Office of Inspector General

**Review of Federal Information Security Management Act
Corrective Actions for July 2004 – March 31, 2005**

FEDERAL TRADE COMMISSION
WASHINGTON, D.C. 20580

TO: Stephen Warren
           Chief Information Officer

FROM: Howard L. Sribnick
           Inspector General

SUBJECT: OIG Review of Corrective Actions Reported to OMB (AR 05-066)

The Office of Inspector General (OIG) completed its review of the Federal Trade Commission's (FTC) Plan of Action & Milestones (POA&M) submission to the Office of Management and Budget (OMB) for the 4th Quarter of Fiscal Year (FY) 2004 through the 2nd Quarter Fiscal Year (FY) 2005. The purpose of this review was to evaluate Information & Technology Management's (ITM) progress in correcting weaknesses identified in previous Government Information Security Reform Act (GISRA), Federal Information Security Management Act (FISMA) and agency-sponsored security reviews.

A POA&M is the authoritative and comprehensive agency management mechanism used to prioritize, track, and manage all agency efforts to close security performance gaps. In addition to identifying tasks that need to be accomplished, it also details resources required to accomplish the elements of the plan, any milestones in meeting the task and scheduled completion dates for the milestones. POA&Ms are used, in part, as a basis for OMB's assessment of agency IT security status as part of the President's Management Agenda Scorecard under the e-Gov score.

FY 2004 POA&M Overview

For the first three quarters of FY 2004, the OIG reviewed ITM submissions to OMB as part of its FY 2004 FISMA reporting. The results of this review are included in the OIG FISMA report (AR 04-061). The OIG concluded that ITM made significant progress in improving its POA&M management program. Most significantly, ITM implemented an OIG recommendation to track all significant weaknesses from other security reviews and studies as well as from FISMA evaluations. This ensures that the universe of security weaknesses are identified and tracked on one document in keeping with OMB requirements. ITM also improved its POA&M recording, tracking, correcting and reporting processes, and its methodology for recording changes to milestones and corrective actions.

The OIG and ITM continued to work together to review completed corrective actions on a quarterly basis to confirm that remedial actions addressed the identified vulnerabilities.

FY 2005 POA&M Review

The scope of the current review covers the 4th quarter of FY 2004, and the 1st and 2nd quarters of FY 2005 (July 1, 2004 – March 31, 2005). During this period, ITM identified 127 weaknesses: During the same period, ITM closed 36 weaknesses from this and prior periods. The OIG reviewed these closed items and the actions taken by ITM to close them. The results of this review are presented below. The OIG concurred with ITM's disposition of these 36 items based on information provided by ITM and independent verification by OIG's IT auditors when applicable. [1]

Review Methodology

To verify that actions taken by ITM addressed the identified vulnerability, the OIG reviewed completed milestones, policies, and other related documents and, when possible, used screen captures and conducted walk-throughs to confirm that corrective actions were effective. The review team also interviewed personnel implementing the corrective actions. The completed actions and the OIG's analysis are presented below.

Recommendations

Although the primary focus of this document is to confirm that corrective actions reported to the Office of Management and Budget were implemented, the OIG also made three recommendations to strengthen corrective actions made by ITM or to address vulnerabilities not specified on the POA&M that are related to the corrected POA&M item. Each recommendation appears within the specific POA&M writeup.

Review Results

Weakness 1: Certify and accredit seven (7) major applications (MA) and the general support system (GSS)

Source: FY03 OIG Review

ITM Actions: ITM completed certification & accreditation (C&A) packages for all major applications and general support systems.

OIG Analysis: OIG reviewed C&A packages for the following systems:

- Do Not Call (DNC)
- e-Premerger
- Documentum
- Matter Management System (MMS)
- Consumer Information System (CIS)
- Federal Financial System (FFS)
- Infrastructure

---

[1] ITM reported 36 closed POA&Ms items to OMB during the period of review. The OIG determined that many POA&M items were identified twice by ITM to facilitate internal tracking. The OIG chose to identify each item once, resulting in 24 unique POA&M items identified and reviewed in this report.

The Department of the Interior (DOI) owns FFS and is, therefore, responsible for certifying and accrediting that system. The FTC relied this year on an SAS-70 report provided by DOI OIG for security assurances.[2]

During the prior year review, the OIG reviewed the C&A package provided to the FTC by the Department of Interior's OIG (without the risk analysis). The following table lists the key documents found in the C&A package.

System Name	System Type	Risk Assessment (Required)	Security Plan (Required)	C&A	ST&E or Vulnerability Report (Required)	POA&M (Required)	Privacy Impact Assessment (If Needed)	C&A Letters (Required)	Self-Assess-ment	MOU
Documentum	MA	✓	✓	✓	✓	✓		✓		
FFS	MA	✓	✓	✓	✓	✓ (FTC)		✓	✓	
MMS	MA	✓	✓	✓	✓	✓		✓		
CIS	MA	✓	✓	✓	✓	✓	✓	✓		
e-Premerger	MA	✓	✓	✓	✓	✓	✓	✓		
Do Not Call	MA	✓	✓	✓		✓		✓		✓
Infrastructure	GSS	✓	✓	✓	✓	✓		✓		

The OIG noted that the DNC C&A package did not include a System Test and Evaluation (ST&E).[3] FTC's C&A policy states that the C&A should contain the following documents:

- **Security Test & Evaluation** (*Emphasis added)*
- Risk Assessment
- System Security Plan
- Privacy Impact Assessment
- Plan of Action & Milestones
- Certifier's Statement

The National Institute of Science and Technology (NIST) Special Publication (SP) 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, does not specifically require an ST&E for accreditation; only that the C&A package contain the following documents:

- Approved System Security Plan
- Risk Assessment
- Plan of Action & Milestones

SP 800-37 also states that appendices in the security plan may contain other key security-related documents such as privacy impact assessments, contingency plans, incident response plans, configuration management plans, security configuration checklists, and any system interconnection agreements. ITM representatives also stated that Telos is in the process of conducting the ST&E for DNC.

As NIST 800-37 does not specify the content of an ST&E, and since ITM is performing a more comprehensive ST&E in FY 2005 of the DNC contractor, the OIG accepts ITM's disposition of this item.

OIG Status: Closed

---

[2] A Statement of Accounting Standards (SAS) 70 report presents the results of security control reviews for organizations providing services to other agencies, organizations, groups, etc. System controls are evaluated by an independent reviewer and provided to these "customers."
[3] The package contained a vulnerability scan. ITM has informed the OIG that it will rely solely on vulnerability scans alone in future ST&Es.

Weakness 2: Conduct risk assessments on all MA's and the GSS

Source: FY03 OIG Review

ITM Actions: ITM completed risk assessments for all MAs and GSS in its domain. (Note: FFS is not in the FTC domain.).

OIG Analysis: OIG reviewed C&A packages for FTC's major applications and its general support system. Risk assessments were found for the following systems:

- Do Not Call (DNC)
- e-Premerger
- Documentum
- Matter Management System (MMS)
- Consumer Information System (CIS)
- Federal Financial System (FFS)
- Infrastructure

OIG Status: Closed

Weakness 3: FTC.BUY – Password stored in clear text

Source: Agency Review

ITM Actions: FTC.BUY is an "off the shelf" procurement package with modifications tailored to FTC requirements. User passwords are encrypted and are now required to be changed at least every 90 days. However, the Oracle database access password and user ID are not hidden. Rather they are identified in clear text in a system file. The password and user ID control access to the procurement program files and must be readable to track user access. All users have access to this file, but do not know in which file the password / user ID is embedded and the location within the file. ITM noted that the application was put into place before the FTC's password policy was implemented.

According to a memorandum from the Chief Information Security Officer to the Chief Financial Officer (CFO) dated August 2004, ITM accepted the risk of storing passwords in clear text.

OIG Analysis: The OIG believes that the factors surrounding the existence of the clear text password mitigate many of its risks. An individual would have to know where to go (which file) and what to look for before he/she could exploit the system. In FY2007, the entire system, including the FTC.BUY component, will be upgraded and/or replaced. ITM told the OIG that no software will contain clear text passwords.   The OIG does not believe that it would be an efficient use of resources to make significant modifications to this system given its life expectancy.

OIG Status: Closed

Weakness 4: Some PCs attached to FTC network have analog phone lines and modems, which may bypass FTC security

Source: VeriSign War Dialing (External Penetration Test)

ITM Actions: ITM developed an *Analog Lines Policy* ITM-2004-16 that states:

- FTC-issued workstations with modems connected to analog lines at FTC facilities shall only be allowed to dial-out. Dialing in is not permitted.
- Fax machines are permitted to have dial-out and dial-in capabilities.
- The Chief Information Security Officer must approve requests for new analog lines for workstations with modems.

ITM maintains a list of fax and modem lines.

OIG Analysis: The OIG reviewed an ITM-provided list of fax and modem lines. To confirm that analog lines were programmed not to accept incoming calls, three modem phone numbers attached to the FTC network were dialed to determine if the modem would accept the call. The numbers called were associated with the library and the financial management system. The OIG verified that these lines did not pick up incoming calls.

However, the OIG noted other modems attached to applications connected to the network that require dial-in capability (e.g., Pitney Bowes system). These systems with dial-in access are not documented.

OIG Status: Closed

Notwithstanding the actions taken by ITM to addresses the observed vulnerability, the OIG believes that ITM should track and monitor all modems and applications that allow dial-in access. The OIG recommends that:

Recommendation 1*: ITM develop and document security controls for modems and systems requiring dial-in access. Security controls should, at a minimum, include:*

- *Limiting access through management, operational, and technical controls*
- *Documenting the phone numbers, locations and POC's for modems and applications allowing dial-in access; and*
- *Monitoring modem usage and investigating suspicious activity.*

Weakness 5: Policy and procedures to secure electronic data in regional offices are needed.

Source: Agency Review

ITM Actions: ITM included procedures for securing electronic data at FTC regional offices in the *Office of Information and Technology Management Central Computer Systems & PBX Disaster Recovery Plan* (DRP). According to the DRP, backup tapes are shipped off site to a tape storage facility on a weekly basis. The DRP identifies the storage sites and contact information for FTC headquarters and each of the regional offices. ITM also provided the OIG a copy of the Regional Office off-site storage procedures.

OIG Analysis: The OIG verified that the policy and procedures on securing electronic data are documented in the DRP. The OIG also reviewed procurement-related documentation for the use of the storage facility and a copy of the regional office storage procedures.

OIG Status: Closed

Weakness 6: Security of home PCs connecting to FTC networks

Source: Agency Review

ITM Actions: The FTC *Remote Access Policy* ITM-2004-11 provides instructions on what users must do to request access to FTC assets. The policy identifies remote access: (i) connection options and restrictions, (ii) training and Security Token responsibilities, (iii) security requirements and security scanning and incident response, and (iv) privacy, acceptable use and the enforcement of security controls.

Users are required to sign a remote access acknowledgement form that identifies the rules that remote access users must follow. Remote access is discussed in ITM annual security awareness training.

The Chief Information Security Officer issued a memorandum to regional administrative officers regarding new procedures for providing new employees with their passwords. These guidelines require employees to review a security slide show presentation and to read and sign a network access acknowledgement form before they receive their passwords. The signed form must be faxed to the Help Desk with 24 hours of acknowledgement. The Operations Assurance branch maintains forms with original signatures.

The *Remote Access Securid Tokens* document provides users with instructions for requesting remote access and returning tokens.

OIG Analysis: The OIG determined that the *Remote Access policy*, the *Remote Access Securid Tokens* document, and FTC Forms 730 (*Remote Access Acknowledgement form*) and 731 (*Network Acknowledgement* form) validate that there are documented policies and procedures for requesting and managing remote access. The OIG confirmed that FTC follows these policies and procedures by validating that both forms (730 & 731) are signed and dated by remote users. Form 730 includes the user name, user signature, token number, and date signed. Form 731 includes the user name and signature, date of training, and the date signed. These corrective actions effectively mitigate this vulnerability. The OIG also inspected a SecurID token and noted that the expiration date is recorded on the back of the token. OIG also obtained and reviewed purchase documentation for the SecurID tokens.

OIG Status: Closed

Weakness 7: Peer-to-Peer file sharing applications on FTC's PCs

Source: Agency Review

ITM Actions: The FTC Administrative Manual, Ch. 550, *Information Technology Usage Policies and Practices* states that:

> 1. A. *Internet Access*. Internet access provided by the FTC is intended primarily for work-related purposes. To the extent possible, users should be aware of an Internet site's primary information content prior to connecting to it. It is the user's responsibility to exercise good judgment when accessing Internet sites and to avoid sites that are inappropriate for use by an FTC user. For example, Internet sites containing sexually explicit, sexually oriented, gambling or related material shall not knowingly be accessed using FTC computer resources, except for law enforcement purposes. Users of FTC-provided computer equipment are not allowed to download or use **peer-to-peer** file exchange software such as Kazaa or Morpheus. Instances of such software will be removed when detected by ITM.

Additionally, FTC annual security awareness training informs users that peer-to-peer software is not permitted on FTC devices. According to notes included in the POA&M package, the FTC Intrusion Detection System (IDS) identifies and removes any peer-to-peer software it finds during scans.

OIG Analysis: The OIG reviewed the guidance found in Administrative Manual Sec.550 and the FTC annual security awareness training and confirmed that policy and training prohibit the use of peer-to-peer software. The OIG also reviewed an e-mail that was generated and sent to users when unauthorized software was found on their workstations. A closed Vantive ticket was also reviewed to confirm that unauthorized software is removed when discovered.[4] Review of FTC's annual security awareness training confirmed that the prohibition of peer-to-peer software at FTC is discussed in security training. OIG also received and reviewed a copy of an eEye Digital Security invoice for the purchase of retina network security scanner software. OIG previously confirmed the installation of the ISS Proventia security appliances in an earlier review. These appliances are used for intrusion detection and for network scanning.

OIG Status: Closed

Weakness 8: DRP vulnerabilities: Record DRP modifications, update the emergency management contact list and include a line of succession for leadership.

Source: FY04 OIG Independent Evaluation

ITM Actions: ITM is now documenting changes to the DRP on the Disaster Recovery change control page on a quarterly basis.

OIG Analysis: Review of the September 2004 and June 2005 DRPs showed that changes to the DRP are recorded. The DRP contains a Disaster Recovery change control page where changes made to the document on November 2004, pp. 40, 41; February 2005, pp. 40, 41; and March 2005, p. 9 were recorded. Comparison of the 1st quarter and 2nd quarter DRPs with the final DRP validated that the DRP is being updated on a quarterly basis.

OIG Status: Closed

---

[4] The Vantive system is a collection of integrated applications that can be used to integrate customer support, help desk, quality assurance/engineering, and remote customers.

Weakness 9: The Senior Agency Information Security Officer position may not be sufficiently independent to act as the Certification Agent (CA)

Source: FY04 OIG Review

ITM Actions: ITM modified the *System Security Certification & Accreditation Policy* (ITM-2004-02). It now states that "… the CA and any individual or organization that the CA may designate to assist in the certification process, shall be independent from anyone directly responsible for the development or day-to-day operation of the system to be certified, and from anyone who is responsible for correcting security deficiencies, if any, that may be identified by the certification process."

OIG Analysis: The OIG's review of the C&A packages found that some of the certification memoranda were signed by the head of the Operations Assurance Branch, an individual with no operations role. In July 2005, the Senior Agency Information Security Officer will become the new OA branch chief. He will thus have dual responsibilities. Since neither position has operations responsibilities, this personnel change will not impact the independence of the certification officer.

OIG Status: Closed

Weakness 10: Master Agreement with AT&T will include relationships with outside vendors

Source: AT&T Risk Assessment

ITM Actions: ITM received Letters of Assurance from AT&T Government Solutions, Inc., relating to TARGUSinfo and West Interactive.

OIG Analysis: OIG reviewed the Letters of Assurance from AT&T relating to TARGUSinfo and West Interactive identifying the FTC security requirements for securing the DNC system. These letters provide assurances to FTC that the DNC security requirements are being followed at TARGUSinfo and West Interactive. Both ITM and OIG relied on these written assurances and did not inspect TARGUSinfo and West Interactive security controls.

OIG Status: Closed

The OIG believes that the agency should take some steps to assure itself that controls are in place and functioning that goes beyond a letter of assurance. This year, for example, ITM is performing an ST&E on select AT&T facilities. While this does provide assurances, it is time consuming and expensive. One alternative is to request SAS 70 reports from the contractor performed by independent reviewers. SAS-70 reports are intended to provide select AT&T customer organizations and their independent auditors with information about the control structure features of services provided by AT&T.

Recommendation 2: *To provide independent assurances that security controls are in place and operational, the OIG recommends that the FTC require AT&T to provide annual SAS 70 reports based on NIST 800-53.*

Weakness 11: Complete Security Plan for Infrastructure

Source: FY03 OIG Review

ITM Actions: ITM developed a security plan for Infrastructure.

OIG Analysis: The OIG reviewed the Infrastructure security plan and confirmed that it is completed. It contains all the required security plan elements.

OIG Status: Closed

Weakness 12: Conduct Security Test and Evaluations for Documentum and Infrastructure
Source: Agency Review, OIG FY03 Audit

ITM Actions: ITM conducted ST&Es on Documentum and Infrastructure.

OIG Analysis: Review of the documents confirmed that ST&Es were conducted for Documentum and Infrastructure. These ST&Es consisted of NMAP and Nessus scans.

OIG Status: Closed

Weakness 13: Configuration management on servers

Source: SAIC UNIX/Oracle Assess

ITM Actions: ITM developed configuration management documentation to address server and desktop configuration management. These documents include:

- *Baseline Win2k Member Server*
- *Desktop Development Standard Operating Procedures* v7, September 20, 2004
- *Exchange 2000 Cluster Server Installation Checklist*
- *Exchange 2000 Server (Non-Cluster) Installation Checklist*
- *Best Practice Guidelines for Building and Securing a SLES 9 Server*
- *Oracle Install* v1 (ORACLE_Install-v1)
- *Configuration Guide for FTC Router/Switches* (Router-Switch_ConfigGuide-v1)
- *Serve Build Procedures*
- *Checklist for new SNAP servers*
- *Best Practice Guidelines for Building and Securing a Solaris 8 Server*
- *Windows 2000 Member Server Installation Checklist*
- *Completed Baseline Build Documentation Check-off Sheets*

OIG Analysis: The OIG reviewed the configuration management documentation provided by ITM. The OIG also reviewed completed configuration management checklists to confirm that operations personnel are using the checklists when building servers. ITM is currently in the process of determining how long to retain and file the completed build checklists.

OIG Status: Closed

Weakness 14: Remote Administration Protocols

Source: SAIC UNIX/Oracle Assess

ITM Actions: ITM developed, tested, and implemented remote administration protocols and processes. ITM provided various e-mail and memorandum dated October 5, 2004, stating that the remote administration protocols are implemented. ITM also provided e-mail from a Unix administrator stating that remote administration protocols established for ITM are being followed and terminal server documentation.

OIG Analysis: The OIG reviewed the documentation provided by ITM and confirmed that remote administration protocols were implemented.

OIG Status: Closed

Weakness 15: Controls on Web mail downloads

Source: Agency Review

ITM Actions: ITM provided a memorandum from the Chief Information Security Officer stating that, based on the research conducted, there is no practical way to block the download of Web mail attachments to FTC desktops, while still allowing access to the Web mail itself. As a result, all web mail is currently blocked.

OIG Analysis: OIG reviewed the memorandum and staff notices regarding the blockinig of web mail..

OIG Status: Closed

Weakness 16: FTC Web servers do not have a legal notice

Source: Science Applications International Corporation (SAIC) Demilitarized Zone (DMZ) Vulnerability Assessment 3/5/2004

ITM Actions: ITM developed an FTC Web policy and posted it on the Web site.

OIG Analysis: The OIG reviewed the FTC Web policy and accessed the FTC website http://www.ftc.gov/ftc/sitepolicy/index.htm. The OIG confirmed that the policy is posted on the web. The policy provides guidance on:

- Unauthorized access
- Disclaimer of Endorsement
- Data Quality Act (Section 515)
- FTC's Web Publication Schedule
- Privacy Policy

OIG Status: Closed

Weakness 17: FTC home user vulnerability issues

Source: Unisys Infrastructure Risk Assessment 6/25/2004

ITM Actions: ITM has taken a number of steps to address FTC home user vulnerability issues. The Chief Information Officer (CIO) issued a memorandum introducing FTC's new remote access policy to FTC staff and contractors. An announcement identifying FTC network security requirements for new employees and remote access requirements was posted in an FTC Daily dated October 8, 2004. Finally, FTC personnel are required to sign *FTC-730 Remote Access* and *FTC-731 Network Acknowledgement* forms when they are given remote access capability or access to the network.

OIG Analysis: The OIG reviewed the memoranda and reviewed completed FTC Forms 730 & 731 to confirm that users are signing these documents.

OIG Status: Closed

Weakness 18: The lead incident response investigator lacks forensic software identified in the FTC's Incident Response Procedures

Source: Unisys Infrastructure Risk Assessment 6/25/2004

ITM Actions: The CIO issued a directive stating that the Incident Response Team (IRT) is to use the FTC Litigation Support Branch's forensic software to investigate security violations. ITM owns and uses its own copy of iLook Software. ITM has created a new contract to procure forensic services from the MEGA II contract. ITM plans to stop using internal resources for computer forensics work

OIG Analysis: The OIG reviewed the CIO-issued directive. Additionally, e-mail from a member of the IRT confirmed that the team used the Litigation Support Branch's forensic software in one investigation. OIG then reviewed incident response reports to confirm that ITM had access to forensic software. ITM provided two reports for events that occurred on July 22, 2004, and March 22, 2005. The reports did not specifically identify iLook as a forensic tool used in the investigation, however, they did indicate that security scanning and logging tools such as Nessus, iPrism, as well as virus and spyware detection software are used as part of the forensic investigation.

OIG Status: Closed

Weakness 19: The incident response plan/procedures have not been tested

Source: Unisys Infrastructure Risk Assessment 6/25/2004

ITM Actions: ITM approved an Internet Response Team policy on April 15, 2004. According to the Operations Assurance Branch, the procedures were not formally tested, but were proven to be effective through their implementation in response to actual incidents.

OIG Analysis: OIG reviewed ITM-2004-04 *Computer Incident Response Team Policy* dated April 15, 2004. The policy defines when a security incident begins and the steps the IRT should take to contain and investigate the incident. The incident response steps are:

1. Preserve and collect data related to the event.
2. Assign a severity level to the event.
3. Determine if data or business continuity is at risk.
4. Identify the primary incident handler.
5. Contain and eradicate the threat.
6. Perform forensic analysis and secure evidence.
7. Follow up with external organizations, if necessary.
8. Create an executive and technical incident report.

The OIG reviewed two incident response reports for events that occurred on July 22, 2004, and March 22, 2005. The reports indicated the following about FTC incident response:

- US CERT is notified when necessary.
- Security and logging tools such as Nessus, iPrism, virus, and spyware checks are run and/or reviewed to assist in forensics investigation and evidence collection.
- Procedures to identify, contain, investigate, correct, and document incidents are followed. When an incident response step is not followed or is ineffective, the issue is noted and corrective action identified.
- A "lessons learned" analysis of the incident and response are conducted after the incident is completed.

OIG Status: Closed

Weakness 20: There is no vulnerability scanning policy for the FTC network

Source: Unisys Infrastructure Risk Assessment 6/25/2004

ITM Actions: ITM approved the FTC Scanning Policy on March 17, 2004.

OIG Analysis: The OIG confirmed that the Vulnerability Scanning Policy was approved on March 17, 2004. Review of the policy revealed that it identifies scanning priorities and IT resources affected by the scans and policy. The policy also states that:

- The staff will not conduct denial of service activities.
- The CIO must explicitly authorize searches of user files, e-mails, or other areas deemed necessary to a security investigation.
- Corrective actions are identified.

OIG Status: Closed

Weakness 21: The security staff does not have multiple tools (only one on-site, but not implemented) with which to perform continuous vulnerability assessments

Source: Unisys Infrastructure Risk Assessment 6/25/2004

ITM Actions: ITM installed ISS Proventia devices on the FTC network. Additionally, FTC purchased eEye Retina to use for additional scanning.

OIG Analysis: The OIG confirmed the installation of Proventia software in a previous review. ITM provided purchase receipts for eEye Retina, but we did not verify its installation.

OIG Status: Closed

Weakness 22: A default password was found on CISCO routers for Hot Standby Routing Protocol (HSRP) service

Source: Agency Review

ITM Actions: ITM changed the default passwords on the CISCO routers.

OIG Analysis: The OIG reviewed Vantive ticket nos. 293879 and 198964. These tickets indicated that the corrective actions were complete and the tickets closed. Additionally, a screen shot of the Intrusion Detection System showed a search for HSRP_Default_Passwords. The screen capture revealed no default passwords.

OIG Status: Closed

Weakness 23: Default passwords used to view video images captured by security cameras

Source: Agency Review

ITM Actions: The passwords to the security captures were changed.

OIG Analysis: The OIG reviewed the Vantive ticket generated for correcting the password vulnerability to confirm that the default passwords were changed. Review of AXIS camera screen captures showed that there are password controls in place, and these controls appear to block incorrect passwords.

OIG Status: Closed

Weakness 24: No backup for DNS functionality

Source: Agency Review

ITM Actions: ITM set up backup servers for the primary UNIX and Windows Domain Name Servers (DNS).

OIG Analysis: Inspection of the FTC Data Center confirmed that backup Unix and Windows servers exist. A review of the configuration was also verified. There are two Unix servers: Dalmatian.FTC.gov (master server) and Akita.FTC.gov (secondary server). These servers are currently Sun Enterprise 250 platforms, but they will be replaced with two Sunfire V120 servers in the near future. If Dalmatian fails Akita will automatically take over. On the Windows DNS, both servers run in parallel and are on two separate circuits. If the main server fails the secondary server will take over. The primary Windows DNS server is called FTC-DNS and the backup is called Standby.

OIG Status: Closed

Recommendation 3: *The OIG recommends that ITM document its document- recovery procedures, record and store passwords in a secure location and maintain copies or backups of all pertinent files that may need to be restored.*