DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Improved Administration Can Enhance Federal Emergency Management Agency Laptop Computer Security (Redacted)

OIG-07-50

June 2007

Office of Inspector General
U.S. Department of
Homeland Security
Washington, DC 20528

June 5, 2007

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (*Public Law 107-296*) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared as part of our oversight responsibilities to promote economy, efficiency, and effectiveness within the department.

This report addresses the strengths and weaknesses of the Federal Emergency Management Agency (FEMA) laptop computer security controls. It is based on interviews with FEMA officials, direct observations, technical tests, and a review of applicable documents.

The recommendations herein have been developed to the best knowledge available to our office, and have been discussed in draft with those responsible for implementation. It is our hope that this report will result in more effective, efficient, and economical operations. We express our appreciation to all of those who contributed to the preparation of this report.

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Executive Summary 1

Background 3

Results of Audit 5

Standard Configuration Will Enhance Laptop Security 5
Recommendations 9
Management Comments And OIG Analysis 10

Improved Patch Management Will Increase Security 10
Recommendations 14
Management Comments And OIG Analysis 15

Enhanced Inventory Management Is Needed For Property Accountability 15
Recommendations 19
Management Comments And OIG Analysis 20

FEMA Needs To Certify And Accredit Laptop Computers To Comply With FISMA 20
Recommendations 21
Management Comments And OIG Analysis 22

Appendices

Appendix A: Purpose, Scope, and Methodology 23
Appendix B: Management Comments to the Draft Report 28
Appendix C: Major Contributors to this Report 31
Appendix D: Report Distribution 32

Abbreviations

ATL	Advanced Technology Laboratory
BIOS	Basic Input Output System
CIO	Chief Information Officer
CSIRC	Computer Security Incident Response Center
DHS	Department of Homeland Security
DISC	Disaster Information Systems Clearinghouse
FEMA	Federal Emergency Management Agency

Table of Contents/Abbreviations

FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
IP	Internet Protocol
IT	Information Technology
LIMS	Logistics Information Management System
MERS	Mobile Emergency Response Support
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
SBU	Sensitive But Unclassified
SP	Special Publication
WSUS	Windows Server Update Services

OIG

Department of Homeland Security
Office of Inspector General

Executive Summary

We audited the Department of Homeland Security and its organizational components' security program to evaluate the security and integrity of select government-issued laptop computers. This report focuses on the Federal Emergency Management Agency. Our objective was to determine whether the Federal Emergency Management Agency has established and implemented adequate and effective security policies and procedures related to the physical security of and logical access to its government-issued laptop computers.

Significant work remains for the Federal Emergency Management Agency to further strengthen the configuration, patch, and inventory management controls necessary to protect its government-issued laptop computers. Specifically, the Federal Emergency Management Agency has not established: (1) effective processes to apply the domain security policy to its laptops that meets required minimum-security settings; (2) effective procedures to patch laptop computers; and (3) adequate laptop computer inventory management procedures. As a result, sensitive information stored and processed on Federal Emergency Management Agency laptop computers may not be protected properly. Further, because the Federal Emergency Management Agency applies the same domain security policies for its desktop computers, the configuration weaknesses identified with laptop computers are relevant to all government-issued computers assigned within the Federal Emergency Management Agency. Finally, we were unable to evaluate the *Federal Information Security Management Act of 2002* requirements because the Federal Emergency Management Agency had not accounted for its laptop computers as part of a recognized information technology system.

To secure Federal Emergency Management Agency data stored on government-issued laptop computers, we are making seven recommendations to the Federal Emergency Management Agency Director. Our recommendations focus on developing a standard configuration, remedying existing vulnerabilities, patching and updating laptop computers, implementing inventory management controls, and complying with Federal Information Security Management Act requirements.

In response to our draft report, the Federal Emergency Management Agency concurred with our recommendations. The Federal Emergency Management Agency's response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

The Federal Emergency Management Agency (FEMA) leads the effort to prepare the nation for all hazards and manages federal response and recovery efforts following any national incident. FEMA employs over 2,600 full time employees and has approximately 4000 standby disaster assistance employees who are available for deployment after disasters. As part of the nation's emergency management system, FEMA partners with state and local emergency management agencies, 27 federal agencies, and the American Red Cross. To fulfill its mission, FEMA has over 32,000 laptop computers in its automated property management system.

As the weight and price of laptops have decreased and their computing power and ease of use have increased, their popularity has grown among government employees. The Department of Homeland Security (DHS) relies heavily on laptop computers for conducting business. The mobility of laptops has increased the productivity of the workforce, but at the same time increased the risk of theft, unauthorized data disclosure, and virus infection. Thefts of laptop computers occur regularly from offices, airports, automobiles, and hotel rooms, and the incidence of laptop thefts is increasing.

According to the DHS Computer Security Incident Response Center (CSIRC), 16 security incidents involving stolen or missing DHS laptop computers were reported in 2006, including government-issued laptops from U.S Customs and Border Protection, United States Secret Service, U.S. Immigration and Customs Enforcement, Transportation Security Administration, and DHS Headquarters. Further, in September 2006, the Government Accountability Office and DHS Office of Inspector General (OIG), in a joint report to Congressional Committees, reported that the Federal Emergency Management Agency (FEMA) had more than 100 missing and presumed stolen laptop computers valued at $300,000.[1]

Government organizations that provide for the use of laptop computers must take steps to ensure that the equipment and the information stored on them are properly protected. Such steps may include ensuring secure storage of laptop computers when they are not in use; encrypting data files stored on laptops; installing adequate security software applications such as firewalls and anti-virus software, disabling and controlling built-in wireless, Bluetooth, and

[1] *Control Weaknesses Leave DHS Highly Vulnerable to Fraudulent, Improper, and Abusive Activity*, September 2006, GAO-06-1117.

infrared connection capabilities; and regularly updating operating system and application software.

DHS Sensitive Systems Policy Directive 4300A and DHS National Security Systems Policy Directive 4300B provide direction to DHS components regarding the management and protection of sensitive and classified systems, respectively. In this report, we refer to DHS Sensitive Systems Policy Directive 4300A and DHS National Security Systems Policy Directive 4300B collectively as "DHS policy."

These policies outline the management, operational, and technical controls necessary for ensuring confidentiality, integrity, availability, and authenticity within the DHS Information Technology (IT) infrastructure and operations. DHS policy requires that its components ensure that strong inventory management, physical security, logical access, and wireless security controls are implemented for all systems processing sensitive or classified information. The department developed the *DHS 4300A Sensitive Systems Handbook* and the *DHS 4300B National Security Systems Handbook* to provide specific techniques and procedures for implementing the requirements of DHS policy. Further, in May 2006, DHS published a series of secure baseline configuration guides for certain operating system and software applications, such as Microsoft Windows.

The National Institute of Standards and Technology (NIST) has issued several publications related to laptop inventory management, physical security, logical access, and wireless security controls. Specifically, NIST Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Handbook*, provides guidance for establishing adequate logical and physical access controls for sensitive government systems, including the use of strong passwords, encryption, and user administration practices. Further, NIST SP 800-46, *Security for Telecommuting and Broadband Communications*, provides security guidelines for laptops used to remotely access government networks, including the use of anti-virus software, personal firewalls, encryption, and basic input output system (BIOS) passwords. BIOS is the software code run by a computer when first powered on. The primary function of BIOS is to prepare the machine so other software programs stored on various media (such as hard drives, floppies, and CDs) can load, execute, and assume control of the computer. This process is known as booting up.

Results of Audit

Standard Configuration Will Enhance Laptop Security

FEMA does not have a secure standard configuration for its laptop computers. We evaluated whether FEMA established and followed adequate procedures to ensure that laptops were configured appropriately to protect sensitive data contained in its government-issued laptops. Also, we assessed the process used by FEMA to develop and apply a domain group policy[2] that establishes the security settings that are applied to all computers connecting to its network. Finally, we tested a sample of 298 user-assigned, shared, loaner, and unassigned laptop computers to ensure that the configuration was in conformance with DHS and federal guidelines.[3] These tests included:

- Automated vulnerability assessment scans and port scanning of 298 laptops to identify configuration weaknesses;
- Detailed technical testing for a subset of 65 laptops to confirm the automated testing results and determine account, audit, access privilege, and password parameter settings;
- Password strength analysis for a subset of 65 laptops to ensure that strong passwords were used; and
- Manual reviews for a subset of 65 laptops to verify the presence and configuration of installed software.

We tested 298 laptop computers to determine whether FEMA had applied adequate logical access controls. FEMA's current process does not establish the required minimum security for laptop computers as directed by DHS. Because FEMA uses the same process to configure both its laptop and desktop computers, the configuration weaknesses are relevant to all FEMA government-issued computers. As a result of the security issues identified, sensitive data may not be properly protected.

Because of its diverse mission, FEMA has developed multiple standard images based on DHS guidelines and industry best practices, as well as requirements established in DHS policy. FEMA has developed eight standard images for

[2] Group policy is an infrastructure used to deliver and apply one or more desired configurations or policy settings to a set of targeted users and computers within an Active Directory environment.
[3] An image contains a group of programs to be duplicated verbatim onto other computers. It typically contains the operating system and a selected set of applications that are preconfigured.

Disaster Information Systems Clearinghouse (DISC) laptop computers. The DISC operates a storage and recycling center that provides centralized control and deployment of all computer and communications equipment necessary to support disaster declarations. FEMA DISC officials said approximately of 32,145 (%) laptop computers contain the DISC standard images established to support disaster operations. In addition, FEMA headquarters, Region 8, and Mobile Emergency Response Support (MERS) Denver had developed their own standard images for laptop computers that were not distributed by DISC. A FEMA MERS detachment provides mobile telecommunications, operational support, life support, and power generation assets for the on-site management of disaster and all-hazard activities. FEMA officials do not know how many standard images are employed throughout its agency.

FEMA standard images contain an operating system and general support applications. Depending on the mission requirements, additional applications may be loaded onto laptops. FEMA's standard images also incorporate anti-virus software, as well as a personal firewall for users that remotely access the FEMA network. Further, FEMA employs a domain group policy that ensures computers, connecting to its network, adhere to an established set of security controls. Local IT administrators cannot remove the security restrictions enforced by the group policy. Local IT administrators can make the group policy more restrictive. Although these measures enhance the security of FEMA's laptop computers, certain critical controls were not incorporated into laptop configuration settings or the domain group policy. Specifically, FEMA needed to:

- [4]

-

[4]

-
-
-
-
-
  -
  -

[5]

-
  -
  -
-
  -
  -

These weaknesses are the result of FEMA not developing a model system that meets minimum-security requirements for laptop computers, as directed by DHS.

DHS policy requires that components establish, implement, and enforce change management and configuration management controls on all IT systems and networks. The DHS IT Security Architecture Guidance also advises that each fully supported operating system have a standard configuration from which every instance is built. According to NIST SP 800-40, standardized configurations reduce the labor involved in identifying, testing, and applying patches; and ensure a higher level of consistency, which leads to improved

security. DHS and federal configuration guidelines also establish requirements related to security parameter settings, including account policy settings, access permissions, and renaming administrator and guest accounts.

DHS and NIST require that sensitive information stored on laptop computers, which may be used in a residence or on travel, be encrypted using NIST Federal Information Processing Standards (FIPS) Publication 140-2 approved encryption.[6] DHS and NIST recommend that the boot priority and BIOS passwords be set on sensitive systems to reduce the possibility of exploitation by an attacker with physical access to the laptop. DHS 4300A requires that functions that transmit or receive infrared signals shall be disabled in areas where sensitive information is discussed. Although personal firewalls are not required under DHS Policy Publication 4300A, security controls are necessary for laptops that remotely connect to the network.

As a result of FEMA not ensuring that all laptop computers are configured appropriately, Because FEMA uses the same process to apply group policy settings for both its laptop and desktop computers, the configuration weaknesses are relevant to all FEMA government-issued computers.

Recommendations

To secure FEMA data stored on government-issued laptop computers, we recommend that the Director of FEMA instruct the Chief Information Officer (CIO) to:

Recommendation #1: Develop and implement a secure standard configuration for all computers. Further, the CIO should establish procedures to ensure that the model system is configured to protect FEMA data and verified prior to implementation.

[6] NIST FIPS 140-2 specifies the security requirements for cryptographic modules used within a security system protecting sensitive but unclassified information. The standard provides four increasing levels of security that are intended to cover a wide range of potential applications and environments. The Cryptographic Module Validation Program substantiates cryptographic modules to FIPS 140-2 and other cryptography-based standards. Products validated as conforming to FIPS 140-2 are accepted by the federal agencies for the protection of sensitive information.

Recommendation #2: Remedy the existing critical vulnerabilities identified on laptop computers based on DHS and federal configuration guidelines. Further, the CIO should confirm whether similar vulnerabilities and remediation are applicable to all government-issued computers within FEMA.

Management Comments And OIG Analysis

FEMA concurs with recommendation 1. FEMA has taken steps to develop and implement standard hard drive images. FEMA will develop a schedule to ensure that laptop computers connected to its network comply with DHS security guidelines.

We accept FEMA's response to implement and distribute a standard image for all government issued computers.

FEMA concurs with recommendation 2. FEMA has begun taking steps to implement the recommended security settings. All laptop computers used for remote access will have a firewall enabled. FEMA is removing all Windows 2000 machines from its network and inventory.

We accept FEMA's response to implement corrective action plans for the existing vulnerabilities in its standard configuration.

Improved Patch and Update Management Will Increase Security

FEMA has procedures to patch and update its laptop computers prior to being placed into operation as part of its image install process. However, for laptop computers in use, FEMA has not established effective procedures to patch and update its laptop computers to protect against known operating system vulnerabilities and computer viruses. For those computers already in operation, FEMA distributes patches and updates through its network by patch management software. We conducted vulnerability assessment scans on a sample of 298 laptop computers to determine whether patches and updates had been applied. To determine if Microsoft, anti-virus, and third-party software patches and updates had been applied, we performed an automated scan with and conducted manual reviews.

Microsoft Patches

Microsoft issues patches to help its customers operate their systems and networks securely. Applying patches is the primary method of fixing security vulnerabilities in vendor software. Our assessment scans identified patches related to critical, important, and moderate risk vulnerabilities that had not been applied. Specifically, ,

Table 1: Number Of Missing Patches For Each Severity Rating			
Critical	Important	Moderate	Total

The oldest missing critical patch is , published in , to correct a vulnerability in . Further, of 298 (%) laptops were missing one or more of Microsoft Window's critical, important, or moderate patches.

Table 2 illustrates the number of missing critical, important, and moderate risk patches on FEMA laptop computers by site.

Table 2: Missing Patches						
Site/Type	**Number of Laptops Tested**	**Number of Laptops With Missing Patches**				
		1 - 3 Patches	4 - 10 Patches	11 - 20 Patches	21 - 30 Patches	31 or More Patches
Total						
Total	298					
Weaknesses by Region						
FEMA Headquarters Washington, DC						
Joint Field Office Albany, NY						
Joint Field Office Baton Rouge, LA						
MERS detachment Denver, CO						
Region 8 Denver, CO						

Source: OIG table based on the results of technical testing and interviews with FEMA personnel.

FEMA uses a Windows Server Update Services (WSUS) server in order to centrally control patch management service for Microsoft Windows operating systems and other software. To receive patches, a laptop computer must be connected to the FEMA domain and access the WSUS server to download the updates. Further, once patches are downloaded onto the laptop, the user must manually initiate the install process. FEMA does not have procedures to download and install patches to laptop computers that do not regularly connect to its network.

Third-Party Software Patches

Software vendors issue patches as vulnerabilities are discovered in system software to assist their customers in protecting their systems and networks. Security patches must be installed according to FEMA's configuration management plans or at the direction of the DHS CSIRC. We tested 298 laptop computers to identify third-party software and to determine whether FEMA had applied patches to mitigate known security weaknesses.

There were patches related to both critical and high-risk vulnerabilities that had not been applied. Specifically, FEMA had not patched:

-
-
-
-

DHS policy requires that IT security patches be installed according to configuration management plans or direction from DHS CSIRC. According to NIST SP 800-40, patching is critical to maintaining the operational availability, confidentiality, and integrity of information technology systems. NIST SP 800-40 recommends that organizations have a systematic, accountable, and documented process for managing exposure to vulnerabilities through the timely deployment of patches.

Because FEMA had not applied all relevant patches to its laptops,

Anti-virus Updates

FEMA maintains anti-virus update servers that check computers, and downloads and install current anti-virus definitions before access is granted to its domain. When a laptop computer is connected to the FEMA domain, it is automatically directed to FEMA's anti-virus update server to ensure compliance with current virus definitions. Laptops that are not compliant with the latest anti-virus signatures are denied access to the network. We manually reviewed 65 laptop computers and

DHS policy requires components to establish and enforce a virus protection control policy. In addition, components shall implement a defense-in-depth strategy that installs anti-virus software on its computers that is properly configured to check all files, downloads, and e-mails. Further, components shall install updates to antivirus software and signature files for each computer in a timely and expeditious manner without requiring the end user to specifically request the update.

As a result of laptop computers not regularly connecting to FEMA's domain, laptops are not updated with the latest anti-virus signatures. Further, since employees may connect to the Internet from a residence, hotel, airport, or public wireless network, viruses and other types of malicious code pose a significant threat to FEMA laptop computers, which can affect the availability, integrity, and confidentiality to the laptop and its data.

Recommendations

To secure FEMA data stored on government-issued laptop computers, we recommend that the Director of FEMA instruct the Chief Information Officer (CIO) to:

Recommendation #3: Implement procedures to ensure that all FEMA laptops are patched and updated in a timely manner, including those that do not regularly connect to the FEMA network.

Management Comments And OIG Analysis

FEMA concurs with recommendation 3. FEMA has taken steps to implement an automated patch management solution to ensure required patches are applied to FEMA's laptop computers. FEMA will require its laptop computers to connect to the FEMA network to ensure patches are downloaded.

We accept FEMA's response to implement an automated patch management solution and monitor its patching process to verify that patches are applied.

Enhanced Inventory Management Is Needed For Property Accountability

FEMA has not established effective inventory management procedures for its laptop computers. We evaluated FEMA procedures for maintaining an accurate laptop inventory, returning equipment upon employee exit or transfer, handling lost or stolen laptops, [redacted], and providing the proper labeling of laptop computers. Also, we reviewed laptop physical security measures, and assessed the FEMA laptop inventory by analyzing the integrity of inventory data on the 298 laptop computers included in our manual reviews.

FEMA has procedures for entering laptop computers into the Logistics Information Management System (LIMS), its property management system. However, FEMA has not implemented several critical inventory management controls. Specifically, FEMA has not:

- Maintained an accurate inventory;
- Ensured that lost or stolen laptops were reported to the appropriate officials;
- [redacted]; and
- Appropriately marked its Sensitive But Unclassified (SBU) laptops.

As a result of these weaknesses in inventory management and property accountability procedures, there is greater risk that FEMA officials will not have a complete and accurate inventory of its laptop computers. In addition,

sensitive information may not be restricted appropriately and unauthorized access to personally identifiable information contained in the laptops could result in an adverse effect, with widespread affect on individual privacy.

Laptop Inventory Is Not Accurate

Although FEMA has an inventory for its SBU laptop computers, it has not established effective inventory management procedures to ensure that its records are accurate. We randomly selected 242 laptop computers to determine the accuracy of FEMA's inventory. FEMA's inventory had a number of discrepancies. Specifically, 74 (31%) laptops were not updated in the LIMS. See Appendix A for additional information about our selection methodology. Upon further analysis, the 74 laptops were:

- Lost, damaged, or excess, that had not been removed from the inventory.
- Desktop computers that had been recorded as laptops.
- Inventory entry errors made by the Accountable Property Officers.
- Laptops that had been transferred to other locations.

In addition, 41 laptop computers located in Denver, Colorado were included on a local inventory but not recorded in LIMS. Local officials said 20 of these laptops were not included in LIMS because FEMA had not yet assumed ownership of the systems. The remaining laptops were not included in the inventory because the Accountable Property Officers had not updated LIMS with the current status.

FEMA does not conduct semiannual inventories as required by DHS policy. Further, FEMA's *Personal Property Management Program Manual 6150.1* is not aligned with DHS policy that requires semiannually inventories. Also, when inventories are conducted, local Accountable Property Officers do not include an examination of installed software. Accountable Property Officers we interviewed were not aware of these requirements.

DHS policy requires that components develop and maintain a property inventory of all portable electronic devices, such as laptops. This inventory is to include serial numbers or seat numbers, user names, use, and location of all portable electronic devices for accountability purposes.[7] In addition, DHS policy requires that components conduct reviews, at least semiannually, of all

[7] A seat, also referred to as a "node," is an intelligent element like a processor that can communicate using interprocessor communications. A seat is where entities and ports reside.

equipment and software to ensure that only government-licensed software and equipment are being used, and that appropriate exceptions have been documented. As a result of an incomplete and inaccurate inventory, there is a greater risk that FEMA officials will not be able to account for their laptop computers or be prepared to manage effectively federal response and recovery efforts following a major incident.

Lost or Stolen Laptops Are Not Reported Appropriately

FEMA has not ensured that lost or stolen laptops are reported to the DHS CSIRC. As illustrated in Table 3, we identified 26 of 242 (11%) laptop computers judgmentally selected from the LIMS inventory that FEMA officials could not locate. FEMA was unaware that these laptops were missing.

Table 3: Unaccountable Laptop Computers

Site	Number of Laptops Randomly Selected for Testing	Number of Laptops FEMA Could Not Account For
FEMA Headquarters Washington, DC	60	
Joint Field Office Albany, NY	60	
Joint Field Office Baton Rouge, LA	60	
MERS Detachment Denver, CO	28	
Region 8 Denver, CO	34	
Total	242	

Further, FEMA's Security Branch issued a memorandum in September 2006 reporting that 58 laptop computers were lost, missing, or stolen since January 2005. The laptop security incidents were investigated and reported to FEMA Headquarters, but were not reported to DHS CSIRC. According to FEMA officials, the 58 missing computers were not reported because the DHS CSIRC is a relatively new entity. FEMA officials said that since our review, they have begun reporting security incidents to DHS CSIRC.

DHS policy requires that components report significant computer security incidents to the DHS CSIRC immediately upon identification and validation of incident occurrence. The DHS CSIRC is normally responsible for notifying

appropriate law enforcement authorities of a security event, who pursue the investigation and recommend disciplinary action, if required. Because FEMA had not reported these security incidents to the DHS CSIRC, senior DHS officials may not be aware of the extent or scope of laptop security issues at the department, and the appropriate corrective actions may not have been taken. Further, without an accurate inventory, FEMA may not be aware of additional missing laptop computers.

Laptops Are

FEMA has implemented procedures for .[8] Specifically:

-
-

In July 2006, FEMA issued a standard operating procedure and technical guidance to ensure compliance with federal laws and regulations. However, FEMA IT staff we interviewed do not adhere to DHS policy or FEMA guidelines.

DHS policy requires that components ensure that DHS policy also requires that components ensure that , As a result of these weaknesses in

[8]

FEMA's [redacted], there is greater risk that access to sensitive information may not be limited properly.

Laptops Are Not Marked Appropriately

FEMA has not ensured that its laptops are appropriately labeled. Specifically, none of the SBU laptops tested were: (1) marked with the highest classification level of the information that has been processed or stored on the device, or (2) labeled indicating that the units were not authorized for classified processing.

FEMA's *Personal Property Management Program Manual 6150.1* does not address marking computers with the highest classification level or affixing labels on units authorized for classified processing. Local IT staff and Accountable Property Officers we interviewed were unaware of this requirement. Headquarters officials said that FEMA had not had the opportunity to label its laptop computers and is currently considering what other DHS components are using to mark and label their systems.

DHS policy requires that all equipment be marked with the highest classification level of the information that has been processed or stored on the device. Because these laptops were not appropriately marked, there is greater risk that classified information may have been processed on an unclassified system. DHS policy also recommends that a label be affixed to PCs, terminals, and laptops not authorized to process classified information, especially in environments where both sensitive information and classified information are processed.

Recommendations

To secure FEMA data stored on government-issued laptop computers, we recommend that the Director of FEMA instruct the Chief Information Officer (CIO) to:

Recommendation #4: Implement appropriate inventory management controls to ensure that an accurate laptop inventory is maintained, including effective inventory reviews.

Recommendation #5: Report computer security incidents to DHS CSIRC in a timely manner to ensure that they are investigated and that appropriate corrective action is taken.

Recommendation #6:

Management Comments And OIG Analysis

FEMA concurs with recommendation 4. FEMA is revising its procedures for accountability and control of its computing resources. An inventory and reconciliation of IT property will be completed by September 30, 2007.

We accept FEMA's response to complete a comprehensive IT inventory. To ensure that an accurate laptop inventory is sustained, we maintain that FEMA should conduct annual inventory reviews.

FEMA concurs with recommendation 5. FEMA Instruction 1540.1 has been updated to include requirements for the Chief Security Officer and the Chief of Information Technology Security to be notified of computer security incidents. Computer security incidents will be reported to DHS CSIRC.

We accept FEMA's response to report all computer security incidents to DHS CSIRC to ensure that the incidents are investigated and appropriate corrective action is taken.

FEMA concurs with recommendation 6. . FEMA will implement policy changes that will ensure that all classified and unclassified laptop computers are appropriately marked.

We accept FEMA's response to

FEMA Needs To Certify And Accredit Laptop Computers To Comply With FISMA

The Federal Information Security Management Act of 2002 (FISMA), Title III of the E-Government Act (Public Law 107-347, December 17, 2002), provides

a comprehensive framework to ensure the effectiveness of security controls over information resources that support federal operations and assets. The agency's security program shall provide security for the information as well as the systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

We were unable to evaluate the effectiveness of FEMA's information security program and practices as implemented for SBU laptop computers. FEMA has 32,145 laptop computers processing sensitive information that may contain personally identifiable information. FEMA officials do not consider laptops a major application or general support system and, therefore, had not certified and accredited its laptop computers. Since our review, FEMA plans to review certification and accreditation requirements for portable computers, evaluate options, and determine the most efficient and cost-effective approach to certify and accredit FEMA laptop computers.

FISMA requires each agency to develop, document, and implement an agency-wide information security program to provide security for its information and systems. Policies should ensure that information security is addressed throughout the life cycle of each agency information system and determine minimally acceptable system configuration requirements. In addition, DHS policy requires that every DHS computing resource (e.g., desktops, laptops, servers, portable electronic devices) shall be individually accounted for as part of a recognized IT system. Further, every computing resource shall be designated as a part of an IT system.

Because FEMA has not certified and accredited its laptop computers, this presents a significant deficiency for the DHS information system security program. We believe that information systems operating without certification and accreditation could increase the risk and potential magnitude of harm. Therefore, FEMA should consider identifying this deficiency as a material weakness pursuant to Office of Management and Budget Circular No. A-123, "Management Accountability and Control," and the Federal Manager's Financial Integrity Act.

Recommendations

To secure FEMA data stored on government-issued laptop computers, we recommend that the Director of FEMA instruct the Chief Information Officer (CIO) to:

Recommendation #7: Adhere to DHS policy that requires every computing resource to be individually accounted for as part of a recognized IT system. Further, the CIO should ensure laptop computers are compliant with FISMA.

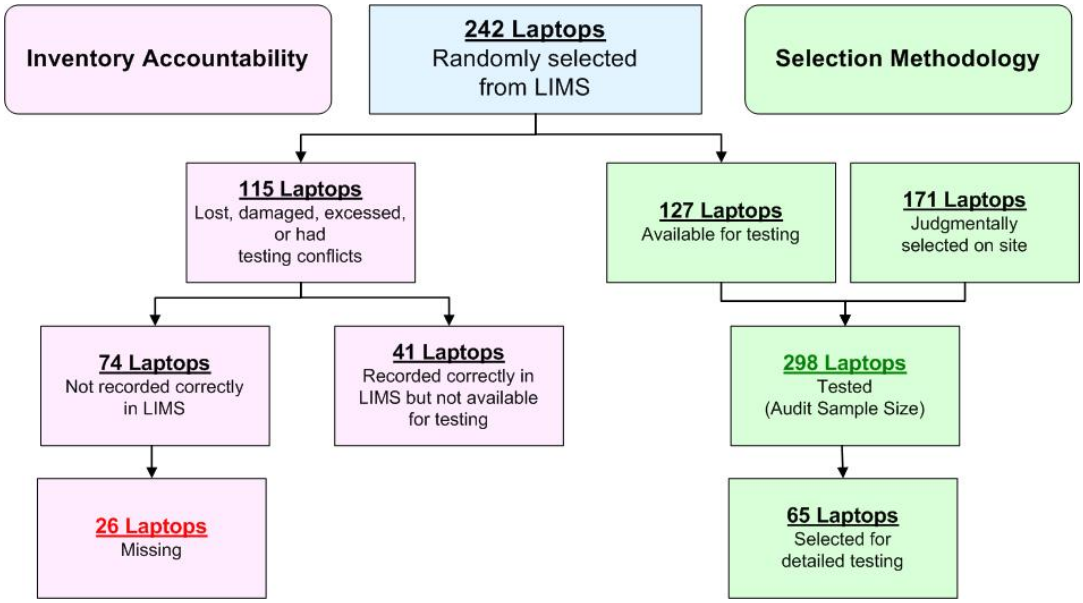
Management Comments And OIG Analysis

FEMA concurs with recommendation 7. FEMA is revising its procedures regarding accountability and control of its computing resources. FEMA's process to certify and accredit its laptops and ensure its computers are FISMA compliant is almost complete.

We accept FEMA's response to ensure its laptop computers comply with FISMA security requirements.

The objective of this audit was to determine whether FEMA had implemented adequate and effective security policies and procedures related to the physical security of and logical access to its government-issued laptop computers. Specifically, we determined whether FEMA had implemented adequate (1) policies and procedures for inventory management; (2) physical security measures; (3) logical access controls; and, (4) wireless security measures for sensitive data contained in its government-issued laptops. Our focus was to test the development and implementation of a model system for laptop computers processing and storing sensitive or classified DHS data, as well as the procedures used to patch and update laptops once placed into operation. In addition, we attempted to obtain FISMA information required for our annual independent evaluation. However, FEMA had not assigned its laptop computers to a recognized IT System.

FEMA's laptop computers are accounted for in LIMS, an automated property management system. On September 7, 2006, LIMS contained 32,145 laptop computers. We selected 242 laptop computers to conduct automated and manual testing. We had to exclude 115 laptop computers from our original sample size because laptops were either missing, excessed, not available, or had hardware/software conflicts. We judgmentally selected an additional 171 laptops on site to give us a sample size of 298 laptop computers.



To identify laptop computers, we analyzed the FEMA laptop computer inventory and selected the following FEMA sites for testing.

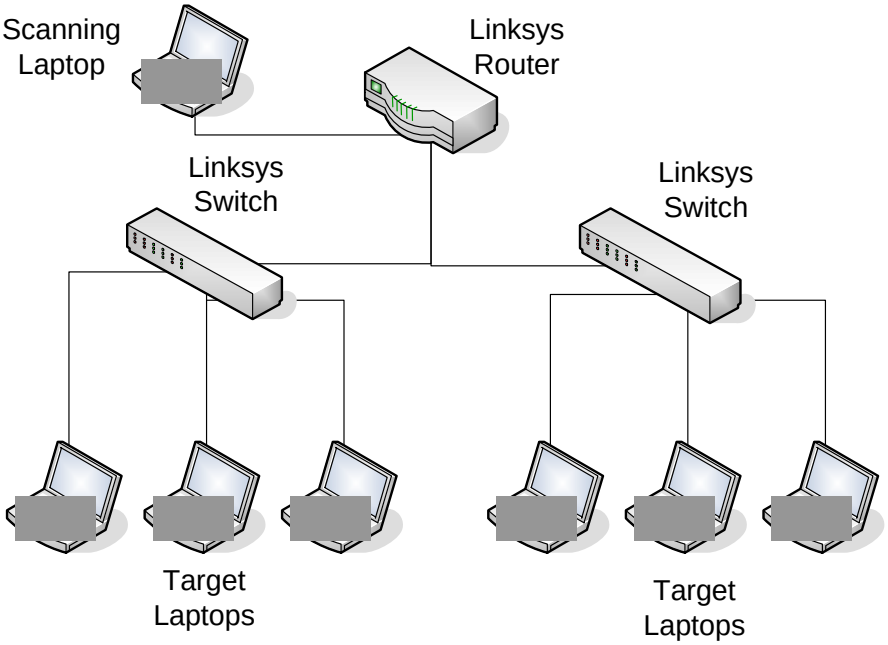
FEMA Testing Locations and Laptop Computers

Region	298 SBU Laptops				
	User-Assigned	Shared	Loaner	Unassigned	Total
Washington, DC	15 Laptops	31 Laptops	2 Laptops	12 Laptops	60 Laptops
Albany, NY	59 Laptops	-	-	-	59 Laptops
Baton Rouge, LA	85 Laptops	-	-	7 Laptops	92 Laptops
Denver, CO	73 Laptops	13 Laptops	-	1 Laptops	87 Laptops
Total	232 Laptops	44 Laptops	2 Laptops	20 Laptops	298 Laptops

We performed automated vulnerability assessment scans and port scanning of 298 laptops to determine configuration weaknesses and missing patches. In addition, we conducted detailed testing for a subset of 65 laptop computers. These test included:

- Detailed technical testing to confirm the automated testing results and determine account, audit, access privilege, and password parameter settings.
- Password strength analysis to ensure that strong passwords were used.
- Manual reviews to verify the presence and configuration of installed software.

We created a closed testing network to assess FEMA's laptop computers with an OIG scanning laptop. This closed network did not connect to the FEMA domain or the Internet. The following diagram illustrates the configuration of the OIG testing network.



Architecture of Testing Network

Upon completion of the tests, we provided component officials with technical reports detailing the specific vulnerabilities detected on their system and the actions needed for remediation.

We used eight testing tools to conduct internal security tests to evaluate the effectiveness of controls implemented for the systems:

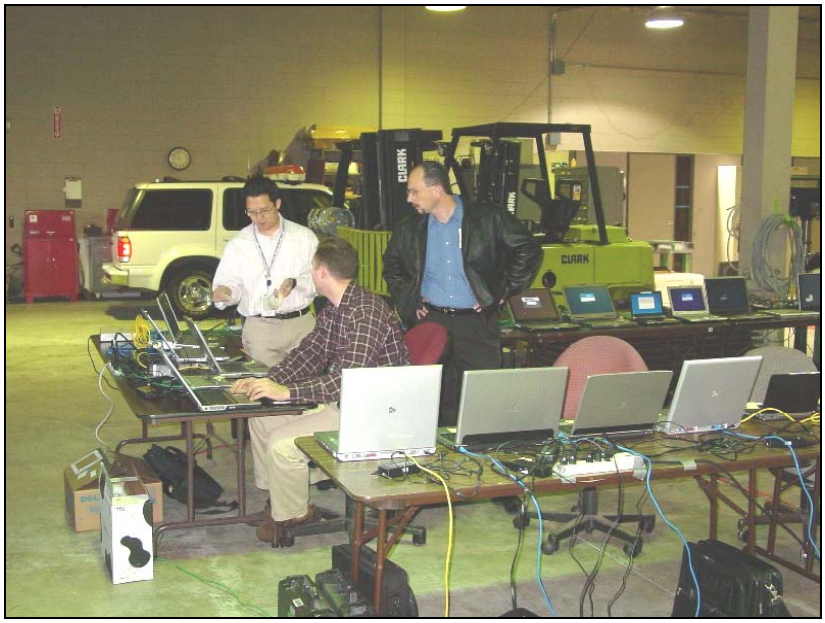
-
-
-

[9] NIST SP 800-42, *Guideline on Network Security Testing*, identifies Internet Scanner as a common testing tool.

-
-
-
-
-

We conducted fieldwork at FEMA facilities in Washington, DC; Bluemont, Virginia; Albany, New York; Baton Rogue, Louisiana; Denver, Colorado; and, the OIG Advanced Technology Laboratory (ATL). The ATL supports our capability to perform effective and efficient technical assessments of DHS information systems in diverse operating environments. The ATL is a collection of hardware and software that allows the simulation, testing, and evaluation of the computing environments that are most commonly used within DHS. We conducted our audit from September to November 2006 under the authority of the Inspector General Act of 1978, as amended, and according to generally accepted government auditing standards. Major OIG contributors to the audit are identified in Appendix C.

Our principal points of contact for the audit are Frank Deffer, Assistant Inspector General for Information Technology Audits, at (202) 254-4100, and Edward G. Coleman, Director, Information Security Audit Division, at (202) 254-5444.



Source: OIG auditors conducting security scans on laptop computers in Denver, Colorado.

Source: OIG auditors conducting security scans on laptop computers in Denver, Colorado.

Appendix B
Management Comments to the Draft Report

U.S. Department of Homeland Security
Washington, D.C. 20472

MAY 17 2007

FEMA

MEMORANDUM FOR: Richard L. Skinner
Inspector General
Department of Homeland Security

FROM: Anthony T. Cira
Chief Information Officer/Director
Information Technology Services Division

SUBJECT: Draft Audit Report – *Improved Administration Can Enhance Federal Emergency Management Agency Laptop Computer Security*, OIG-07-XXX, February 2007 – Comments on Report and Actions on Recommendations

We appreciate the opportunity to review and comment on your draft audit report, *Improved Administration Can Enhance Federal Emergency Management Agency Laptop Computer Security*. We concur with the recommendations made and are developing Plans of Actions and Milestones (POA&M) to implement the seven recommendations contained in the report.

Recommendation #1. *Develop and implement a secure standard configuration for all computers. Further, the CIO should establish procedures to ensure that the model system is configured to protect FEMA data and verified prior to implementation.*

Work is underway to develop and implement standardized hard drive images, along with procedures that adhere to the "DHS Windows Secure Baseline Configuration Guide." FEMA is developing deployment schedules to implement the standardized hard drive images and ensure that laptops connected to the network are in compliance with DHS security guidelines.

Recommendation #2. *Remedy the existing critical vulnerabilities identified on laptop computers based on DHS and federal configuration guidelines. Further, the CIO should confirm whether similar vulnerabilities and remediation are applicable to all government-issued computers within FEMA.*

FEMA has already taken steps to implement the recommended security settings that change the standard personal computer configuration image. All laptops used for remote access have a Firewall enabled. FEMA IT Security and IT Operations Branch are formulating a methodology for implementing compensating controls for all remaining laptops. DHS recently revised its software configuration guide and now does not require BIOS passwords on Windows XP machines. FEMA is removing all Windows 2000 machines from the network and inventory.

Recommendation #3. *Implement procedures to ensure that all FEMA laptops are patched and updated in a timely manner, including those that do not regularly connect to the FEMA network.*

FEMA is implementing an automated patch management solution to ensure required patches are applied to FEMA's laptops. Policies are being issued to require the connection of laptops to the network for minimum periods to ensure the downloading of patches, and compliance with this policy will be monitored to verify that patches are applied.

Recommendation #4. *Implement appropriate inventory management controls to ensure that an accurate laptop inventory is maintained, including effective inventory reviews.*

FEMA is revising its procedures regarding accountability and control of its computing resources, which will include reviews and incident reporting procedures. An inventory of IT property is being conducted and all reconciliation and updates of property accountability records are to be completed by September 30, 2007.

Recommendation #5. *Report computer security incidents to DHS CSIRC in a timely manner to ensure that they are investigated and that appropriate corrective action is taken.*

FEMA Instruction 1540.1, Management of Information Technology Security Incidents, is updated to include requirements for the Chief Security Officer and the Chief of Information Technology Security to be notified of computer security incidents. The Security Branch has incorporated FEMA Instruction 1540.1 into their procedures for the reporting of computer security incidents to the DHS Computer Security Incident Response Center (CSIRC).

Recommendation #6. *and ensure that SBU laptops are marked appropriately, in accordance with DHS and federal guidelines.*

The Security Branch is implementing policy changes that will ensure that all classified and unclassified laptops are appropriately marked. The Security Audit Program, that is the responsibility of the Security Branch, is being enhanced to ensure that all Special Security Representatives are trained and informed of the marking requirements. FEMA is planning to complete the labeling of its laptops by the end of September 2007.

Recommendation #7. *Adhere to DHS policy that requires every computing resource to be individually accounted for as part of a recognized IT system. Further, the CIO should ensure laptop computers are compliance with FISMA.*

FEMA is revising its procedures regarding accountability and control of its computing resources. These new procedures will be documented and implemented by August 2007 to ensure accountability records are complete, accurate, and properly maintained. The process FEMA will follow to certify

and accredit FEMA's laptops is almost complete to ensure our laptop computers are FISMA compliant.

Over the next 30 days we will develop a POA&M for each of the recommendations and begin reporting their status to the OIG every 90 days after issuance of the final Audit Report. The senior leadership of FEMA will monitor progress of the POA&M to ensure the successful implementation of audit recommendations.

Finally, we authorize the public release of this draft audit report in its entirety.

Appendix C
Major Contributors to this Report

Information Security Audits Division
Edward G. Coleman, Director
Patrick Nadon, Audit Manager
Eugene Yu, Audit Team Leader
Swati Mahajan, Referencer

Advanced Technology Division
Marcus Badley, Senior Security Engineer
David Hawkins, Senior Security Engineer
Jordan Fox, Security Engineer, Space and Naval Warfare Systems Command

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretary
Director, GAO/OIG Liaison Office
Assistant Secretary for Policy
Assistant Secretary for Public Affairs
Assistant Secretary for Legislative and Intergovernmental Affairs
Chief Information Officer
Deputy Chief Information Officer
Chief Information Security Officer
Director, Compliance and Oversight Program
Chief Information Officer Audit Liaison
Chief Information Officer, FEMA
Audit Liaison, FEMA
Director, Information Security Audit Division
Chief Privacy Officer

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Congressional Oversight and Appropriations Committees, as appropriate

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4199, fax your request to (202) 254-4305, or visit the OIG web site at www.dhs.gov/oig.

OIG Hotline

To report alleged fraud, waste, abuse or mismanagement, or any other kind of criminal or noncriminal misconduct relative to department programs or operations:

- **Call our Hotline at 1-800-323-8603;**
- **Fax the complaint directly to us at (202) 254-4292;**
- **Email us at DHSOIGHOTLINE@dhs.gov; or**
- **Write to us at:**
  DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations - Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528.

The OIG seeks to protect the identity of each writer and caller.