



governmentattic.org

"Rummaging in the government's attic"

Description of document: Two (2) releases of Federal Trade Commission (FTC) Inspector General (OIG) Audit Report AR 01-051, (Government Information Security Reform Act) GISRA Security Evaluations Report, 2001

1st Requested date: 07-November-2016

1st Released date: 21-December-2016

2nd Requested date: 23-May-2017

2nd Released date: 06-Jul-2017

Posted date: 23-July-2018

Note: Report version released 2017 begins on PDF page 27

Source of document: Freedom of Information Act Request
Office of General Counsel
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, D.C. 20580
Fax: (202) 326-2477
Email: FOIA@FTC.GOV

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

DEC 21 2016

Re: FOIA-2017-00130
FTC OIG Report

This is in response to your request dated November 7, 2016, under the Freedom of Information Act seeking access to FTC OIG Report AR-02-51, which is incorrectly named on the FTC's website. The correct nomenclature for the report is AR-01-51. In accordance with the FOIA and agency policy, we have searched our records as of November 8, 2016, the date we received your request in our FOIA office.

The Commission's fee regulations specify that fees less than \$25 will be waived. *See* 16 C.F.R. § 4.8(b)(4). Because the fees associated with the processing of your request did not exceed \$25, we have processed your request free of charge.

We have located the responsive record. I am granting partial access to the record. Portions of these pages fall within one of the exemptions to the FOIA's disclosure requirements, as explained below.

Some information is exempt from disclosure under FOIA Exemption 7(E), 5 U.S.C. § 552(b)(7)(E). Exemption 7(E) protects information that would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law. *See Foster v. DOJ*, 933 F. Supp. 687 (E.D. Mich. 1996).

If you are not satisfied with this response to your request, you may appeal by writing to Freedom of Information Act Appeal, Office of the General Counsel, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580, within 90 days of the date of this letter. Please enclose a copy of your original request and a copy of this response.

You also may seek dispute resolution services from the FTC FOIA Public Liaison Richard Gold via telephone at 202-326-3355 or via e-mail at rgold@ftc.gov; or from the Office of Government Information Services via email at ogis@nara.gov, via fax at 202-741-5769, or via mail at Office of Government Information Services (OGIS), National Archives and Records Administration, 8601 Adelphi Road, College Park, MD 20740.

If you have any questions about the way we handled your request or about the FOIA regulations or procedures, please contact Brian Welke at 202-326-2897.

Sincerely,

A handwritten signature in cursive script, reading "Sarah Mackey". The signature is fluid and elegant, with a long horizontal stroke extending from the end of the name.

Sarah Mackey
Associate General Counsel

**FEDERAL TRADE COMMISSION
OFFICE OF INSPECTOR GENERAL**



AUDIT REPORT
GISRA SECURITY EVALUATIONS REPORT



FEDERAL TRADE COMMISSION
Office of Inspector General
GISRA Security Evaluations Report

Developed By
SeNet International Corporation
"Delivering Practical e-Security Solutions"

September 4, 2001

Table of Contents

Maintaining Competition Program

- 1.1 Program Description**
- 1.2 IT Support Infrastructure**
- 1.3 Evaluation of Security Controls**

Consumer Protection Program

- 2.1 Program Description**
- 2.2 IT Support Infrastructure**
- 2.3 Evaluation of Security Controls**

General Support Systems

- 3.1 Description**
 - 3.2 Evaluation of Security Controls**
-

Introduction

Dramatic increases in computer interconnectivity, especially in the use of the Internet, are revolutionizing the way Federal Government agencies are conducting their business. With the benefits, however, the widespread interconnectivity poses significant risks to agency computer systems and networks. The General Accounting Office (GAO) has identified information security weaknesses at several federal agencies. (*Federal Information Security: Serious and Widespread Weaknesses Persist at Federal Agencies*, AIMD-00-295, September 6, 2000.) Many of these problems appear to be systemic in nature.

The Government Information Security Reform Act (GISRA) attempts to address information security weaknesses. It codifies existing Office of Management and Budget security policies (Circular A-130, Appendix III) and reiterates security responsibilities outlined in the Computer Security Act of 1987, the Paperwork Reduction Act of 1995 and the Clinger-Cohen Act of 1996. In addition, GISRA requires annual agency program reviews and annual independent evaluations. This document contains Office of Inspector General (OIG) findings resulting from the GISRA program reviews for FY 2001 at the Federal Trade Commission (FTC).

The OIG contracted with an independent information security consulting firm to assist in conducting this review and to prepare the OIG portion of the report. The review followed the National Institute of Science and Technology's (NIST) Information Technology Security Assessment Framework and was performed in accordance with Government Auditing Standards.

The OIG applied the NIST Framework to the three program areas (Maintaining Competition, Consumer Protection and General Support) identified by management. For each program area, the OIG selected four major applications. The applications reviewed were:

Maintaining Competition

Premier Notification System	Clearance Notification System
Matter Management System	Document Management System

Consumer Protection

Consumer Information System	eConsumer.gov & other web-based systems
Business Intelligence Reporting	Identify Theft

General Support

Internet Access and Applications	E-mail
Data Warehousing	LAN/Network Infrastructure

Office of Inspector General

Security Evaluations

The following sections provide detailed information concerning the two major programs reviewed in this effort: Maintaining Competition and Consumer Protection. Section C. provides information concerning the support systems reviewed under this effort including network and server infrastructure.

The format for these sections is derived from the CIO Council's Self Assessment Guide for IT Systems, NIST Publication 800-18.

1. Maintaining Competition Program

1.1 Program Description

The Bureau of Competition (BC) is responsible for enforcing Federal antitrust and trade regulation laws under Section 5 of the Federal Trade Commission Act, the Clayton Act, and a number of other special statutes that the Commission is charged with enforcing. In carrying out these responsibilities, BC examines a wide variety of industries and commercial practices. When appropriate, it takes action to ensure that competition in the nation's markets for goods and services is maintained in a manner that will best assure the working of free market forces. Such action may include seeking injunctive relief in Federal District Court, complaint and litigation before the agency's administrative law judges, and formal nonadjudicative settlement of complaints. The Bureau also conducts compliance investigations and initiates proceedings for civil penalties to assure compliance with final Commission orders dealing with competition and trade restraint matters.

The data collected, stored and created as a byproduct of the Bureau's activities tends to be of sensitive to highly sensitive value. In particular, data filed by firms in conjunction with merger activity and legal proceedings, if improperly disclosed or tampered with, could have a significant economic impact on all parties involved and may expose the Commission to adverse legal action.

In FY 2001, the Maintaining Competition mission had an allocated budget of approximately \$60 million and staff of over 490 full time employees.

1.2 IT Support Infrastructure

The Bureau of Competition relies upon a variety of applications, system and IT support staff to perform its mission. These include major applications such as:

- Matter Management System (MMS)
- Premerger Notification System (PNS)
- Clearance Notification (Joint FTC-DOJ Application)
- Document Management System (LANDOC)

In addition, the Bureau makes use of a variety of General Support Systems to carry out its activities. These include:

- LAN and network infrastructure
- E-mail
- Internet/Intranet Access and Applications
- Data Warehousing (SAN)

The Bureau of Competition obtains IT support for its applications from multiple components within ITM - the Software Development Team for applications development and maintenance, Technology Operations for systems and user administration and the Litigation/Customer Support group for end-user help desk and special operations support.

1.3 Evaluation of Security Controls

The OIG evaluation of security controls was based on interviews with the director and staff from the premerger notification office (PNO). Additional support staff from ITM were also interviewed in conjunction with this evaluation.

1.3.1 Management Controls

1.3.1.1 Risk Based Management

The OIG found that the program areas we reviewed in the Bureau of Competition do not conduct formal periodic risk assessments of their major applications, as called for by OMB A-130. On certain occasions, security issues are addressed and steps are taken to improve security controls. For example, after several users noticed suspicious activities in the Hart-Scott-Rodino (HSR) applications during off-hours, access to the application was restricted to normal business hours.

1.3.1.2 Security Responsibility Assignment

Bureau programs we reviewed have not formally assigned the responsibility for information security to any Bureau staff. In the premerger notification office, this responsibility, by default, falls with the PNO director. Much of the day-to-day operations, including security, fall under the responsibility of the ITM Software Development Branch, and the assigned system manager for the Bureau's major applications.

1.3.1.3 Review of Security Controls

Security controls are not reviewed on a regular basis as indicated in 1.3.1.1 above. For example, despite explicit FTC policy (Section 550, Computer Security, FTC Administrative Manual), the Bureau does not review access lists on a monthly basis as required. Consequently, access may still be possible for separated personnel or staff who changed their position and no longer need such access.

1.3.1.4 Security Management in the Program Lifecycle

Like other aspects of an IT system, security is best managed if planned for throughout the IT system life cycle. Of the five basic phases, initiation, development, implementation, operation and disposal, we found that security is actively considered and addressed only during the first three. Security requirements are first defined in functional terms by the program staff, then are converted to technical requirements by the development staff. Technical security controls (e.g. user roles) are then implemented and tested before moving to the production/operations phase. However, the OIG noted some exceptions to this process. For example, while the requirements called for a firewall on the link between DOJ into the Premerger and Clearance databases, such firewall has not been implemented. The System Manager was not aware that the required firewall was not put in place by the telecommunications group.

In the operations phase, security appears to receive even less attention, for example:

- Access rights to the applications are not reviewed on a regular basis
- Applications logs and usage reports are not reviewed on a regular basis
- No formal Security Plan for the Bureau Major Applications have been developed

While program officials may be attempting to promote and maintain a secure environment, they are not familiar with the specific requirements of Federal guidelines such as OMB A-130, NIST 800-18 and others. Better knowledge of the requirements will help address the above issues.

1.3.1.5 System Security Plan

The Bureau has not developed System Security Plans for any of its major applications. The purpose of such plan is to document security requirements and describe the security controls, both in place and planned. The plan also identifies security responsibilities and the expected behavior of all individuals who access the system.

1.3.1.6 Rules of Behavior

There are no specific "Rules of Behavior" for the Bureau of Competition's major applications. FTC has an official, agency-wide Statement of Computer Hardware and Software Use and other guidelines (e.g., policy on "Strong Passwords"), but these guidelines do not cover specific security requirements of the Bureau of Competition. While the staff may be aware of and follow these guidelines, the Bureau should document and formalize them into its official "rules of behavior."

1.3.2 Operational Controls

1.3.2.1 Personnel Security

No special security screening is done prior to granting access to the Bureau of Competition's applications. The Bureau also accepts requests for access from the Department of Justice, without any specific screening (DOJ is considered a "trusted partner") although its access rights are limited in comparison to FTC staff. Developers and database administrators are also granted access to the operational data, without prior screening or specific authorization from program officials.

1.3.2.2 Physical and Environmental Controls

The systems running the Premerger, Clearance and other major applications used by the Bureau of Competition are housed in the first floor Data Center, which is a controlled access facility with adequate physical and environmental controls. End-users facilities, on the other hand are relatively open. Anyone authorized to enter the FTC building (to visit the library, cafeteria, etc.) may gain access to offices where premerger material (both paper-based and in electronic form) is processed because there are no physical barriers, such as key card entry, to those offices.

1.3.2.3 Production Input/Output Controls

Premerger application material is registered and stamped as confidential upon receipt by FTC staff. Application material is then processed by various staff who analyze it and create/update entries in the Premerger and MMS systems. Application material is stored in a filing room during the clearance process, and from there it is shipped to off-site storage for a period of 10 years. The Bureau is considering moving to a document imaging system to alleviate this burden. Printouts and other material deemed of no

further use are stored in “burn bags” located in every office. Material from these bags is collected periodically and destroyed by a third party contractor.

1.3.2.4 Contingency Planning

The Bureau does not have formal plans in case major applications are not available to its staff. The Bureau has experienced several downtime occasions lasting from one to three days. Such down time could affect, for example, the ability to issue “early termination” decisions for premerger requests. Other activities may continue for a short period of time using the paper-based material available to the staff. A Disaster Recovery Plan is severely out of date (1997) and is not known or practiced by agency program and IT staff.

1.3.2.5 Hardware and Software Configuration Management (CM)

Bureau of Competition officials and ITM Software Development Branch staff closely adhere to the CM process. New features requested by the program staff and the corresponding development and testing activities are tracked and periodically reviewed until such upgrades are rolled into production. For major upgrades, formal acceptance sign sheets are completed and signed by program and ITM officials.

1.3.2.6 Data Integrity Verification

The Bureau of Competition has a designated data steward whose responsibility is to ensure the integrity of the premerger data. Measures have been instituted to prevent modification of data – regular users cannot modify records after the “closing out” date has passed. Staff may request the data steward to make such changes with justifications, which are then entered as comments into the modified records. Besides the data steward, the ITM system manager is also authorized to make such changes.

1.3.2.7 Security Documentation

Documentation of security settings exists, but in a fragmented form. Network and systems documentation is not maintained in a centralized, methodic way. Documentation of software applications is fairly well maintained by tools such as Oracle Designer and the Configuration Management process.

1.3.2.8 Security Awareness Training

The Bureau of Competition does not have specific security training for its users beyond the agency-wide activities which include new staff orientation, an annual “security week” event and security tip sheets published occasionally by the Litigation and Customer Support Group.

1.3.2.9 Incident Response Handling

There is a disconnect between the programmatic side and ITM on the subject of Security Incident Response handling. The CIO's incident handling policy is not well known and the program officials are not aware of security incidents which may be "discovered" by IT staff. Program officials' incident handling is limited to conduct issues or ad-hoc access/activities audits usually outside the formal incident response handling process.

1.3.3 Technical Controls

1.3.3.1 User Identification and Authentication

The agency has a strong password policy recommending passwords' length and composition that is automatically enforced by the system for entry into any of the agency's technology resources. This is done by passing through network security using either an authorized User ID and enforced strong password or a SecureID token.

However, once into the agency's network, systems like the Premierer, Clearance and other Bureau of Competition applications use an [REDACTED] as the main mechanism for user identification and authentication. (Dial-in remote access is also possible and requires [REDACTED] token as an extra measure of strong authentication). [REDACTED] applications can, but are not set to, limit failed log on attempts. Users are not forced to change passwords, and there is no mechanism in place (automatic or manual) to enforce the selection of strong passwords (at the [REDACTED] level).

Creation of users' IDs is supposed to be controlled by the "Check-In/Check-Out" process, however requests for new user access are sometimes received (and processed) via phone, voice mail and e-mail messages. The "check out" process lacks controls to ensure that all departing employees are removed from previously-authorized applications. For example, review of current user accounts of the premierer application found one active account for a staff member who left the agency three months earlier. There is even less certainty when it comes to Department of Justice users accounts. The FTC does not automatically receive notice that DOJ disables the account of departing employees in a timely manner.

1.3.3.2 Logical Access Controls

Similar to other FTC applications, the Premierer, Clearance and other Bureau of Competition applications use the concept and mechanism of "roles" to limit access to certain functions or sections of the database. For example, the Premierer application has the [REDACTED] among other roles. Users are assigned to a role based on their functional needs. Program officials review and approve requests

2. Consumer Protection Program

2.1 Program Description

The Bureau of Consumer Protection's (BCP) mission is to protect consumers from unfair, deceptive, or fraudulent practices. The Bureau enforces a variety of consumer protection laws enacted by Congress, as well as trade regulation rules issued by the Commission. Its actions include company-specific and industry-wide investigations, administrative and federal court litigation, rulemaking proceedings, and consumer and business education. In addition, the Bureau contributes to the Commission's on-going efforts to inform Congress and other government entities of the impact that proposed actions could have on consumers.

The Bureau recently began new initiatives – cooperation with international law enforcement agencies and new Internet-based interfaces with consumers (e.g., www.econsumer.gov web site).

In FY 2001, the Consumer Protection Bureau had an allocated budget of approximately \$78 million and staff of over 550 full time employees.

The data collected, stored and created as a byproduct of the Bureau's activities tends to be of sensitive to highly sensitive value. In particular, data filed by individuals in conjunction with consumer fraud and identity theft falls under the Information Privacy Act and is very personal and sensitive. Such data, if improperly disclosed or tampered with, could have adverse impact on ongoing investigations, further harming private parties.

2.2 IT Support Infrastructure

The Consumer Protection Bureau relies upon a variety of applications, system and IT support staff to perform its mission. These include major applications such as:

- Consumer Information System (CIS/Sentinel)
- Business Intelligence Reporting
- Identity Theft
- eConsumer.gov and other web-based systems.

Other special-purpose applications used by the Bureau include Identity Theft, Care and Energy labeling, Textile RN Tracking System and Consumer Response Center. The Bureau also makes use of General Support Systems to carry out its activities. These include:

- LAN and network infrastructure
- E-mail
- Internet/Intranet Access and Applications

The Bureau of Consumer Protection obtains IT support for its applications from multiple components of the IT Management Office - the Software Development Team for applications development and maintenance, Technology Operations for systems and user administration and the Litigation/Customer Support group for end-user help desk and special operations support.

2.3 Evaluation of Security Controls

Evaluation of the security controls was based in large part on interviews with program staff members. Support staff from ITM were also interviewed in conjunction with this evaluation.

2.3.1 Management Controls

2.3.1.1 Risk Based Management

The Bureau of Consumer Protection does not conduct formal periodic Risk Assessments of its Major Applications, as called for by OMB A-130. On certain occasions, especially application initiation/development, security issues are addressed and steps are taken to improve security controls. Program officials were not aware of their role in initiating and conducting periodic reviews of security controls. To the extent such reviews are conducted, they tend to focus on technical controls, primarily in the system initiation and development phases.

2.3.1.2 Security Responsibility Assignment

At the program level there is no single person who has the assigned responsibility for information security of BCP applications. This responsibility is spread "by default" among multiple individuals, some program staff and others from the software development and technology operations group.

2.3.1.3 Review of Security Controls

Security controls pertaining to BCP applications are reviewed primarily during their initiation and development phases. Program management is not involved in review of security controls nor does it initiate such reviews on a regular, planned basis beyond the development phase. For example, in response to the CIS/Consumer Sentinel System Questionnaire, dated 5/22/01, program officials indicated that they believe it is the

Security Officer's responsibility to ensure that corrective actions are effectively implemented.

2.3.1.4 Security Management in the Program Lifecycle

Bureau application support staff are generally highly aware of the sensitivity of the information handled by their applications. This is best expressed during the initiation and development phases of new applications where an estimated 20% of the design is dedicated to security issues. This approach however changes when applications move into the operational phase. At this point security is assumed to be handled externally to the program, for example by Technology Operations or Customer/Legal Support (help-desk).

2.3.1.5 System Security Plan

None of the major applications in use by the Bureau of Consumer Protection has a formal System Security Plan as required by OMB Circular A-130, Appendix III.

2.3.1.6 Rules of Behavior

Rules of Behavior define how and what users are allowed to perform using a specific application.

We found that only one application, CIS/Sentinel, had a formal agreement titled "Consumer Sentinel Network Confidentiality Agreement" which specifies access and confidentiality requirements. This agreement though is only for external users of the CIS and Identity Theft applications and is acknowledged at the organization level rather than the end-user level.

Beyond the agency wide "Statement of Computer and Hardware Software Use," specific Rules of Behavior codes for end-users of Bureau of Consumer Protection applications are not defined.

2.3.2 Operational Controls

Operational controls are those security mechanisms which are primarily executed by people as opposed to systems. These include procedures and practices put in place to improve the security of a system or group of systems.

2.3.2.1 Personnel Security

Bureau of Consumer Protection staff (as all FTC employees and contractors) is subject to a background investigation as a condition of employment at the agency. The type of clearance depends on the position. According to the agency's Physical/Personnel security officer, all positions have been assigned a "sensitivity level" – Non-sensitive, Moderate

and Sensitive. About 90 percent of the employees and staff have been cleared by OPM so far. This applies to contractor staff as well – and in the case of BCP, the call center operators.

2.3.2.2 Physical and Environmental Controls

The systems running the major applications used by the Bureau of Consumer Protection are housed in the first floor Data Center, which is a controlled access facility with adequate physical and environmental controls. Staff workspace areas, on the other hand, are relatively open. Anyone authorized to enter the FTC building (to visit the library, cafeteria, etc) may gain access to offices where consumer protection material (both paper-based and in electronic form) is processed because there are no physical barriers, such as key card entry, to those offices. Though physical security requirements are defined in the contract, the agency has not conducted a survey of the call center outsourcing facility to verify they are implemented as required.

2.3.2.3 Production Input/Output Controls

Input/output material to the applications operated by BCP is primarily electronic in nature. Complaints are submitted electronically or entered by FTC Call Center staff for "phoned-in" complaints. Once entered, this material falls under the inherent security controls of the application and its underlying support systems. Paper-based material that is no longer needed is collected in "burn bags" and destroyed by an outside contractor.

2.3.2.4 Contingency Planning

Program officials indicated that within the consumer information system (CIS), the primary applications need to have a high degree of availability. However there is no formal Service Level Agreement with ITM specifying this requirement. There are preliminary discussions of a "hot backup" for Sentinel. In general the contingency planning situation is similar to that of Bureau of Competition – an agency-wide Disaster Recovery Plan is severely out of date (has not been revised since 1997) and is not known or practiced by agency program and IT staff.

2.3.2.5 Hardware and Software Configuration Management

Bureau of Consumer Protection officials and ITM Software Development Branch staff closely adhere to the CM process. New features requested by the program and the corresponding development and testing activities are tracked and periodically reviewed until such upgrades are rolled into production. For major upgrades, formal acceptance sign sheets are completed and signed by program and ITM officials.

2.3.2.6 Data Integrity Verification

Data analysts at the Bureau of Consumer Protection are tasked to verify the correctness of data entered by phone operators or data entered via the Web (electronic complaint form). BCP applications have built in checking, tracking and auditing features to assist in

reviewing changes to data. In addition, there are database analysis tools which are executed daily against the operational data to check it.

2.3.2.7 *Security Documentation*

Documentation of security settings exists, but in a fragmented form. Network and systems documentation is not maintained in a centralized, methodic way. Documentation of software applications is fairly well maintained by tools such as Oracle Designer and the Configuration Management process.

2.3.2.8 *Security Awareness Training*

In general, no specific security training is required of BCP staff, nor is there specific security training material associated with BCP applications. The exception to this observation is the call center outsourcing contract -- Contractor personnel at the Consumer Response Center receive security training as part of the orientation process. The training material was developed by the FTC. Training is conducted by contractor staff. This training, along with background screening, is a pre-requisite for accessing CIS.

2.3.2.9 *Incident Response Handling*

Program officials are not involved or aware of security incidents. The assumption/expectation is that these issues are addressed by the ITM staff software development, help desk and/or operations. BCP Program officials could not recall a security incident in recent time.

2.3.3 *Technical Controls*

2.3.3.1 *User Identification and Authentication*

For internal users, Login IDs and passwords are the mechanism for user identification and authentication. BCP applications, as all [REDACTED] based applications at the agency, require a valid user name and password at the application level. Users cannot access these systems without first passing through network security by either using a strong password and authorized user ID or a [REDACTED]

The OIG has found though, that while the agency has a policy requiring users to choose "strong" passwords, this is not enforced automatically for entry into specific BCP systems either by the application or manually by the Database administrators (DBAs). Passwords are not checked for minimum size or composition. Users are not forced to change passwords. Users of the CIS application will lock themselves out if they enter a wrong password more than 5 times in a row. Only a DBA can then reset their password.

External access to Sentinel is authenticated by the use of [REDACTED]. The agency contracted with [REDACTED] to issue certificates to authorized end users. The Sentinel

application also makes use of the [REDACTED] to encrypt user sessions. Combined, these measures provide good protection for this application. The digital certificates are set to expire automatically after one year from issuance, providing a built-in default mechanism to prevent access by users who no longer need it. FTC relies on the external entity (e.g. a law enforcement agency) for notification if a certificate needs to be revoked prior to that time, and to ensure that certificates are re-issued only to valid users.

2.3.3.2 Logical Access Controls

BCP applications employ the concept of roles. Roles are pre-defined sets of features or capabilities users are entitled to. Users are assigned to a role based on their functional needs. Program officials review and approve requests for roles which allow users to write or modify records, but read-only access roles are not reviewed by program officials. New users are assigned the default role [REDACTED] which limits the user to connect to the database but not view it or change its content. BCP has a few designated staff members who can create new user accounts and assign their roles.

2.3.3.3 Audit Trails

BCP applications incorporate auditing features in each database table. Such features allow administrators to identify when and by whom a change to a data record has been made. Reports are not generated, nor reviewed on a regular basis.

2.3.3.4 Systems Interconnections

BCP systems are not functionally interconnected to external systems. As all FTC applications, BCP relies on common IT infrastructure (hosts, LANs, WANs etc.), which includes physical connectivity to external entities.

2.3.3.5 Public Access Controls

Some of BCP's major applications provide access to the public. These applications have reasonable measures of protection since they do not allow interactive access to FTC data. For example, the Consumer Complaint Form is a "one-way" mechanism for the public to submit complaints the agency. Access from the Internet does not allow for subsequent retrieval of information regarding a previously submitted complaint.

3. General Support Systems

The FTC relies on a common IT infrastructure to support its major programs. Consequently, the level of security of the applications operated by these programs is derived, to a large extent, from the security controls (management, operational and technical) employed in conjunction with these general support systems. The following is an evaluation of the security controls of these systems. FTC personnel interviewed for this purpose include the Acting and departing CIOs, the Information Security Officer, heads of the Software development group and Technology Operations group and other staff members.

3.1 Description

The General Support Systems we reviewed as part of this GISRA Review effort included the Unix servers which run the agency's major applications and the telecommunications (LAN/WAN) infrastructure which connects them to FTC personnel and remote users.

There are a total of [REDACTED] running the various applications including –

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

All of the above are running a [REDACTED] Development and Production systems use the [REDACTED] database platform and related support applications.

External connectivity is comprised of [REDACTED] plus connections to Department of Justice, Department of the Interior National Business Center and the BCP call center contractor. A number of desktop systems have direct Internet access (via modem or DSL). These systems are not connected to FTC's internal LAN.

3.2 Evaluation of Security Controls

The evaluation is primarily based on information provided by ITM staff – either verbally or documented. On a few occasions we asked for user access reports to be generated from selected applications. We used these reports to compare against the agency's staff separation list obtained from Human Resources Management Office to assess controls over the removal of former employees from access to FTC databases.

3.2.1 Management Controls

3.2.1.1 Risk Based Management

ITM does not conduct security risk assessments and vulnerability testing on a regular basis. The last third-party technical controls evaluation was conducted in late 1998. An in-house security vulnerability assessment was conducted in mid 1999. ITM is planning to contract with an IT security firm to conduct a penetration test in the "near future."

3.2.1.2 Security Responsibility Assignment

The responsibility for information security is not clearly defined. While at the high management level this responsibility clearly falls with the CIO (or the currently Acting CIO), at the operations level it seems to be split between the Information Security Officer, the Director of the Technology Operations Group and the Director of the Litigation and Customer Support Group (help-desk). The Information Security Officer issues policies and guidelines but does not, for example, approve systems security settings or review operations logs. The help desk is responsible for desk-top security and for security awareness training.

3.2.1.3 Review of Security Controls

There is no formal process to routinely review security controls. Such reviews are usually conducted as part of system modifications or upgrades. For example, ITM is selecting a new e-mail system to replace the current [REDACTED] application, and security considerations are playing a role in this process. However this is not a mandatory part of the CM process as the CIO can approve a change without full committee review. This outcome occurred when wireless devices were introduced into the IT environment on a pilot basis.

3.2.1.4 Security Management in the Program Lifecycle

Not applicable at FTC. The systems and applications reviewed in this section are used in support of other FTC programs.

3.2.1.5 System Security Plan

None of the General Support Systems have a written System Security Plan at this time.

3.2.1.6 Rules of Behavior

The FTC issued an agency wide Rules of Behavior document titled "Statement of Computer Hardware and Software Use" which clearly specifies "Do's and Don'ts" for end-users. This policy is not required to be acknowledged in writing by FTC staff/contractors and was not included in the sample "New Employee Package" provided for our review.

3.2.2 Operational Controls

3.2.2.1 Personnel Security

***** Covered Previously *****

3.2.2.2 Physical and Environmental Controls

Servers and telecom gear are housed in access controlled facilities on the first floor of the FTC HQ building. Only Technology Operations staff have access using their appropriately encoded employee badges. LAN gear is installed in locked wiring closets throughout the building. The help desk facility is also access controlled after hours. Laptops and other valuable gear is stored in a locked room.

3.2.2.3 Production Input/Output Controls

**** Not Applicable to FTC ****

3.2.2.4 Contingency Planning

The agency-wide Disaster Recovery Plan ("Central Computer Systems & PBX Disaster Recover Plan" Release 2.0) is out of date (has not been revised since 1997) and is not known or practiced by agency program officials and IT staff. This document should be "reviewed annually and revised as appropriate." This issue goes beyond a "paper exercise" – during a recent power outage, computer room staff did not follow proper shut-down procedures and caused an extended downtime lasting up to 30 hours with certain applications.

ITM and program officials considered deploying backup systems and "hot-sites," however this idea has not been pursued further due to funding shortages. A new emergency generator is to be installed by year end.

It should be noted that in some program officials' opinion, their program can continue for a day or two without computer resources – using paper tickets and the analysts working with hard copies of case material.

3.2.2.5 Hardware and Software Configuration Management

There is a very detailed Configuration Management process in place. A CM committee meets on a weekly basis to coordinate upgrade and change activities. Proposed changes are tracked in [REDACTED] – the trouble-ticketing and help desk system. The process appears to work well, especially in the application development arena. However it appears that not all IT changes are introduced this way (see reference to the wireless PDAs in Section 2.1.3 above).

3.2.2.6 Data Integrity Verification

The technology operations group assigned a staff member to perform backup and restore operations as well as system-level monitoring. Database administrators perform daily integrity checks on operational data.

3.2.2.7 Security Documentation

Security controls are not sufficiently documented. Network diagrams that we were shown do not provide sufficient level of detail and are inaccurate. The Security Officer, for example does not have a copy of the security rule set of the firewalls. Most of the relevant information is known to one person only, which exacerbates the situation. As mentioned in Section 2.1.5 above, none of the General Support Systems has a written System Security Plan.

3.2.2.8 Security Awareness Training

The agency conducts general security awareness training events about once a year. The agency also publishes security tip-sheets and guidelines on its intranet web site. Virtually all users have access to both types of training, but there is no definitive census of attendance. Security awareness training is part of the orientation process for new employees and contractor personnel. Training is conducted by staff of the Litigation and Customer Support Group.

Security awareness material is available on the FTC Intranet site as well as in printed form. The publication "Federal Trade Commission Guidelines for Security" provides good coverage of the topic, combining the agency's policies with practical advice.

3.2.2.9 Incident Response Handling

ITM published a formal "Information Technology Security Incidence Response Policy" (No. 2000-01) in November 2000. Overall the policy is detailed and clear on the subjects of purpose, roles and responsibilities and the actual mechanics of resolving and documenting the resolution of a security incident. One area that lacks a sufficient level of detail concerns who and under what circumstances security staff should report security incidents to FedCIRC and to Law-enforcement agencies (e.g., local police, FBI or OIG).

In practice we have found this policy to be little known outside the small group of people involved in information security or system administration – No program officials were familiar with it. Further more, the prescribed procedures for incident resolution and reporting were most often ignored by the persons involved. Many incidents go unreported. Some of the documented incidents we reviewed have not been fully resolved (at least according to the reporting entity). It is unclear to what extent the ITM Incident Response Team was aware/involved in the resolution process of these incidents and there were no follow up management decisions.

A common opinion among ITM staff is that the security measures are effective in blocking hackers. Staff told us that the traffic filters in the router block 95 percent of the attempts and the firewall takes care of the rest. The OIG believes that such opinion may explain a less than universal recognition of the incident response handling policy and procedures.

3.2.3 Technical Controls

3.2.3.1 *User Identification and Authentication*

Generally users at FTC have login access to one or more of the following systems:

- LAN (including e-mail and NT servers)
- [REDACTED]
- [REDACTED]
- Dial-In System

The user identification and authentication mechanisms vary between these systems and are handled by different groups within the Technology Operations Branch and Litigation/Customer Support (in the case of the CIS application, Bureau of Consumer Protection staff creates the user accounts).

Internal access is controlled by user login ID and passwords. While ITM published a Strong Password Policy (NS 14, October 2000) accompanied by other guidelines and tip-sheets, it is not uniformly implemented and enforced. In NT servers, for example, “weak” passwords are rejected while in other systems they are left for the user’s best judgment. [REDACTED] account passwords are frequently tested with a “password cracker” while [REDACTED] passwords are not.

Remote access via dial-in requires the use of [REDACTED] as a strong authentication measure. Certain web applications such as Sentinel require a digital certificate to authenticate the remote user. These certificates are granted by the FTC Bureau of Consumer Protection and expire after one year.

The Check-in/Check Out process is the primary mechanism for enrolling new users and deleting them from the systems if they leave the agency or move to another position. FTC Form 255 –Application For Access To Automated Systems is required to initialize the enrollment process. The form is sent to the Help Desk which notifies the relevant system administrators via the [REDACTED] system.

The reverse, or check-out, process does not always work to eliminate un-needed access. In our review we found valid network and application level accounts for 36 personnel

who left the agency months and in some cases years ago. Although personnel separation lists are distributed twice monthly to system administrators who are supposed to verify that all accounts have been disabled, this is not consistently practiced.

3.2.3.2 Logical Access Controls

The [REDACTED]-based applications developed at FTC employ the concept and mechanism of “roles” to limit access to certain functions or sections of the database. For example, the Premerger application has the [REDACTED] among other roles. Users are assigned to a role based on their functional needs. Program officials review and approve requests for roles which allow staff to write or modify records but read-access roles are not reviewed by program officials.

Other access control measures are used at the network and operating system levels. NT accounts are assigned to NT Groups based on their organizational unit. This limits a user’s access to resources belonging to their organization’s data. If no organizational affiliation is specified at check-in, users are assigned to the default “domain user” group which allows them access to basic applications (e.g. MS Office) but prevents access to Program applications’ data.

The Internet connection is protected at two levels – the first is level consists of traffic filtering rules embedded in the Internet router operational configuration. The second level consists of two firewalls [REDACTED] which are set in a load-sharing configuration. The firewall rules are set to allow most “well behaved” protocols out but only a limited set of protocols and addresses from the outside into FTC’s network.

The connection to the Department of Justice had a Gauntlet firewall as well, but it was removed due to incompatibility with some of the applications that run across this connection.

The Web and E-mail servers are placed in parallel to the firewalls, between the external Internet Server and the internal FTC network.

3.2.3.3 Audit Trails

The network gear and servers are configured to log significant events:

- Web server logs are downloaded daily and analyzed with a third party product [REDACTED]
- Firewall logs are produced daily and weekly plus a summary log which is e-mailed to Technology Operations staff

- The Internet router generates syslog messages which are forwarded to a syslog server for storage and analysis.
- Key network gear is monitored via a network management system [REDACTED] [REDACTED] server logs are reviewed at least once daily.

3.2.3.4 Systems Interconnections

The FTC network has a number of external interconnection points:

- Direct point-to-point link to Department of Justice
- Direct point-to-point to the Consumer Response Center contractor in Beltsville
- A frame-relay connection to Department Of Interior National Business Center (NBC)
- Remote Dial In access.

The first two links terminate inside the network and are not “firewalled”. The other party is considered informally a “trusted entity”. The NBC connection is terminated “outside the firewall” and the only traffic allowed in is associated with the remote printing service. The remote dial-in service requires SecurID tokens to authenticate the remote user before the user is allowed access to internal resources.

3.2.3.5 Public Access Controls

Some of the recently introduced web-based applications provide access to the public (e.g ID Theft and econsumer.gov web sites. These applications have reasonable measures of protection since they do not allow interactive access to FTC data. For example the Consumer Complaint Form is a “one-way” mechanism for the public to submit complaints the agency. The applications use secure socket layer (SSL) encryption to protect the transmission of the submitted information while in transit. The applications do not provide for subsequent retrieval of information regarding a previously submitted complaint.



UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

06 2017

Re: FOIA-2017-00967
GISRA Report

This is in response to your request dated May 23, 2017 under the Freedom of Information Act seeking access to the cover page, table of contents, and the management response for the following report "GISRA Security Evaluation Report (Non-Public Report) Audit Report Number AR-02-51. Please note the correct number for the report is AR-01-51. In accordance with the FOIA and agency policy, we have searched our records, as of May 23, 2017, the date we received your request in our FOIA office.

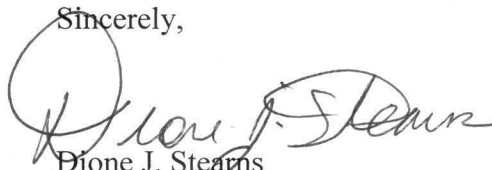
We located 21 pages of responsive records. You are granted full access to the responsive records, which are enclosed.

If you are not satisfied with this response to your request, you may appeal by writing to Freedom of Information Act Appeal, Office of the General Counsel, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580, within 90 days of the date of this letter. Please enclose a copy of your original request and a copy of this response.

You also may seek dispute resolution services from the FTC FOIA Public Liaison Richard Gold via telephone at 202-326-3355 or via e-mail at rgold@ftc.gov; or from the Office of Government Information Services via email at ogis@nara.gov, via fax at 202-741-5769, or via mail at Office of Government Information Services (OGIS), National Archives and Records Administration, 8601 Adelphi Road, College Park, MD 20740.

If you have any questions about the way we are handling your request or about the FOIA regulations or procedures, please contact Anna Murray at (202) 326-2820.

Sincerely,



Dione J. Stearns
Assistant General Counsel

Enc: 21 pages

AR 01-051

**FEDERAL TRADE COMMISSION
OFFICE OF INSPECTOR GENERAL**



AUDIT REPORT
GISRA SECURITY EVALUATIONS REPORT



FEDERAL TRADE COMMISSION
Office of Inspector General
GISRA Security Evaluations Report

Developed By
SeNet International Corporation
"Delivering Practical e-Security Solutions"

September 4, 2001

Table of Contents

Maintaining Competition Program

- 1.1 Program Description**
- 1.2 IT Support Infrastructure**
- 1.3 Evaluation of Security Controls**

Consumer Protection Program

- 2.1 Program Description**
- 2.2 IT Support Infrastructure**
- 2.3 Evaluation of Security Controls**

General Support Systems

- 3.1 Description**
 - 3.2 Evaluation of Security Controls**
-



OFFICE OF THE
EXECUTIVE DIRECTOR

UNITED STATES OF AMERICA
FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

OTB COPY
GISRA I

September 10, 2001

The Honorable Mitchell E. Daniels, Jr.
Director, Office of Management
and Budget
Executive Office of the President
Washington, DC 20503

Dear Mr. Daniels:

Pursuant to OMB Memorandum M-01-24, dated June 22, 2001, enclosed is the Federal Trade Commission's report required under the Government Information Security Review Act.

This report includes an executive summary developed by our Acting Chief Information Officer and our Inspector General. It also includes an agency security program review and the Inspector General's independent evaluation. Our staff is preparing the plan of action addressing issues outlined in our report that will be submitted to OMB by October 31, 2001.

If you have any questions about the report, please contact either Keith Golden, Acting Chief Information Officer (202-326-2410), or Frederick J. Zirkel, Inspector General (202-326-2800).

Sincerely,

Rosemarie A. Straight
Executive Director

Enclosures

P 13 SY TRAINING
8 EXCEPTION REPORT RECOMMENDATIONS



**Government Information Security Reform Act
Chief Information Officer and Office of Inspector General
Executive Summary**

September 10, 2001

The executive summary presents Federal Trade Commission, Information and Technology Management Office (ITM) and Office of Inspector General (OIG) analysis of the review topics identified by OMB memorandum M-01-24, "Reporting Instructions for the Government Information Security Reform Act," dated June 22, 2001.¹ These reporting instructions provide a consistent form and format for agencies to report back to OMB. Each topic in the reporting instructions relates to a specific agency responsibility outlined in the Security Act or OMB Circular No. A-11.

The Government Information Security Reform Act (GISRA) is found in Title X, Subtitle G of the Fiscal Year 2001 Defense Authorization Act (P.L. 106-398). It establishes a mechanism for oversight of Federal Agency information security programs. OMB Memoranda M-01-08 and M-01-24 further define the scope, methodology and reporting format to be followed by agency program officials and OIG's. A summary of ITM and OIG responses pertaining to the OMB topics is provided below.

A. General Overview

1. Identify the agency's total security funding as found in the agency's FY01 budget request, FY01 budget enacted, and the FY02 budget request. This should include a breakdown of security costs by each major operating division or bureau and include critical infrastructure protection costs that apply to the protection of government operations and assets. Do not include funding for critical infrastructure protection pertaining to lead agency responsibilities such as outreach to industry and the public.

ITM Response: The FTC's technology development and operations approach integrates security issues directly into our infrastructure and application development and management processes. OMB staff recognized the FTC's approach and requested that separate requests for individual components of budget requests, such as those related to security issues, not be identified in materials submitted for FY01 or FY02. Virtually all of the 52 FTE assigned to the FTC's central organization responsible for providing information technology products and services, ITM, perform some duties related to computer security. In FY 2000, in addition to the staff and other resources already devoted to computer security, the FTC approved an increase in the staff resources for ITM. With these resources, the agency hired the Computer Security

¹ Per OMB guidance, CIOs working with program officials should respond to all 14 topics identified in OMB M-01-24. OMB asked that OIG's respond to topics 2 - 13.

Officer and a Configuration/Change Manager, who account for approximately 1.25 FTE (\$100,000) in direct computer security costs. However, no estimates of other staff time or costs can be made based upon available information. We have integrated both of those positions into all of the operations of the agency involving information and technology management. The work of these two staffers is a component of our computer security program.

OIG Evaluation: Per OMB instructions, the OIG did not evaluate security funding.

2. Identify the total number of programs included in the program reviews or independent evaluations.

ITM Response: To respond to the reporting requirements under GISRA, the FTC identified three "programs." Those are the agency's two official missions, Maintaining Competition and Consumer Protection, and General Support systems.

OIG Evaluation: By prior agreement with management, the OIG performed its evaluation within the framework of the three program areas identified by management.

3. Describe the methodology used in the program reviews.

ITM Response: The Office of the Chief Information Officer employed the Information Technology Security Assessment Framework approach developed by the National Institute of Standards and Technology (NIST) to assess the computer security aspects of the General Support Systems and Major Applications of the agency.

OIG Evaluation: The OIG contracted with an independent information security consulting firm to assist in conducting this review and to prepare the OIG portion of the report. The review followed the CIO/NIST Information Technology Security Assessment Framework used by management and was performed in accordance with Government Auditing Standards. To address the review objectives, the team:

- Analyzed GISRA, OMB A-130 and other relevant security directives in order to establish evaluation and reporting criteria;
- Met with the Acting CIO and the FTC Computer Security Officer to define a framework of cooperation for this effort to include coordination of activities and schedules;
- Reviewed information security documents produced and maintained by ITM including past security risk assessments, self assessment questionnaires, information security policies, plans and procedures, as well as security training material and "tip sheets" distributed to FTC employees and contractors;

- Interviewed key program and IT operations staff to fill in gaps in the collected information and to gauge the level of adherence to established FTC security policies and procedures;
- Validated key security controls via requests to system operators to demonstrate parameter settings or produce logs and reports; and
- Discussed our findings and recommendations with the CIO.

4. Report any material weakness in policies, procedures, or practices as identified and required to be reported under existing law. (Section 3534(c)(1)-(2) of the Security Act).

ITM Response: No material weaknesses were identified during the security reviews, although areas for improvement were noted. Those areas will be addressed in the Plan of Action that will be submitted to OMB by October 31, 2001.

OIG Evaluation: The OIG has identified two material weaknesses and five reportable conditions that are summarized below. Reportable conditions are matters coming to the auditor's attention relating to significant deficiencies in the design and operation of the information technology program that, in the auditor's judgment, could adversely affect the Commission's ability to record, process, summarize and report data consistent with mandated security objectives. Material weaknesses are reportable conditions in which (i) the risk of eventual harm or abuse approaches near certainty, and (ii) failures may occur and not be detected in a timely period.

Material Weakness 1. – *There is no documented security policy for the three programs identified by management (see topic #2 above) as required by OMB A-130 and other government guidelines.*

According to NIST, a documented security policy ensures adequate and cost effective organizational and system security controls. A sound policy delineates the security management structure, clearly assigns security responsibilities and lays the foundation to reliably measure progress and compliance.

The Federal IT Security Assessment Framework (Framework) developed by NIST identifies five levels of IT security program effectiveness.² The five

² The "Framework" approach begins with the premise that all agency assets must meet the minimum security requirements of OMB Circular A-130, "Management of Federal Resources," Appendix III, "Security of Federal Automated Information Resources" (A-130). The criteria that are outlined in the

levels measure specific management, operational and technical control objectives. Level 1 requires that the FTC have a formally documented and disseminated security policy covering its three major programs. Policy documentation should address, at a minimum, the purpose and scope of the policy, the person(s) responsible for implementing the policy, and the consequences and penalties for not implementing the policy. Subsequent levels build on this basic foundation, culminating with the highest level of security preparedness, Level 5, in which the organization has "fully integrated procedures and controls."

As the FTC does not have a documented security policy for any of its three major programs the OIG has concluded that the FTC has not achieved a level one security rating in accordance with NIST guidelines.³

Material Weakness 2 – Established security procedures were not routinely documented or followed in the general support program area. Further, the agency's contingency plan is outdated.

Level 2 of the NIST Framework requires formal, complete and well-documented procedures for implementing policies established at level one.

The OIG found that documented procedures were largely not prepared in the general support program area. Although the OIG does not believe there is imminent danger of disruption to operations, the FTC relies substantially on the critical knowledge of a few individuals. Documentation of technology configuration would provide a needed blueprint into current IT operations and would mitigate reliance on those individuals.

Contingency planning allows individuals to determine how best to secure data and maintain the agency's IT resources should a disaster; e.g., flood, electrical outage, fire, etc., occur. OMB guidelines require that the plan be reviewed annually and revised as appropriate. The agency's contingency plan was last updated in 1997. It identifies many systems that no longer exist at the agency, while other newer systems are not mentioned. The OIG believes that this deficiency likely contributed to the protracted loss of services resulting from a recent power outage. In this instance, computer room staff did not follow proper

"Framework" are abstracted directly from long-standing requirements found in statute, policy, and guidance on security and privacy.

³ ITM management told the OIG that agency size and IT staff experience lessen the need for formal documentation as required by OMB A-130. To a large extent the OIG agrees that ITM can efficiently and effectively meet the agency's IT needs without the need to document every system and procedure. However, a certain baseline level of documentation is needed, at least for the 12 major system applications selected for review by the OIG, to ensure that the agency maintains its focus on providing adequate security and that the agency is protected from unforeseen events.

shut-down procedures, causing certain applications to remain offline for upwards of 30 hours.

Moving to Level 3 of the framework requires that IT security procedures and controls to be implemented in a consistent manner and reinforced through training. Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged. Security controls for an asset could be implemented and not have procedures documented, but the addition of formal documented procedures at level 2 represents a significant step in the effectiveness of implementing procedures and controls at level 3.

In select areas where documentation does exist, the OIG found security procedures were not always followed. Most serious were those procedures requiring IT staff to periodically check network and applications "user lists."⁴ (FTC Administrative Manual, Section 550)

Beginning with an OIG report issued on December 23, 1996⁵ and in subsequent reviews, the OIG has reported to management that controls were not implemented to ensure that all former employees are removed from network access and other sensitive applications when they leave the agency. Comparing separation reports against active IT user lists, the OIG found significant numbers of employees that had valid network, email, and other application access for months and in some cases years after leaving the Commission. In all cases, management quickly removed all former employees from these lists once identified by the OIG. An Investigative Alert (99-07) issued on January 20, 1999 regarding email vulnerabilities identified 256 active email accounts belonging to former staff. When brought to its attention, ITM management again deleted the invalid accounts. While management has reacted quickly, it appears that little has been done to implement controls to prevent future occurrences, as illustrated below.

For example, in this GISRA review, the OIG once again identified employees who left the agency as far back as December 1998 who still had active network accounts. The OIG identified valid network accounts for 36 personnel who left the agency. Ten of the 36 separated in 1998 or earlier; four left the agency in 1999; and 15 separated in 2000. The remaining seven employees left the agency in 2001.⁶

⁴ Personnel separation lists are distributed twice monthly to system administrators to verify that all accounts have been disabled. A cross check against active accounts would identify accounts to terminate.

⁵ See "Review of the Federal Trade Commission's Computer Systems Security," AR 97-034.

⁶ It is possible that some of these employees may have returned to the agency as contractors. The OIG could not determine from readily available information the extent of this occurrence.

The OIG also noted that the agency's IT Security Incident Response Policy (No. 2000-01) is not always followed. This vulnerability can lead to wrong doing by agency staff not being detected timely, and/or external attacks not being reported to senior management consistently. The incident policy is not well known outside the small group of people involved in information security or system administration. As a result, many incidents go unreported. Incidents that were fully resolved did not contain evidence of followup with management.

The OIG found no indication that senior management is routinely made aware of events affecting agency information resources. Although six incidences were reported, the OIG suspects that, based on interviews with both program officials and technical operations staff, dozens more were "resolved" by operations with no reports prepared. Short cutting the Incidence Response Policy means there is little, if any, effective management oversight as no records are maintained as to incident types or their ultimate resolution.

Reportable Condition 1 – No reporting on internal incidences.

The OIG found no internal reporting on IT resource usage. Far from monitoring individual employee habits, such activity reports could be designed and produced to identify egregious exceptions to what is considered normal usage of ITM resources by agency employees. For example, it may be of little interest to management to know the amount of time all employees spend "surfing the web" each week. On the other hand, an employee's supervisor may be very interested in knowing that an employee within his/her organization was identified as one of only five agency employees who exceeded 16 hours a week "surfing." Once alerted, the supervisor could make a determination whether this level was appropriate given the employees' job responsibilities, or whether there is potential abuse taking place.

Reportable Condition 2 – Inadequate separation of duties among ITM staff.

Separation of duties is the practice of allocating the work of a vulnerable function among different individuals. The OIG noted that a senior staff person in technology operations is the sole producer and custodian of security-related reports that, among other things, would enable the security officer and/or the CIO to review the performance of operations. The OIG believes that the security officer needs direct access to system logs as a check on not only the larger FTC community but on ITM employees as well.

Reportable Condition 3 – No periodic Risk Assessments.

Program managers do not adequately integrate security into their program's life cycle. The OIG was told in interviews with program staff that they

believe that security is the responsibility of ITM, not program staff. After a system or an application has been moved to production there are no periodic risk assessments by either ITM staff or bureau program managers, per requirements in OMB A-130. As program staff is removed from the process and given no risk assessments are periodically performed, security considerations are, in effect, addressed only at the front end of the system application lifecycle.

Reportable Condition 4 – Reliance on external organizations for security.

The FTC relies on security procedures at other Federal, state, local and foreign law enforcement organizations to ensure security of select FTC information resources. In the Consumer Protection program, there are executed confidentiality agreements with each law enforcement organization; however, these agreements do not detail security processes and procedures and no checks are performed by the FTC to verify security requirements. The agreements reviewed by the OIG were silent on expiring certificates and deleting employees from user lists when they separate. However, management informed the OIG that certificates are issued to specific personal computers identified by users and expire every 12 months and that certificates can only be renewed by the law enforcement personnel reapplying for an additional 12 months.

In the Maintaining Competition program, no formalized process is in place to routinely ascertain that the rights to access FTC applications by former Department of Justice employees are revoked once they leave that agency. Further, the OIG found no MOU with DOJ detailing security processes and procedures.

Reportable Condition 5 – Security Officer responsibility is not clearly defined nor well integrated into ITM operations.

The newly created position of Computer Security Officer (April 2000) does not, in the opinion of the OIG, possess the authority to effectively monitor and report on IT resource usage by agency employees or external threats. As noted earlier in this document, the Computer Security Officer must often rely on others, especially ITM operations staff for security-related information and the content and format of the reports that are available. The security officer, under the guidance of the CIO, needs to identify the information required to effectively evaluate system security and to independently produce reports as needed. If required, technical training should be provided.

OIG Recommendations: To address the two material weaknesses (MW) and five reportable conditions (RC) identified in the OIG's evaluation, the OIG recommends that the CIO, in conjunction with program officials, do the following:

Recommendation 1 – Develop an agency-wide system security plan along with security policies for each of the three program areas (CP,MC and GS). (MW -1)

Recommendation 2 – Develop System Security Plans for the 12 major systems/ applications identified in this report. Update security policies and procedures annually including the agency contingency plan in keeping with Circular A-130. Periodically test various aspects of the plans for correctness and training of staff. (MW - 2)

Recommendation 3 – Disseminate the Incidence Response policy to all program and ITM employees including contractor staff. Define what constitutes an “incident” for reporting purposes. Provide the computer security officer with the necessary authorities to adequately fulfill the position’s mandate. (RC - 1 & 5)

Recommendation 4 – Enhance “internal security” controls by identifying areas of potential abuse of IT resources, and producing exception reports. Unusual activity as noted on the exception report should be provided to employee supervisors for follow up. Strengthen procedures to remove inactive or unauthorized accounts. (MW - 2, RC - 1)

Recommendation 5 – Review current practices and redefine roles and responsibilities to ensure no single individual possesses all knowledge and access to security information. (RC - 2)

Recommendation 6 – Work with program officials to conduct periodic security reviews of their applications and systems to ensure that risks are addressed throughout their life-cycle. (RC - 3)

Recommendation 7 - Accounts of external users (i.e., not FTC staff) should be limited in duration and renewed after an affirmative endorsement as received from the external organization. In addition ITM needs to conduct periodic reviews of internal users’ accounts to eliminate outdated access privileges in a timely fashion. (RC - 4)

Recommendation 8 - Service level agreements need security requirements to be detailed and verified periodically. Specifically, FTC should (i) modify and implement the Department of Interior *Products & Services Security Administration Data Custodian Responsibility Statement* (NBC PS-01) to reflect two-way responsibility; (ii) inspect call center contractor premises to ensure complete separation of contractor and FTC networks; and (iii) exchange an MOU with Department of Justice concerning

security responsibilities of both sides. (RC -4)

B. Security Program Performance

5. The specific measures of performance used by the agency to ensure that agency program officials have:

5.1) assessed the risk to operations and assets under their control;

ITM Response: The ITM Board of Directors reviews major proposals to develop information technology products and services and approves those that both meet the law enforcement needs of the agency and are, conceptually, appropriately designed. The Board of Directors reviews the recommendations of agency program staff who have identified specific needs that can be met through technological services and recommendations from ITM staff who have determined that the requested services can be met within the security and cost constraints imposed on the agency. The Board of Directors decides to approve new technological approaches after assessing the costs of developing and operating the approach, the benefits to be gained through the approach, and the risk to other agency operations.

OIG Evaluation: The OIG identified no performance measures in this area. Generally the agency does not conduct risk assessments on a regular basis - not agency-wide nor application specific as required by A-130. The last agency-wide risk assessment was conducted over two years ago. The ITM Board of Directors does not require a formal risk assessment as a pre-requisite for the initiation of a new application effort.

5.2) determined the level of security appropriate to protect such operations and assets;

ITM Response: The CIO, who is the program official responsible for the agency technology infrastructure, is held accountable for its security through his annual performance reviews. The CIO works in concert with other agency managers to establish an appropriate balance between access that permits agency staff to conduct law enforcement and research efforts effectively and security that prevents unauthorized access to agency resources. Agency managers hold responsibility for granting and maintaining access rights of individuals and groups to specific applications that operate on the agency technology infrastructure. Those agency managers, who are most knowledgeable about the specific needs of the programmatic area supported by an application, are permitted to assign access rights based upon roles established by the CIO. The CIO has established and publicized "rules of behavior" that apply to all agency technology resources.

OIG Evaluation: The OIG identified no performance measures in this area. Overall, security needs are taken into consideration primarily from the technical perspective. Program managers' involvement concentrated in granting access rights to program applications under their control. No applications had specific security training plans or "rules of behavior" codes for use by staff, as required by OMB A-130.⁷ Program managers must review and endorse these.

5.3) maintained an up-to-date- security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control;

ITM Response: The FTC has not used a consistent, formal methodology for documenting the security considerations and plans associated with individual parts of our infrastructure or applications. Security issues are addressed in all phases of the design, implementation, maintenance, and operation of every component of our technology. Potential threats or vulnerabilities are assessed by ITM staff based upon the anticipated location of the product being developed within the agency infrastructure and the sensitivity of the information to be stored. During the implementation phase, security controls are installed and tested to ensure that the conceptual designs meet actual requirements. Throughout the operation cycle, security controls are maintained to ensure that evolution of the system or application has not altered the security requirements. Finally, periodically, a separate assessment of both the system or application and its security structure is conducted and evaluated.

OIG Evaluation: None of the agency's 12 major system applications⁸ had specific dedicated security plans, nor does the agency have a current, up-to-date security program plan as required by A-130 for any of its three major programs identified in Response 2. Based on interviews, the OIG believes that security is considered primarily at the front end of the process with significantly less attention being provided as systems age. No performance measures exist to help ensure that such plans are developed and revised in keeping with A-130 guidance.

⁷ Rules of behavior are the rules that have been established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system, and should cover matters such as work-at-home, dial-in access, connection to the Internet and unofficial use of Federal government equipment.

⁸ The OIG reviewed four major applications from each of the three program areas identified by management. MC Mission: Matter Management System, Premerger Notification System, Clearance Notification System and Document Management System; CP Mission: Consumer Information System, Business Intelligence Reporting, Identify Theft, eConsumer.gov and other web-based systems; and General Support: LAN and Network infrastructure, E-mail, Internet Access and Applications, Data Warehousing.

5.4) tested and evaluated security controls and techniques.

ITM Response: ITM has implemented a Change Management Program that requires that all new technology products, services, and procedures be submitted to an internal review committee at stages of development and immediately prior to implementation. All aspects of the item, including its security may be reviewed and critiqued by the committee to ensure that the item is both appropriate and ready for implementation. As part of the Change Management Program, a separate test facility has been constructed in which most infrastructure and application development can be tested prior to implementation without affecting any production environment.

OIG Evaluation: While the OIG identified no performance measures in this area, some security testing is done as part of a new application development or upgrade effort. Technical security tests are conducted on an irregular basis. The latest external penetration test was conducted in 1998, and a self assessment exercise was conducted in 1999.

6. The specific measures of performance used by the agency to ensure that the agency CIO:

6.1) adequately maintains an agency-wide security program;

ITM Response: As noted above, the CIO is held accountable for areas for which he is responsible through his annual performance reviews. Because of the centralized approach to information technology management employed by the FTC the bulk of computer security responsibilities lie directly within ITM, the organization led by the CIO. ITM works in partnership with staff throughout the agency who share management, and therefore some level of responsibility for security, of agency information and technology resources. That partnership ensures that all parts of the agency are aware of procedures and responsibilities. The CIO has established an independent Computer Security Program with oversight authority over all aspects of computer security at the FTC.

OIG Evaluation: The OIG identified no performance measures in this area. While not following a prescribed, documented Security Program Plan, the OIG did observe that the CIO has initiated multiple activities to assess and/or improve the security posture of the Commission. These included:

- Requesting an external Security Test & Evaluation study by the National Security Agency in 1998;
- Initiating an internal Security Review covering threats, risks and vulnerabilities to FTC's IT infrastructure in 1999;

- Appointing a full time Computer Security Officer in 2000 reporting directly to the CIO;
- Issuing new policies in the areas of Incident Handling (Nov. 2000) and Configuration Management; and
- Issuing a “strong password” policy (Oct. 1999).

The CIO’s actions, by themselves, were not sufficient to define and document a detailed security program as required by public law. The undated draft of FTC’s IT security program policy reviewed by the OIG audit team lacked major details regarding human resources, budget allocation and target schedules. Program managers’ security responsibilities were limited to granting access approval to bureau applications. ITM staff told the OIG that a draft policy is being considered that will include outlines of program goals; staff responsibilities to include the CIO, security officer, and program staff; and address compliance.

6.2) ensures the effective implementation of the program and evaluates the performance of major agency components;

ITM Response: The CIO holds the Computer Security Officer accountable for the implementation and operation of the agency Computer Security Program. Again, because of the nature and structure of the FTC, the components of the agency play a supporting or partnering role on computer security. ITM holds primary responsibility for the agency program. The Computer Security Officer conducts periodic reviews of various systems and applications and makes recommendations for improving both overall and specific security.

OIG Evaluation: The OIG identified no performance measures in this area. Since the CIO has not created a formal security program, the OIG was unable to assess implementation against stated goals.

6.3) ensures the training of agency employees with significant security responsibilities.

ITM Response: ITM has a strong history of providing staff with training, both formal and on-the-job, needed to accomplish their responsibilities. The Computer Security Officer regularly attends general training sessions concerning a broad range of issues related to computer security. ITM follows a practice of providing training to other technology staff on computer hardware and software that is either already part of our infrastructure or that we intend to incorporate in the near future. Security features of that technology are integral parts of those training opportunities. We believe that training in the specific security aspects of those products helps to ensure that they are implemented appropriately in our environment.

OIG Evaluation: The OIG identified no performance measures in this area. While training does occur, IT personnel did not receive training that focused exclusively on security-related topics. For example, technical operations staff with responsibility for security in ITM told the OIG that they have not attended technical security training classes (specific for the technology in use at the FTC). The OIG found no plan for training agency employees with significant security responsibilities. It appears IT personnel receive technical security training only as part of other training programs. For example, system administration staff attended an NT Operating System class which covered security aspects of the system.

7. How the agency ensures that employees are sufficiently trained in their security responsibilities. Identify the total number of agency employees and briefly describe what types of security training was available during the reporting period, the number of agency employees who received each type of training, and the total costs of providing such training (Section 3534(a)(3)(D), (a)(4), (b)(2)(C)(i)-(ii) of the Security Act).

ITM Response: The agency implemented a computer security awareness and training program several years ago and actively promotes security with employees at all levels. The training program includes initial computer security training to newly assigned personnel concurrent with being granted access to FTC information systems, periodic notices related to various aspects of computer security, and an annual computer security awareness session. During the initial and annual training sessions, attended by approximately 600 staff, employees were instructed on their responsibilities as users of FTC information systems, including items such as password protecting systems, never sharing user privileges, understanding security policies and where to obtain them, never leaving workstations unattended, and knowing who to contact if in the event of a possible security compromise. The annual training sessions consist of presentations by security experts, demonstrations showing how to institute safe computing practices, and other approaches. Approximately 600 staff attended the initial training, the annual sessions, or both. We estimate that the nonsalary cost of providing those sessions was approximately \$600.00. In addition, special, formal notices were distributed to the agency's entire 1,049 FTE periodically outlining agency policy and practice covering such issues as security violations, working at home, remote access, acceptable use of government equipment, and connecting to the Internet. Computer security information is also posted on the agency Intranet.

OIG Evaluation: Over 1000 federal employees and 50-200 contract/temporary employees use the agency's IT resources. All staff members receive some security training as part of their orientation. However, there is no special security training for the agency's major applications, and such training is not a prerequisite for access. The agency conducts security awareness training events about once a year (attendance is not mandatory). The agency also publishes security tip-sheets and guidelines on its intranet web site. Virtually all users have access to both types of training. The cost of providing these training programs was not readily available. Security training is also conducted informally through one-on-one discussions, for example by the help-desk to end users or by the Security Officer to Program Managers.

8. The agency's documented procedures for reporting security incidents and sharing information regarding common vulnerabilities. Include a description of procedures for external reporting to law enforcement authorities and to the General Services Administration's FedCIRC. Include information on the actual performance and the number of incidents reported. (Section 3534(b)(2)(F)(i)-(iii) of the Security Act).

ITM Response: The Computer Security Officer has implemented an information security incident response policy and procedure that covers the five stages of proper handling of an incident: Incident detection practices: Identification of threats; Process for reporting incidents; Assignment of incidents; and Status and final report. That policy does not cover incidents, such as the recent "Red Code" worm attack, that are known and addressed in advance. In FY2001, six incidences were reported through that process. The Computer Security Officer notifies FedCIRC if she believes that an incident is of a criminal nature or appears to have an impact beyond the FTC.

OIG Evaluation: The FTC's Information Technology Security Incident Response Policy (No. 2000-01) became effective on 11/20/2000. Overall the policy is detailed and clear on the purpose, roles and responsibilities, and the actual mechanics of resolving and documenting the resolution of a security incident. However, it does not identify who and under what circumstances staff should report security incidents to FedCIRC and to law-enforcement agencies (e.g., local police, FBI or OIG).

Based on interviews with program staff and ITM employees, we found this policy to be little known outside the small group of people involved in information security or system administration. Consequently, the prescribed procedures for incident resolution and reporting were not carried out by the persons involved. Many incidents go unreported. It is unclear to what extent the five-member ITM Incident Response Team was aware/involved in the resolution process of these incidents.

9. How the agency integrates security into its capital planning and investment control process. Were security requirements and costs reported on every FY02 capital asset plan (as well as exhibit 53) submitted by the agency to OMB? If no, why not? (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act).

ITM Response: The FTC's capital planning and investment control process requires that ITM staff, and, if appropriate, staff from other organizations within the agency, recommend to the ITM Board of Directors that a new product or service be developed and implemented. Any special security requirements of a proposed product or service are noted in the recommendation. As noted above, OMB staff did not require the FTC to submit exhibit 53 during planning for FY02.

OIG Evaluation: There were no separately-identifiable security line items noted in the FY 2001 budget submitted to OMB. Requests for security initiatives or technology go through

the normal budget process. "Exhibit 53" was not available for review for the reason explained above.

10. The specific methodology (e.g., Project Matrix review) used by the agency to identify, prioritize, and protect critical assets within its enterprise architecture, including links with key external systems. Describe how the methodology has been implemented. (Sections 3535(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act).

ITM Response: As a small agency, the FTC was not required to create an enterprise architecture under Presidential Decision Directive 63. The limited and consolidated nature of our architecture has allowed the agency to operate very successfully without the documentation that would be critical in a more complicated environment. However, we do recognize the benefit of documentation, have begun to create documentation appropriate to our needs, and plan to complete the "base line" component of the project by the beginning of calendar year 2002. Creation and maintenance of the enterprise architecture documentation is under the leadership of the Change/Configuration Manager. We believe that tying the architecture documentation to the change process will ensure that the documentation is updated effectively. The Computer Security Officer is a member of our Change Management Committee and reviews all proposed changes to our infrastructure and applications as they progress through the development and implementation phases to ensure that we give appropriate considerations to the security of those products.

OIG Evaluation: An effort by management to catalogue and prioritize the agency's IT infrastructure has been undertaken as part of the Y2K effort. ITM has recently compiled a list of projects, titled "FY2001 GISRA Designation of Matters," categorizing these activities as "Major Applications," "General Support Systems" or "Other." The list does not attempt to prioritize or assign criticality ranking to these initiatives.

11. The measures of performance used by the head of the agency to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system. Include information on the actual performance. (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act).

ITM Response: The ITM Board of Directors, very senior agency managers, and the CIO are individually held accountable for the success of the program areas for which they are responsible through their annual performance reviews. Computer security is integrated throughout the ITM life cycle process to ensure security is performed during any major systems event or change. When the detailed Security Plans are finalized, the life cycle process will be formally altered to ensure that changes to the plans are incorporated into the process.

OIG Evaluation: For FY 2001, the OIG did not identify any measures of performance pertaining to IT in general or computer security specifically. Similarly, no internal measures were identified.

12. How the agency has integrated its information and information technology security program with its critical infrastructure protection responsibilities and other security programs (e.g., physical and operational). (Sections 3534(a)(1)(B) and (b)(1) of the Security Act).

ITM Response: The FTC has a Computer Security Officer and a Personnel and Physical Security Officer. These two individuals work together in divisions of the Office of the Executive Director and work together closely on many issues. This approach is designed to ensure cooperation and redundant oversight. As an example, the Personnel and Physical Security Officer is responsible for conducting security background screening for new government and contractor employees. The Computer Security Officer also monitors the progress of all staff and contractors who occupy positions with special access to either information or technology. The two security officers worked together to review the physical security and environmental controls in place in our central computer facility.

OIG Evaluation: Informal coordination between the physical/personnel security officer and the computer security officer exists. For example, there was an effort recently to classify IT personnel job descriptions for the purpose of conducting background checks. As the agency is not subject to PDD 63, critical infrastructure protection responsibility does not apply.

13. The Specific methods (e.g., audits or inspections) by the agency to ensure that contractor provided services (e.g., network or website operations) or services provided by another agency are adequately secure and meet the requirements of the Security Act, OMB policy and NIST guidance, national security policy, and agency policy. (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Security Act).

ITM Response: FTC government staff carefully review and inspect the products and services provided directly to the FTC by contractors, providing a level of assessment and quality control. That approach has ensured that work provided by contractors has met the needs and requirements of the FTC. In situations where services are provided by other agencies, FTC staff have reviewed the concepts of the security of data transmission between the FTC and the other agency, but we have not performed audits or inspections of the actual transmission practices or of other operational practices of the agency. Our Plan of Action will include actual reviews of the interactions with other agencies.

OIG Evaluation: Contractor personnel employed on site are subject to the same security requirements as FTC staff. The OIG was informed that all IT contractor staff undergo background checks. However, there are no consistent methods or measures employed by ITM to ensure that outside service providers maintain the agency's security standards. For example, the long-term agreement of the agency with its payroll and accounting outsourcing bureau (Department of Interior) does not cover security requirements beyond a brief mention of the phrase "system security." Security requirements were defined in greater detail in another outsourcing contract (Call Center operations), but no reviews of the Center are conducted to ensure these requirements are met.

14. Each agency head, working with the CIO and program officials, must provide the following information to OMB by October 31, 2001. Provide a strategy to correct security weaknesses identified through the annual program reviews, independent evaluations, other reviews or audits performed throughout the reporting period, and uncompleted actions identified prior to the reporting period. Include a plan of action with milestones that include completion dates that: 1) describes how the agency plans to address any issues/weaknesses; and 2) identifies obstacles to address known weaknesses.

ITM Response: ITM will submit a Plan of Action to OMB by October 31, 2001 that addresses each of the areas for improvement identified by ITM and OBM.