that documents the FTC's IT security program as well as define its IT security framework and requirements. This document also outlines the personnel roles and responsibilities related to IT security on a high level.

However, there are several areas that the program does not address. For example, a patch management policy is not documented, policies for cell phone usage need to be refined, annual self-assessments required by OMB are not discussed, responsibility for maintaining the system inventory is not assigned, and the process on how the FTC determines what systems are major applications and general support systems is not addressed. The procedures in the existing Administrative Manual, Section 550, Chapter 1, are not sufficiently detailed or referenced for personnel to properly follow and implement the FTC's security program. Not having documented procedures may lead to security policies not being implemented consistently across the enterprise. Also, an incomplete agency-wide IT security program makes it difficult to implement policy throughout the organization.

RECOMMENDATION

OIG recommends that ITM:

7. Expand Administrative Manual Section 550, Chapter 1 to accurately reflect roles and responsibilities and policies and procedures.

5.1.2 Not All Security Policies and Procedures are in Place or Implemented Consistently

The FTC made progress in the development and implementation of security policy. However, the OIG identified instances where security policies were not implemented consistently across the agency. For example, not all risk assessments are documented even though the FTC's certification and accreditation policy requires it; password policy is not being consistently followed; not all required patches are being

installed; self-assessments are not being performed annually; and system test plans and results are not being documented. This may be caused by not having operational procedures in place that instructs FTC personnel on how to implement the policies. Two examples of vulnerabilities found where security policy was not being followed are presented below.

1. The FTC established and practices a Patch Management process, however, it is not documented. This process consists of the Computer Incident Response Team (CIRT) monitoring patches and threats and determining which patches and threats are critical to the FTC's Oracle, UNIX servers and the network. The CIRT decides whether to do the fix immediately or wait until a service pack is released. If it decides to apply a patch before it comes out in a service pack, it is tested.

System Management Server (SMS) is used by ITM to distribute patches and Vantive, a software tracking program, is used to centrally manage and track patches. The FTC is also signing up for a Sun program that will run agents for packages.

The OIG noted that multiple IT components at the network, system, and application levels contained vulnerabilities for which vendor patches for Microsoft were not applied. This was discovered as a result of the internal vulnerability assessment scan performed by the OIG. ITM believes that its process may account for some needed patches not being applied at the time of the scan (some patches not deemed critical enough for immediate application) while other patches, including the recent Blaster/Lovesan virus patch, were applied, but had to be removed because they "adversely impacted the IT environment." Both ITM and the OIG agree that all hosts should be reviewed to ensure all the latest "critical" Windows patches have been applied.

2. The vulnerability assessment scan was able to guess several passwords on some servers. These accounts either had a blank password, a default password, or the password was the same as the login name. In seven cases, it was the Administrator account that did not have a password. The same finding was identified in the prior year GISRA review, albeit on different servers. Blank passwords and passwords that are very similar to the login name are an easy way for attackers to gain access to the system. The passwords on these accounts were found to be weak and should be changed immediately to a value that meets the FTC password policy criteria.

One host was found with an account (the "sa" account) with no password. This account, by default, has no password. If left unchanged, a remote attacker could use this account to execute arbitrary commands on the operating system. The *Spida* worm actively exploits this vulnerability. All SQL Server accounts should be assigned a password.

This finding points to the need to better track corrections (on POA&Ms) to ensure that recommendations made on one machine or system are applied to all machines/systems to which they apply.

RECOMMENDATIONS

OIG recommends that ITM:

8. Document its patch management policy.
9. Change weak passwords to comply with FTC password policy.

5.1.3 Policies for Cell Phone Use Need to be Refined

Cellular phone security is a relatively new area of security that is identified as a major security issue by government and private sector IT experts. NIST Special Publication 800-30, *Risk Management Guide for Information Technology Systems,* states that organizations should identify and evaluate risks and risk impacts, and recommend risk-reducing measures.

The FTC has issued approximately 50 cell phones to FTC personnel in FY 2003 The OIG found that the FTC does not have a cellular phone policy outlining where cellular phones may be used within the FTC and what information may be discussed on unencrypted cellular lines. Without cellular phone policies, there are no established guidelines or rules of behavior for FTC personnel to follow when using them. It is possible that sensitive data could be discussed or transmitted without encryption, or phones may be used or activated in areas where sensitive information could be overheard or retrieved.

RECOMMENDATION

OIG recommends that ITM:

10. Develop a targeted cell phone usage policy.

5.1.4 Procedures For The Sanitizing, Handling, And Labeling Of Storage Media Are Not Documented for CND

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.

As of the close of fieldwork, the FTC did not have documented procedures in place for sanitizing, handling, and labeling of storage media for CND. For example, in one case the FTC relies on a contractor for the special handling and shipping of storage media. The contractor's procedure is practiced but not documented.

CND will soon contain Privacy Act data that will require special handling of storage media. The FTC has not established guidelines for the contractor to follow to ensure that this data is handled properly. By not having documented procedures on how storage media should be protected, shipped or labeled, it is possible that security procedures used to protect sensitive data may not meet FTC or federal requirements for the protection of Privacy Act data.

RECOMMENDATION

OIG recommends that ITM:

11. Establish media sanitization, labeling, shipping and handling procedures to protect CND data.

5.1.5 Administration of User Accounts Improves

The FTC continues to strengthen its Check-in Check-out and Move (CICOM) procedures to ensure that accounts are set up for new employees and terminated for employees who are separated or transferred are properly handled. However, in interviewing program officials, the OIG learned that transfers within the FTC continue to be a problem as personnel files are not always matched with user accounts to ensure that transferred individuals do not retain access to systems where access is no longer needed. It appears managers may not be aware of the need for them to notify the Information Technology Support Office whenever personnel are transferred. This result in accounts remaining active and having unneeded privileges when employees are transferred between FTC organizations

RECOMMENDATION

OIG recommends that ITM:

12. Establish a procedure to ensure that intra agency transfers only have access to systems and/or databases needed to perform their job responsibilities.

5.1.6 Progress Made in Background Check Procedures

As a result of last year's GISRA assessment, the FTC made progress in reducing its backlog of required background investigations. The Administrative Services Office (ASO) had documented personnel security procedures for full-time equivalents (FTEs) and contractors. These procedures describe the personnel security process which an individual must complete prior to gaining access to FTC systems. These procedures are internal to ASO and do not serve as an agency-wide policy. ITM is responsible for notifying ASO as to who needs access to each system so the clearance level can be determined. Contractors are not given access to certain systems until a background check has been completed. These procedures do not define any criteria by which to determine the level of clearance needed. However, ASO is working with the Office of Personnel Management (OPM) to define the appropriate clearance requirements. Once these clearance requirements have been defined, all FTC personnel will be reviewed to ensure that each person possesses the appropriate clearance level.

Of the approximately 1100 personnel at the FTC, 933 have background investigations. To date, there are 48 FTC personnel with less than 15 years of service that have outstanding background checks. These background checks were submitted to OPM and are awaiting final adjudication. Personnel files for 119 individuals with more than 15 years of service are being reviewed to determine if a background check was completed. At the time these individuals were hired, background investigations were not required. OPM does not retain any automated records for personnel with more than 15 years of service. ASO is working with OPM to determine if these 119 individuals have appropriate background checks.

During an interview with ASO personnel, it was noted that the average amount of time from the point of hire to the completion of the screening process is two weeks for fingerprints, up to six months for a background check, and up to one year for a top-secret clearance. Currently, there is not an investigation backlog for clearances at a secret level or higher.

5.2 Security Awareness and Training

OMB A-130 requires that agencies provide security awareness training for all employees. The FTC recently updated its security awareness and training course and has begun to instruct the FTC user community through a series of security awareness briefings on an annual basis. Security awareness training for FY 2003 began in July 2003. As of September 1, 2003, 387 or 35% of FTC employees and contractors received security awareness training. The security staff received security training in evidence

handling, network security and Voice Over Internet Protocol (VOIP). Also, new FTC personnel receive training on safe computer practices during orientation. Conducting annual security awareness training helps to improve the security awareness of FTC personnel, as demonstrated by the outcome of the OIG's social engineering test. (See 5.6.3)

5.3 Security Incident Reporting

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 Physical Security Officer and IT Security Officer are notified. The CIRT then goes into action and tries to resolve the problem. FedCIRC is notified when the incident is new or drastically affects agency operations. If the event is of a criminal nature, the Office of General Counsel is contacted for advice and to make a determination if law enforcement should be contacted. Law enforcement, to include the OIG, is contacted if the Office of General Counsel determines such action is required. The CIO reported four incidents to FedCIRC this past year.

If a physical security incident occurs, the ASO security officer is notified. If the incident takes place within the FTC facility, Federal Protective Services (FPS) is contacted and responds to the incident. The Washington Metropolitan Police (MPD) is contacted and responds to incidents outside the facility. The ASO Security Officer and his staff would initially respond to the incidents internal to the FTC.

RECOMMENDATION

OIG recommends that ITM:

13. Modify the Incident Response Policy to include notification to the OIG for internal security incidents where criminal activity is suspected.

5.4 Continuity of Operations

The FTC made progress in developing its continuity of operations program. It developed a DRP and conducted tabletop tests of the plan. Additionally, the FTC is working toward integrating its IT security with its physical security program. The OIG identified two areas that can be strengthened

1. NIST Special Publication 800-34, *Contingency Planning Guide for Information Technology Systems*, states that contingency plans should contain detailed records of system configurations in order to enhance system recovery capabilities. The contingency plan should identify vendors that supply essential hardware, software, and other components. The OIG learned that contingency plans for the FTC's major applications were incorporated into the DRP. However, the DRP has not undergone a functional test. A functional test will help identify weaknesses and oversights in the plan and help bring the tool to the level of detail it needs to be effective. Not having a detailed and tested disaster recovery plan may increase the recovery time from a disaster, as well as, create additional confusion when the plan is activated. ITM informed the OIG that it has no plans to perform a functional test of the DRP until it develops system redundancy to ensure systems remain operational during the test.

2. 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." The OIG believes that FTC needs four MOU's and one SLA given its various IT partnerships.

The FTC has relationships with two contractors and three government agencies for various information processing arrangements. The OIG found that the FTC has one MOU and one SLA with two agencies. The needed MOUs for the one remaining agency and two contractors are, according to ITM officials, in the process of being finalized.

RECOMMENDATIONS

OIG recommends that ITM:

14. Conduct a functional test of the DRP and modify the plan as indicated by the results of the test.
15. Finalize appropriate agreements with the three government/contractor organizations.

5.5 Configuration Management

The FTC maintains many good configuration practices. For instance, all IT management decisions must go through the CIO. Change request forms are completed and a Change Management Board tracks, approves, and reviews system changes and projects. Additionally, hardware and software inventories are conducted semi-annually. There are also policies in place for managing patches and handling security incidents. Operations and Support also established "system-hardening" checklists that must be completed for each device before it can go into the production environment. However, the OIG identified areas of configuration management that could be strengthened.

5.5.1 The FTC System Inventory Identification Process Needs to be Documented

FISMA (section 305(c)) requires the head of each agency to develop and maintain an inventory of major information systems operated by or under the control of the agency. An inventory of each agency's major information systems has been required for many years by the Paperwork Reduction Act and, more recently, by the 1996 Electronic Freedom of Information Act amendments. The FISMA amendments also provide that the inventory be updated at least annually, made available to the Comptroller General when requested, and used to support information resources management including monitoring, testing and evaluation of information security controls.

In the 2002 GISRA assessment, 11 FTC systems were identified. At the time of this assessment, the number of systems was reduced from eleven to eight. The FTC is currently redefining its systems using the definitions of major applications and general support systems in accordance with OMB A-130 and SP 800-26, resulting in still additional consolidation.

The Assessment Team identified seven major systems and one general support system. The major systems are:

- Consumer Information System (CIS)
- Matter Management System (MMS)
- Office of the Secretary Control and Reporting System (OSCAR)
- Premerger Notification (Premerger) HRS and DOJ Clearance System
- CND Registry (CND)
- Financial Management Operations (FMO)
- Documentum
- Infrastructure (General Support Systems)

In the previous year, the FTC identified five general support systems and reduced the number of general support systems to three consisting of the FTC Network, e-mail, and Internet/Intranet. The FTC recently

combined the three general support systems into one general support system called Infrastructure in accordance with NIST 800-26 guidance on defining system boundaries and analyzing organizational boundaries.

While consolidation and mandatory updates are part of the system evolutionary process, the FTC has not documented its process on how it determines what systems are major applications and general support systems. For example, the OIG did not find any documentation assigning responsibility for maintaining the system inventory, nor was there sufficient documentation to identify the interface between each system and all other systems and networks.

RECOMMENDATIONS

OIG recommends that ITM:

16. Maintain a single system inventory for the FTC major applications and general support systems and review and update the inventory at least annually.
17. Modify the inventory to reflect interfaces between systems.
18. Document the process for identifying major applications and general support systems.

5.5.2 Security Documentation is Distributed Throughout ITM

The ITM is in the process of updating and developing security documentation for its major applications and general support system. ITM has recently filled a vacant secretary position for the ITM office. One of the responsibilities of the position will be to maintain a centralized security document library. Under the current distribution system, security documentation is often difficult to obtain. Although, there is no mandate requiring agencies to maintain a centralized library of its security documentation, a centralized library would likely make it easier for the FTC to keep track of its security documentation and track when security documents should be updated. As a security best practice among other Federal agencies, ITM should consider developing a centralized library for security documentation.

5.5.3 Configuration Management Documentation Needs Updating

FISMA requires that each agency develop specific system configuration requirements that meet its own needs and ensure compliance with them. This provision encompasses traditional system configuration management, employing clearly defined system security settings, and maintaining up-to-date patches. Simply establishing such configuration requirements is not enough. Adequate ongoing monitoring and maintenance must accompany effective configuration management.

The current configuration management documentation consists of network diagrams and some configuration management documents. The OIG reviewed the configuration management documentation and found it to be outdated and not sufficiently detailed enough for FTC personnel to use as an effective configuration management tool. This became apparent when the OIG used the existing documentation to set up and conduct a network vulnerability scan to detect system vulnerabilities. For example, IP addresses were not current, making it difficult to configure a targeted scan.

RECOMMENDATION

OIG recommends that ITM:

19. Update the configuration management documentation to accurately reflect the current network configuration.

5.5.4 Version Control Software Does not Exist on the Production Network

FISMA does not require version control software but it is considered a security best practice. The FTC currently does not use version control software to track the software versions running on the servers, routers, and switches on its network. The effect of not using version control software makes it more difficult to track software versions running on routers, servers and workstations. This makes it difficult when trying to install patches and determine what devices require upgrades. As a security best practice among other federal agencies, ITM should consider installing version control software on the FTC production network.

5.6 Annual Testing and Evaluation (T&E)

NIST guidance for security self-assessments requires that T&E be performed annually. In addition to agency-sponsored tests, the OIG annually tests select systems and processes as part of its security review. Annual testing conducted by the OIG in this year's review included phone messaging tests, a social engineering exercise, and internal and external vulnerability testing. Findings for each of these areas are discussed below.

5.6.1 Self-Assessment

FISMA and OMB Guidance requires all agency systems to be reviewed at least annually. In FY2003, the OIG found that ITM technically met the self-assessment requirement by preparing security plans for all of its systems in accordance with OMB A-130 and SP 800-30, *Risk Management Guide for Information Technology Systems*. However, the format of the security plans make it difficult to determine the level of system security compliance as outlined in the NIST Self-Assessment Guide. For example, the OIG noted that vulnerabilities were not detailed for any of the eight FTC systems.

The *Federal Information Technology Security Assessment Framework* published by NIST in November 2002, identifies the importance of tests and examinations of key controls. *"Reviews of documentation, walk-throughs [sic.] of agency facilities, and interviews with agency personnel, while providing useful information, are not sufficient to ensure that controls, especially computer-based controls, are operating effectively. Examples of tests that should be conducted are network scans to identify known vulnerabilities, analyses of router and switch settings and firewall rules, reviews of other system software settings, and tests to see if unauthorized system access is possible (penetration testing). Tests performed should consider the risks of authorized users exceeding authorization as well as unauthorized users."*

Based on the NIST guidance, it is clear that testing and evaluating security controls is a critical component of any IT security program. While OMB allows for flexibility in the comprehensiveness of the tests based on other factors, to include the results of risk assessments and whether the systems were certified and accredited, the OIG notes that, with the exception of one system, neither testing nor evaluation was performed in FY 2003 (except for the CND system). Hence, ITM may not have as complete a picture of its security posture as envisioned by OMB and NIST.

RECOMMENDATION

OIG recommends that ITM:

20. Perform and document NIST-defined self-assessments or some other FTC documented security assessment methodology that meets or exceeds NIST SP 800-26 guidance requirements on an annual basis.

5.6.2 Phone Messaging Tests

As part of the 2003 FISMA evaluation the OIG evaluated the FTC's voice mail system to determine if personnel were using strong passwords to protect their voicemail accounts. To conduct this test, 35 names were randomly selected from the FTC's 1,100 employees. For the actual test, the OIG dialed the voice mail number and selected the individual's four-digit extension. Because the voice mail system only allows three unsuccessful login attempts, two series of three predetermined, commonly used passwords were entered to determine if any of them would open the voice mailbox.

Based upon this sampling, the OIG concluded that voice mailboxes are relatively secure against a limited attack. The FTC password policy provides specific guidance for developing good passwords. While these guidelines do not apply to voice mail passwords, personnel should not use default passwords or any other easily guessed passwords on its voice mailboxes.

5.6.3 Social Engineering Exercise

As part of the 2003 FISMA evaluation, the Assessment Team performed a social engineering test to determine how effectively FTC personnel are adhering to FTC security policy. FTC password policy states that personnel are required to protect their passwords. The social engineering test addressed how well FTC personnel protect their passwords when asked to provide the password to someone over the telephone.

The OIG devised a script to determine if FTC employees could be persuaded to provide their password over the telephone. For this test, an individual claiming to be from the FTC Help Desk contacted 12 FTC employees. The tester telephoned the individuals and told them he was checking to determine if their virus protection software was functioning properly and needed to run keystroke-monitoring software to do this. The employee was then asked for their password. Of the 12 individuals contacted, four or 33% of the individuals provided his/her password. The remaining eight individuals refused to provide their passwords, and three of these reported the incident to the Help Desk. Upon notification that personnel disclosed passwords during the test, ITM issued an alert over the FTC e-mail notifying staff of a potential hacker and reminding them of their responsibility to protect their passwords.

The OIG noted that of the four individuals that gave up their passwords, three had not attended ITM's security awareness training. On the other hand of the three staff who contacted the HelpDesk to alert it of the attempts, two attended security training and attributed their response to the training content. This latter point is important because staff is generally the first to recognize malicious activity and well trained staff can alert ITM before significant damage is done.

5.6.4 Internal and External Vulnerability Assessment

The OIG conducted a vulnerability assessment of the FTC network that included both an internal and an external assessment.

The internal vulnerability assessment was conducted by using the Security Administrator's Integrated Network Tool (SAINT™). SAINT™ analyzes the network signature of a given host, assesses the signature for probable vulnerabilities, ranks the vulnerabilities in terms of severity, reports the vulnerabilities and suggests a remedial course of action. In addition, SAINT™ screens every live system on a network for Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) services. For each service it finds running, it launches a set of probes designed to detect anything that could allow an attacker to gain unauthorized access, create a denial-of-service, or gain sensitive information about the network. A full SAINT™ scan of components for FTC was performed on August 5, 2003, and August 8, 2003. The data from all the scans was combined together for analysis.

The findings from the vulnerability analysis conducted during the 2002 GISRA review were compared against the findings from the 2003 vulnerability assessment. Appendix I, "Vulnerability Summary Matrix," from the FTC OIG Audit Report, "GISRA Technical Evaluation Report" (AR 02-053), listed thirty-one specific vulnerabilities found during the 2002 evaluation. These vulnerabilities were reviewed to determine if any were found again during the 2003 scan. Some of the types of tests performed in 2002 were not repeated in 2003, as the 2002 evaluation used a different methodology and was, in selected instances, a more intrusive review.

The internal vulnerability assessment identified several vulnerabilities. Passwords were guessed on several hosts, and in some cases the passwords for the Administrator account were blank. There were many hosts that needed Windows updates. Several web servers were also found with possible vulnerabilities. A number of hosts were found with several services that may be vulnerable. These services may have vulnerabilities that would allow malicious users to run arbitrary commands as a privileged user, typically *root*.

The internal vulnerability assessment also found that some of the same types of vulnerabilities identified in the 2002 evaluation were found again in 2003. Frequent examples involved default passwords protecting servers and routers, and hosts with blank password for the Administrator account.

The external assessment was performed using a variety of tools, including SAINT™, nslookup, whois, nmap, host, and xprobe. In addition, several attempts were made to access specific ports and services identified by the SAINT™ scan. The external assessment was conducted partially "blind" – i.e., information from the previous internal assessment and other information previously learned about the FTC network was not used for most of the external assessment. This was done, in part, to more closely simulate how an actual "hacker" might approach the penetration attempt. The external assessment was conducted using several steps:

- **Identify FTC IP Space** – The first step was to identify the IP space "owned" by FTC. A combination of nslookup and the ARIN whois service were used to identify the target IP space.

- **SAINT™ Scan** – The next step was to perform a SAINT™ scan on the identified IP space.

- **Nmap, host, and xprobe Scans** – After the SAINT™ scan, additional probes were performed using nmap, host, and xprobe.

- **Port and Service Tests** – Information gathered by the different scans was used to try and connect to various ports and use various services.

The external vulnerability assessment identified several vulnerabilities in the FTC web servers. Several FTC web servers may provide more information about their configuration than is necessary. In addition, there may be too much information about FTC hosts in one system accessible to the public.

Internal and external scan results were provided to ITM management under separate cover for additional analysis and corrective action.

RECOMMENDATION

OIG recommends that ITM:

21. Develop a plan and schedule to correct the vulnerabilities identified by the internal and external vulnerability assessments. The plan should be communicated on the POA&M.