

Department of Homeland Security **Office of Inspector General**

Progress Has Been Made in
Securing Laptops and Wireless
Networks at FEMA





Homeland
Security

June 27, 2012

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's efforts to safeguard laptop computers and implement controls to protect the sensitive data processed by its wireless networks and devices from potential exploits. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, 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. We trust 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.

A handwritten signature in black ink, appearing to read "Frank Deffer".

Frank W. Deffer
Assistant Inspector General
Information Technology Audits

Table of Contents/Abbreviations

Executive Summary	1
Background.....	2
Results of Audit	5
Actions Taken To Enhance Laptop and Wireless Security	5
Laptop Inventory Management Controls Need Strengthening	7
Recommendations.....	9
Management Comments and OIG Analysis	9
Improvements Needed on Laptop Security Management.....	9
Recommendations.....	16
Management Comments and OIG Analysis	16
Performing Assessments Can Enhance Wireless Security	17
Recommendation	19
Management Comments and OIG Analysis	19

Appendices

Appendix A: Purpose, Scope, and Methodology.....	20
Appendix B: Management Comments to the Draft Report	22
Appendix C: Major Contributors to this Report.....	25
Appendix D: Report Distribution	26

Abbreviations

DHS	Department of Homeland Security
DISC	Disaster Information Systems Clearinghouse
EOC	Enterprise Operations Center
FEMA	Federal Emergency Management Agency
FMD	Facilities Management Division
IT	information technology
JFO	Joint Field Office
LIMS	Logistics Information Management System
MERS	Mobile Emergency Response Support
NACS	National Emergency Management Information System Access Control System
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
USGCB	United States Government Configuration Baseline

OIG

*Department of Homeland Security
Office of Inspector General*

Executive Summary

We audited the Federal Emergency Management Agency's (FEMA) efforts to protect its laptop computers and controls implemented to protect sensitive data processed by its wireless networks and devices from potential exploits. Specifically, we evaluated FEMA's inventory process for safeguarding its laptops, reviewed its configuration management program, and conducted security assessments on its wireless networks. Additionally, we followed up on FEMA's actions to address the recommendations cited in two prior audit reports.

FEMA has taken actions to improve the inventory and configuration management controls to protect its laptop computers and the sensitive information they store and process. Furthermore, FEMA has implemented technical controls to protect the information stored on and processed by its wireless networks and devices.

However, we found weaknesses in the component-wide adoption of FEMA's automated property management system, reporting of lost and stolen laptops, implementation of hard drive encryption, use of a standardized laptop image, timely installation of security patches, documentation of laptop sanitization, and accounting for wireless networks. These weaknesses put laptops and the sensitive information stored and processed on them at risk of exploitation. Improvements are needed to address security risks and ensure the security of laptops and wireless networks and devices.

We are making two recommendations to the Chief Administrative Officer and five recommendations to the Chief Information Officer. FEMA concurred with all of our recommendations and have begun to take actions to implement them. FEMA's responses are summarized and evaluated in the body of this report and included, in their entirety, as appendix B.

Background

FEMA coordinates the Federal Government's role in preparing for, preventing, mitigating the effects of, responding to, and recovering from all natural or manmade domestic disasters, including acts of terror. As of October 2011, FEMA had more than 7,400 employees, who include a mix of full-time and part-time employees on standby for deployment after disasters. Employees are stationed at FEMA headquarters in Washington, DC; at regional and area offices across the country; and at the National Emergency Training Center in Emmitsburg, MD.

To accomplish its mission, FEMA relies heavily on the use of laptop computers, which have grown in popularity across the Federal Government. As of October 2011, FEMA reported an inventory of more than 40,000 laptops across the enterprise. Although the mobility of laptops has increased the productivity of the Federal workforce, it has also increased the risk of theft and unauthorized disclosure of sensitive data.

The use of wireless networks and devices (e.g., Institute of Electrical and Electronics Engineers 802.11x) is increasing throughout the Federal Government.¹ Wireless technologies are used to support FEMA's mission in a variety of ways at Joint Field Offices (JFOs), regional offices, and distribution centers.² Wireless networks extend the range of wired networks by using radio waves to transmit data to wireless-enabled devices, such as mobile devices and laptops. Wireless technologies offer many potential benefits in improving employee productivity and flexibility. In addition, deploying wireless networks can provide tremendous cost savings compared with wired infrastructures. However, wireless networks and devices can also introduce significant security issues when they are not properly configured, such as eavesdropping, the need for physical protection of wireless devices, and unauthorized deployment of wireless access points.

In June 2007, we reported deficiencies in configuration, patch, and inventory management controls over FEMA's government-issued laptops.³ We found that sensitive information stored and processed on FEMA laptops might not have been protected

¹ The 802.11x (e.g., 802.11a, b, g, and n) standards developed by the Institute of Electrical and Electronics Engineers are frequently used for transmission specifications on wireless devices.

² A JFO is a temporary Federal multiagency coordination center established locally to facilitate field-level domestic incident management activities related to prevention, preparedness, response, and recovery.

³ *Improved Administration Can Enhance Federal Emergency Management Agency Laptop Computer Security* (OIG-07-50), June 2007.

properly. Specifically, we found that FEMA had not established (1) effective processes to apply the domain security policy to its laptops that met required minimum security settings, (2) effective procedures to patch laptops, and (3) adequate laptop inventory management procedures. We also determined that FEMA had an incomplete and inaccurate laptop inventory. We were unable to locate 26 of 242 (11percent) of a random selection of laptops.

The Operations Support Branch of the Office of the Chief Information Officer (OCIO) is responsible for providing information technology (IT) capabilities to FEMA and State and local governments in support of the component's all-hazards mission. The Operations Support Branch manages, operates, and maintains FEMA's IT systems, networks, and services centers. The Field Support Team within the Operations Support Branch maintains a distribution warehouse, known as the Disaster Information Systems Clearinghouse (DISC).

The DISC centralizes wireless network deployment in support of local, regional, and field offices across the country. In addition, the DISC serves as a centralized facility where selected laptops and communications equipment are housed in preparation for a disaster, shipped to JFOs once they are activated, and eventually returned upon closure of the disaster. DISC laptops are stored in ready-to-ship sets of 50 units each known as "kits," as shown in figure 1.



Figure 1: Kits upon arrival at the Albany Joint Field Office

In December 2010, the OCIO established the Enterprise Wireless Local Area Network General Support System to provide wireless local area network connectivity across FEMA and network infrastructure resources to its end users. In addition, wireless networks are deployed at 9 of 10 Regional Offices to grant public

Internet access only (i.e., the FEMA Enterprise Network⁴ is inaccessible) to Federal, State, local, tribal, and private sector partners during Regional Response Coordination Center activations.⁵ JFOs, in comparison, are initially activated with a wireless network that grants users access to the FEMA Enterprise Network.

FEMA centrally manages the authorization, deployment, security, and monitoring of wireless networks. The FEMA OCIO Authorizing Official tracks and authorizes wireless networks. Members of Disaster Response Teams at the DISC are responsible for deploying and securing wireless networks at JFOs. The JFO wireless networks follow a standardized deployment and security architecture, as shown in figure 2.

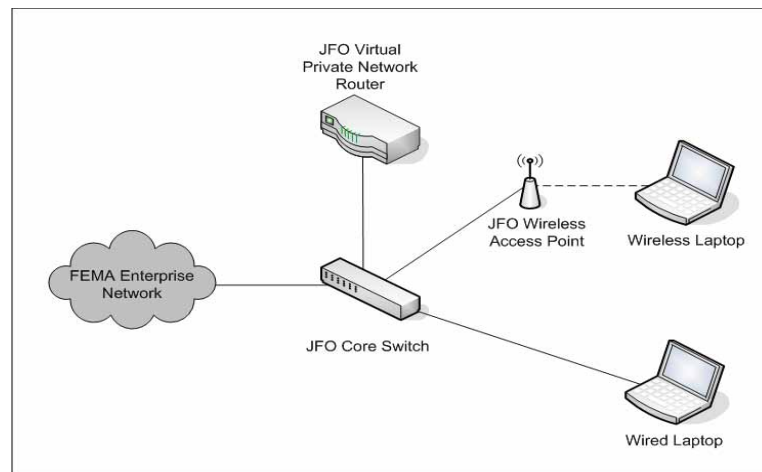


Figure 2: Architecture for wireless local area network installation

After deployment and throughout the rest of the life cycle, the FEMA Network Operations Center monitors wireless networks. The wireless networks at JFOs are either taken down when the site is deactivated or are replaced with a wired network when the site becomes a permanent office.

⁴ All facets of FEMA’s community use the FEMA Enterprise Network to transmit data between users, systems, and applications; to connect to external agencies with which FEMA conducts business; and to provide server infrastructure for applications and systems that support FEMA’s mission.

⁵ Regional offices activate their Regional Response Coordination Centers to serve as the main coordination point between Federal agencies to support State and local governments with disaster response and recovery.

Results of Audit

Actions Taken To Enhance Laptop and Wireless Security

FEMA has made progress in implementing management controls to safeguard laptops through improved inventory maintenance. For example, we selected 178 laptops at five sites to determine whether FEMA had accurately recorded the laptop locations in its property management system. We were able to locate all 178 laptops. This is an improvement over the results from our prior audit. Table 1 summarizes the results of our 2011 inventory evaluation.

Location	Laptops Selected	Laptops Located	Percent Located
DISC Winchester, VA	101	101	100%
Region 10 Headquarters Bothell, WA	8	8	100%
Mobile Emergency Response Support Detachment Bothell, WA	19	19	100%
Joint Field Office Albany, NY	29	29	100%
Joint Field Office New Orleans, LA	21	21	100%
Total	178	178	100%

Table 1: Results of 2011 OIG Inventory Evaluation

FEMA has also implemented the following inventory controls:

- Issued the FEMA Personal Property Manual to establish a comprehensive framework to help manage and account for government property procured by FEMA;
- Captured more than 40,000 laptops in its automated property management system, the Logistics Information Management System (LIMS); and
- Conducted comprehensive annual reviews of accountable property, including laptops, as specified in the FEMA Personal Property Manual.

In addition, FEMA has implemented the following technical controls to safeguard the information stored on and processed by its laptops and wireless networks:

- FEMA centrally manages the configuration and patch management process on laptops using a combination of controls, including a FEMA-developed password management solution and third-party vulnerability management software. In addition, FEMA has deployed standardized images on its laptops. A standardized image can help to establish a consistent baseline implementation of configuration controls across the enterprise.
- The Chief Information Officer approved a standardized Windows 7 image on March 30, 2011. FEMA began to deploy the new image in November 2011. As of January 2012, 300 laptops with the Windows 7 image had been shipped from the DISC to two sites.
- The OCIO has developed standard operating procedures for sanitizing its laptops to ensure that sensitive information is not recoverable when laptops are transferred, become obsolete, or are no longer usable.
- Wireless signals are not broadcasting beyond the perimeter of buildings at the sites visited, as FEMA has deployed wireless access points strategically to minimize signal leakage and potential unauthorized access. Further, we identified no rogue or unauthorized wireless networks or devices with access to the FEMA Enterprise Network.⁶ Wireless access points are configured not to broadcast extended service set identifiers to avoid advertising wireless networks' identities and functions to potential attackers.⁷
- Virtual private network software is required to be installed on laptops before users can connect to wireless networks. Secure connections are established through an encrypted virtual private network tunnel using either one-factor or two-factor authentication.
- FEMA employs wireless intrusion protection systems to monitor and detect malicious behavior on its Enterprise Wireless Local Area Network.

⁶ We used AirMagnet software to scan for unauthorized wireless networks and to detect signal leakage at four sites: the DISC, Region 10 headquarters, Albany JFO, and New Orleans JFO.

⁷ An extended service set identifier is used to identify a wireless network to client devices, as specified in the Institute of Electrical and Electronics Engineers standards for 802.11x wireless networks.

Although FEMA has taken actions to strengthen its inventory and configuration management controls, improvements are needed to ensure the security of its laptop computers and wireless networks and devices. Specifically, FEMA must address remaining weaknesses in the component-wide adoption of LIMS, reporting of lost and stolen laptops, implementation of hard drive encryption, use of a standardized operating system image, timely installation of security patches, documentation of laptop sanitization, and accounting for wireless networks.

Laptop Inventory Management Controls Need Strengthening

Although FEMA has made progress in strengthening the inventory management process for its laptop computers, it can make further improvements by implementing additional inventory management controls. Specifically, FEMA needs to account for all laptops in LIMS and ensure that lost or stolen laptops are reported to the Department as security incidents. These weaknesses hinder FEMA's ability to quickly distribute laptops in response to an emergency declaration and may prevent management from taking appropriate corrective actions in response to the loss or theft of laptop computers.

FEMA Is Not Accounting for All Laptops in LIMS

Some FEMA offices are not properly accounting for laptop computers in LIMS. While evaluating incidents of lost and stolen laptops, we found that 13 government-purchased laptops were reported missing to the Department of Homeland Security's Enterprise Operations Center (DHS EOC) in 2011. However, 3 of these 13 laptops had never been accounted for in LIMS. The discrepancy exists because the Facilities Management Division (FMD) does not have the component-wide management support needed to ensure that LIMS is used to account for all government property. An FMD official told us that some FEMA offices choose to procure laptops and not record their purchase in LIMS.

The FEMA Personal Property Manual requires the use of LIMS to account for all government accountable property. Further, DHS requires components to establish and maintain an accurate information systems inventory. When laptops are not properly accounted for, FEMA officials do not have a complete and accurate inventory of their disaster response equipment. This hinders FEMA's ability to facilitate the distribution of laptops needed to manage response and recovery efforts following a disaster. It also creates an opportunity for theft and fraud, as offices have property that is not subject to inventory reviews.

Lost or Stolen Laptops Are Not Reported Consistently

Lost or stolen laptops are not being reported consistently to the DHS EOC as security incidents. FEMA requires a Report of Survey to be completed whenever a laptop is lost, stolen, damaged, or destroyed. In 2011, 60 Reports of Survey were completed for 242 laptops. However, FEMA could not determine how many of these 242 laptops were lost or stolen. FMD estimated that 95 percent were lost or stolen and 5 percent were damaged or destroyed. By this estimate, approximately 230 laptops should have been reported as lost or stolen to the DHS EOC as security incidents. However, FEMA reported only 13 lost or stolen laptops to the DHS EOC in 2011. This is an indicator that FEMA cannot account for all of its laptops and does not comply with DHS security incident reporting requirements. As a result, FEMA and DHS may have underreported FEMA's security incidents in the Department's fiscal year 2011 *Federal Information Security Management Act* submission.

FMD was able only to estimate how many laptops were lost or stolen versus damaged or destroyed because LIMS users do not properly populate fields in LIMS to record this information. FMD must then rely on hard copies of Reports of Survey to obtain more detail about a specific incident. In 2007, we reported that FEMA identified 58 lost or stolen laptops between January 2005 and September 2006.⁸ We noted that these incidents were reported to FEMA headquarters but not to the DHS Computer Security Incident Response Center, which is now part of the DHS EOC.

DHS requires components to report significant incidents to the DHS EOC no later than 1 hour after the security event is confirmed as an incident. Minor incidents must be reported to the DHS EOC in a weekly incident report. However, the Report of Survey procedures as outlined in the FEMA Personal Property Manual, as well as the instructions on the Report of Survey itself, do not address the requirement to report the loss of sensitive personal property, such as laptops, to the DHS EOC.

Not reporting the loss or theft of laptops to the DHS EOC prevents FEMA from taking appropriate corrective actions in response to the loss or theft of a laptop. Also, it limits senior officials' knowledge of the extent of laptop security issues.

⁸ *Improved Administration Can Enhance Federal Emergency Management Agency Laptop Computer Security* (OIG-07-50), June 2007.

Recommendations

We recommend that the Chief Administrative Officer:

Recommendation #1: Implement appropriate management controls to ensure that all government-purchased laptops are accounted for in LIMS in accordance with applicable policy.

Recommendation #2: Work with the Chief Information Officer to establish a process to ensure that the loss or theft of laptops are reported timely as security incidents to the DHS EOC.

Management Comments and OIG Analysis

FEMA concurred with recommendation 1. The Chief Administrative Officer will put measures into place to ensure that unaccounted-for laptops discovered in LIMS are escalated as an issue and addressed in compliance with policy. Further, compliance will be evaluated in July 2012 once an annual inventory review is completed.

We agree that the steps FEMA plans to take begin to satisfy this recommendation. This recommendation will remain open until FEMA provides documentation to support that all planned corrective actions are completed.

FEMA concurred with recommendation 2. The Chief Administrative Officer will put measures in place to ensure that accountable property reported as missing during inventories is reconciled with the incident reports received by the FEMA Security Operations Center. Instances of missing laptops will be escalated and appropriately addressed. Compliance with policy will be evaluated when the annual inventory review is performed in July 2012.

We agree that the steps FEMA plans to take begin to satisfy this recommendation. This recommendation will remain open until FEMA provides documentation to support that missing laptops are reported timely as security incidents to the DHS EOC.

Improvements Needed on Laptop Security Management

FEMA has not implemented all required controls on its Windows XP laptops to prevent unauthorized access. Nor has FEMA encrypted the hard drives to protect sensitive data stored on its laptops. Finally, some of

the sites we visited are not following documented sanitization procedures to reimage, reissue, or transfer laptops.

To evaluate FEMA's patch management process, we performed vulnerability scans on 116 laptops at four regional offices and one JFO to determine if security patches were deployed timely to mitigate software vulnerabilities. In addition, we evaluated the compliance with applicable United States Government Configuration Baseline (USGCB) and DHS required settings on 73 laptops.

FEMA Has Not Encrypted All of Its Laptops

FEMA has not encrypted all of its laptop hard drives to protect its sensitive information from unauthorized access. FEMA encrypts the entire laptop hard drive according to DHS requirements to prevent operating system controls from being circumvented and to restrict access to the information stored on the hard drive. However, as of January 2012, only 7,956 (20 percent) of its 40,130 laptop hard drives are encrypted. FEMA expects all laptop hard drives to be encrypted by April 2012. DHS requires that laptops be encrypted according to National Security Agency requirements. Additionally, electronic data must be encrypted using at least 256-bit Advanced Encryption Standard according to Federal Information Processing Standards.⁹

In 2011, 60 Reports of Survey were completed for 242 laptops that were lost, stolen, damaged, or destroyed. If the hard drive for any of these laptops was not encrypted, sensitive information stored would be accessible by circumventing other technical controls. We reported in June 2007 that we were able to access all the information stored on an unencrypted FEMA laptop.¹⁰

Laptop Images Are Not Standardized

FEMA has not configured its laptop computers with all USGCB settings. We determined that the standard Windows XP baseline image complies with 92 percent of USGCB controls. However, our scan results revealed that Windows XP laptops in the field are not being configured with this standard image. In comparison, Windows 7 laptops are consistently compliant with most USGCB controls. As figure 3 shows, our scan results from a selection of

⁹ Federal Information Processing Standard 197 details the Advanced Encryption Standard, a cryptographic algorithm that can be used to protect electronic data.

¹⁰ *Improved Administration Can Enhance Federal Emergency Management Agency Laptop Computer Security* (OIG-07-50), June 2007.

laptops revealed an average of 55 percent Windows XP compliance and 92 percent Windows 7 compliance.

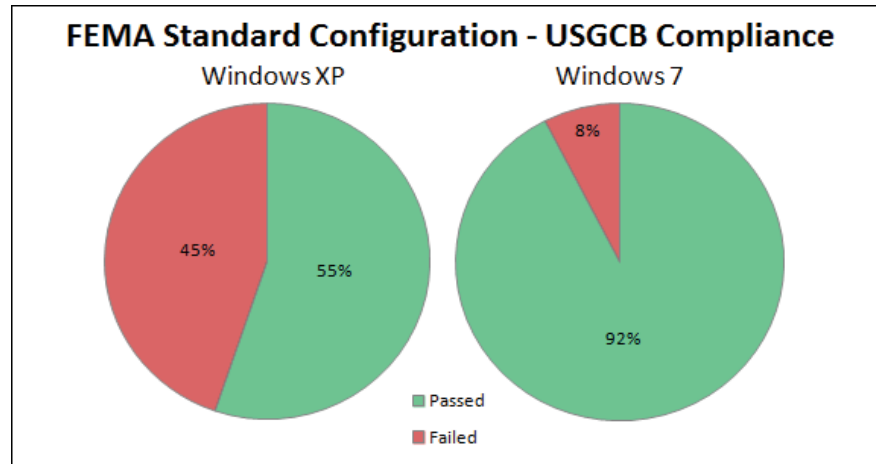


Figure 3: Windows 7 and Windows XP USGCB compliance

We identified the following examples of noncompliance with USGCB requirements:

- Administrative rights are granted automatically when users log in through the Windows recovery console.¹¹ Granting administrative rights automatically when using the recovery console increases the risk of unauthorized access and allows system controls to be circumvented.
- Default administrator accounts on laptops have not been renamed or disabled. When Windows is installed, it configures several built-in accounts by default, such as an administrator account. Default administrator accounts provide attackers with a known user that has elevated permissions to access information stored locally on the laptop.
- Password-protected screen savers are not used to secure unattended computers after a period of inactivity. Without screen saver passwords, a malicious user may log into an unattended laptop to gain unauthorized access to FEMA information.

The discrepancy between Windows XP and Windows 7 compliance exists because Windows XP laptops lack the policy that enforces these settings throughout the FEMA domain. As a result,

¹¹ The recovery console is used primarily to repair damaged installations of Windows.

compliance with USGCB settings on Windows XP laptops varies greatly throughout FEMA.

The *Federal Information Security Management Act of 2002* requires agencies to apply configuration management principles to Federal information systems, including hardware, software, and standardized configuration settings.¹² In September 2010, the Chief Information Officer Council approved USGCB settings required for Windows 7 in addition to those previously specified for Windows XP.¹³

Without proper USGCB controls in place, sensitive information stored on FEMA laptops could be subject to potential exploits. Additionally, a compromised laptop could provide unauthorized access to the FEMA network. Fully implementing a standard configuration across the component will reduce the risk that sensitive information may be exposed.

Security Patches Are Not Applied to Laptops Timely

FEMA is not effectively deploying security patches to its laptops. Our vulnerability scans identified missing security patches, such as a July 2007 patch for Microsoft Visio that could allow arbitrary remote code execution. Arbitrary remote code execution would allow unauthorized users to take over control of a laptop. Other examples of missing security patches include Adobe Acrobat, Java, Adobe Flash Player, Microsoft patch bulletins, Adobe Air, and Web browsers. Figure 4 shows the percentage of scanned laptops with at least one detected instance of a known high-risk vulnerability.

¹² Congress enacted Title III of the *E-Government Act of 2002* (Public Law 107-347, Sections 301–305) to improve security within the Federal Government. Title III of the *E-Government Act*, entitled the *Federal Information Security Management Act*, provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support Federal operations and assets.

¹³ Office of Management and Budget 07-11 required that agencies running Windows XP adopt the settings outlined in the Federal Desktop Core Configuration no later than February 1, 2008. In September 2010, the USGCB replaced the Federal Desktop Core Configuration as the baseline for configuration requirements.

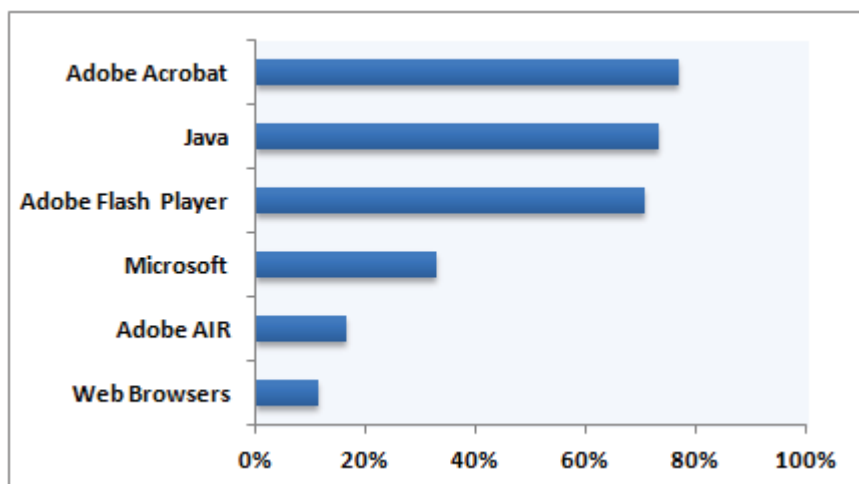


Figure 4: Percentage of laptops with known application vulnerabilities

FEMA uses a centralized third-party software solution to deploy patches to systems throughout the enterprise. The current process requires security patches to be approved and sent to servers at regional offices to deploy locally. Local administrators are then notified to deploy patches to the systems at their site. An OCIO representative explained that patches may not be deployed timely because of delays between the time patches are sent to onsite servers and when they are applied to local systems.

DHS requires components to reduce system vulnerabilities by promptly installing security and software patches. Security patches are required to protect systems from potential exploits and vulnerabilities as they are discovered. The DHS EOC releases vulnerability management messages to alert components to security patches. The messages direct users of the timeframe in which a security patch should be applied.

Failure to install software patches could expose FEMA laptops to risk, depending on the severity of the vulnerability identified. Malicious emails can trick users into visiting a Web page or opening files designed to exploit vulnerabilities in software installed on laptops. Ensuring that software is up to date minimizes this risk and protects laptops and the sensitive information they process and store.

FEMA Password Policy Is Not Enforced for Local Users

FEMA local administrator accounts are not configured to comply with DHS password policy. Weak password controls are configured on laptops, resulting in easily guessed passwords on

local accounts. Specifically, Active Directory has not been configured to remember any of the previous passwords used, require local passwords to be changed every 180 days, and require password complexity. Additionally, local accounts are being shared among onsite administrators. Weak password controls may allow malicious users to gain unauthorized access to sensitive information stored on laptops.

Although FEMA has configured Active Directory controls that are applied to all users, these controls do not adhere to DHS password requirements. Instead, FEMA uses the National Emergency Management Information System Access Control System (NACS), an in-house developed software tool, to enforce user password settings. Although password controls enforced through NACS apply to all domain accounts, this policy does not apply to local accounts on FEMA laptops. Since local administrator accounts receive only the Active Directory settings and not the stronger NACS controls, these accounts may have weak passwords.

DHS requires users to change their passwords every 90 days to prevent users from gaining unauthorized access. DHS also requires accounts to be assigned to one user and not shared among personnel. Additionally, USGCB policy states that password complexity must be enabled and account history set to remember the last 24 passwords used.

Weak password controls can result in a compromised administrator account. FEMA information stored on a laptop with a compromised local administrator account could be exposed to unnecessary risk. Additionally, since these accounts do not belong to a single person, audit trails cannot be used to identify who accessed information stored on a laptop.

Laptop Sanitization Is Not Consistently Documented

Laptop sanitization is not being consistently documented at the sites visited.¹⁴ Specifically, these sites do not document execution of this process and certify the completion of sanitization according to FEMA policy. When laptop sanitization is not performed and documented consistently, FEMA cannot ensure that unauthorized users cannot recover deleted data from the hard drives.

¹⁴ Sanitization refers to the process of removing and erasing data from storage media such that there is reasonable assurance that the data may not be easily retrieved and reconstructed.

For example, although laptop sanitization is being performed and documented at the DISC, Bothell Mobile Emergency Response Support (MERS) Detachment, and New Orleans JFO, the process is not recorded at the FEMA Region 10 headquarters or Albany JFO. In addition, a locally developed form is used to document laptop sanitization at the DISC, Bothell MERS Detachment, and New Orleans JFO, instead of the required OCIO certification. We also determined that the forms developed at these sites do not contain all the required information, such as date, sanitization method used, and name of the Property Custodian.

In November 2010, the Administrator issued Directive #137-2, which requires documentation of laptop sanitization and includes a Sanitization Certification Form for use in meeting the requirement. In addition, it specifies that no electronic media will be issued, transferred, disposed of, or returned to vendors or manufacturers without being sanitized to the standards of this Directive.

DHS requires components to maintain records of the sanitization and disposition of information systems storage media. In addition, FEMA requires the Property Custodian and Enterprise Service Desk/Local IT Site Support to complete the Sanitization Certification Form included in the media sanitization and release directive when a laptop is sanitized. The National Institute of Standards and Technology recommends that agencies sanitize digital media using approved equipment and procedures. In addition, agencies should track, document, and verify media sanitization and destruction actions and periodically test sanitization equipment and procedures to ensure correct performance.

According to FEMA personnel, they do not document laptop sanitization according to OCIO requirements because the OCIO has not informed offices of the media sanitization procedures issued in November 2010. Further, the OCIO does not verify whether offices comply with the media sanitization requirements.

Without documenting media sanitization, FEMA cannot verify that a laptop has been sanitized, and deleted data cannot be easily recovered. As a result, there is greater risk of mistakenly disposing of or reassigning a laptop that has not been wiped of sensitive information. This may compromise the confidentiality of information on the laptop, especially if the laptop is unencrypted.

Recommendations

We recommend that the Chief Information Officer:

Recommendation #3: Accelerate the implementation schedule to deploy full hard drive encryption for all laptops to prevent unauthorized access to information.

Recommendation #4: Ensure that all required USGCB configuration settings are implemented on FEMA laptops.

Recommendation #5: Ensure that security and software patches are deployed in a timely manner to all FEMA laptops.

Recommendation #6: Implement appropriate management controls to ensure that laptop sanitization procedures, including documentation, are followed at all FEMA facilities.

Management Comments and OIG Analysis

FEMA concurred with recommendation 3. The Chief Information Officer has accelerated the upgrade of all laptops from Windows XP to a Windows 7 image that includes hard drive encryption software. The estimated completion date of the upgrade and implementation of hard drive encryption is November 2012.

We agree that the steps FEMA has taken and plans to take begin to satisfy this recommendation. This recommendation will remain open until FEMA provides documentation to support that all planned corrective actions are completed.

FEMA concurred with recommendation 4. FEMA stated that the required USGCB configuration settings had been implemented on all Windows laptops, and asked that this recommendation be closed.

During our audit, scan results revealed that Windows 7 laptops are consistently compliant with most USGCB controls. However, we also found that Windows XP laptops in the field are not being configured with this standard image. We agree that FEMA will improve the compliance of USGCB settings when all laptops are upgraded to the Windows 7 image. This recommendation will remain open until FEMA provides documentation to support that all planned corrective actions are completed or the implementation of USGCB settings is verified through security testing.

FEMA concurred with recommendation 5. The Chief Information Officer has begun replacing current patch management solutions with an agency-wide centralized patching mechanism. The new patching mechanism will be fully deployed by September 2012.

We agree that the steps FEMA has taken and plans to take begin to satisfy this recommendation. This recommendation will remain open until FEMA provides documentation to support that all planned corrective actions are completed.

FEMA concurred with recommendation 6. The Chief Information Officer will improve the awareness of FEMA's Electronic and Hard Copy Media Sanitization and Release standard operating procedure and establish a process to monitor its enforcement by July 2012. The standard operating procedure requires the use of FEMA Form 137-1-1 to certify sanitization.

We agree that the steps FEMA plans to take begin to satisfy this recommendation. This recommendation will remain open until FEMA provides documentation to support that all planned corrective actions are completed.

Performing Assessments Can Enhance Wireless Security

FEMA can enhance its wireless security by assessing the associated risks and the effectiveness of controls implemented to protect the data stored on and processed by its wireless networks and devices. When these assessments are not performed, there is greater risk that security controls implemented to protect FEMA's wireless networks can be circumvented.

The Risks of JFO Wireless Networks Have Not Been Assessed

FEMA has not performed risk assessments on its wireless networks at JFOs, as they are not included as part of the authorization boundary of any information systems. The use of sensitive wireless systems is approved by the OCIO, but JFOs are not included as part of any FEMA General Support System or major application, as required by DHS' system inventory methodology. As a result, the Authorizing Official does not have the most updated information to make credible risk-based decisions regarding the system.

The OCIO is aware that the JFOs are not accounted for in any recognized IT system. According to the OCIO, JFO wireless networks will eventually be included in the Enterprise Wireless Local Area Network system boundary. However, the process of formally accounting for them will take some time. As of

January 2012, the Enterprise Wireless Local Area Network has not received a full Authority to Operate, and the current system boundary includes only wireless networks deployed at distribution centers, not JFOs. The OCIO did not provide an expected date for granting the full Authority to Operate or for adding JFO wireless networks to the system boundary.

DHS requires that all IT assets be itemized and accounted for as part of a General Support System or Major Application. The use of wireless communications technologies is prohibited until it is approved by the appropriate Authorizing Official. Further, Authorizing Officials must approve the implementation and use of wireless systems at a specified risk level during the assessment and authorization process. Finally, appropriate and effective security measures are to be included in the System Security Plan.

As of January 2012, 56 JFOs were activated across the country. Including JFOs in recognized IT systems will help to ensure that the systems are tracked and secured as required by DHS. Further, the OCIO will be kept informed of risks associated with each wireless system.

Annual Security Assessments Have Not Been Performed for JFO Wireless Networks

FEMA has not performed annual security assessments on all of its JFO wireless networks as required by DHS. For example, the New Orleans JFO wireless network has not undergone a security assessment since the office was established in October 2005. JFO personnel said that they were not aware of the requirement to perform security assessments on wireless networks. The OCIO confirmed that assessments had yet to be performed.

According to the OCIO, since FEMA does not include JFO wireless networks in the boundary of any recognized IT system, annual wireless assessments are not required. However, the Network Operations Center does monitor the hardware that operates FEMA's wireless networks.

DHS requires that security assessments be conducted annually on all approved wireless systems. Wireless security assessments result in the ability to enumerate vulnerabilities, risk statements, risk levels, and corrective actions. The Information Systems Security Officer is required to perform a risk assessment periodically or when a major change is made that affects the overall system security posture.

Since annual wireless security assessments have not been performed, FEMA may not be aware of vulnerabilities that may lead to potential exploits. Routine security assessments can be used to identify rogue or unauthorized access points, backdoors, and other system vulnerabilities, as well as to enumerate vulnerabilities, levels of risk, and corrective actions. Further, risk mitigation plans prioritize corrective actions and implementation milestones in accordance with defined risk levels.

Recommendation

We recommend that the Chief Information Officer:

Recommendation #7: Account for all wireless networks within a recognized IT system and implement management controls to ensure that annual wireless security assessments are conducted.

Management Comments and OIG Analysis

FEMA concurred with recommendation 7. The Chief Information Officer will require that all wireless networks and devices be enrolled into the FEMA Network Operations Center for management and monitoring. In addition, the Chief Information Security Officer will establish controls to ensure that wireless security assessments are conducted annually. These efforts are expected to be completed by September 2012.

We agree that the steps FEMA plans to take begin to satisfy this recommendation. This recommendation will remain open until FEMA provides documentation to support that planned corrective actions are completed and all wireless networks are accounted for within a recognized IT system.

Appendix A

Purpose, Scope, and Methodology

The objective of our audit was to determine whether FEMA has implemented effective controls to protect its laptop computers and the sensitive data processed by its wireless networks and devices from potential exploits. Specifically, we determined whether FEMA has (1) implemented an effective inventory management process to safeguard its laptop computers, (2) implemented effective configuration management controls to protect its laptop computers, (3) implemented effective controls to ensure that sensitive information processed by its wireless networks and devices is protected from potential exploits, and (4) taken corrective actions to mitigate the findings cited in our prior audit reports, OIG-07-50 and OIG-08-14 (*SECRET*).

Our audit focused on requirements outlined in the *DHS Sensitive Systems Handbook 4300A, United States Government Configuration Baseline, DHS Windows XP Secure Baseline Configuration Guide, DHS Windows 7/Internet Explorer 8 Configuration Guidance*, and *FEMA Personal Property Manual 119-7-1*. We interviewed selected personnel and management officials in the Support Services and Facilities Management Division of the Office of the Chief Administrative Officer, IT Security Branch and Operations Support Branch of the Office of the Chief Information Officer, the Logistics Management Directorate of the Office of Response and Recovery, as well as personnel stationed at JFOs. Fieldwork was performed at the DISC in Winchester, VA; FEMA JFO in Albany, NY; FEMA JFO in New Orleans, LA; MERS Detachment in Bothell, WA; FEMA Region 10 headquarters in Bothell, WA; and FEMA headquarters in Washington, DC.

We reviewed FEMA inventory maintenance policies and procedures, employee exit processing procedures, access rights to LIMS, laptop sanitization procedures, laptop distribution procedures, laptop configuration and patch management plans, and wireless network security policy. In addition, we conducted vulnerability and USGCB compliance scans of Windows XP and Windows 7 laptop images on a random selection of 116 deployed laptops. We conducted testing to identify unauthorized wireless networks and signal leakage and performed an inventory evaluation of a random selection of 178 laptops. The laptops identified for our inventory evaluation were randomly selected from LIMS once we judgmentally identified locations for our site visits based on the concentration of laptops and use of wireless networks. The laptops identified for scans were randomly selected

Appendix A

Purpose, Scope, and Methodology

from four regional offices and one JFO, including from sites we visited.

We conducted this performance audit between September 2011 and January 2012 pursuant to the *Inspector General Act of 1978*, as amended, and according to generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based upon our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based upon our audit objectives. Major OIG contributors to the audit are identified in appendix C.

The principal OIG point of contact for the audit is Frank W. Deffer, Assistant Inspector General, Information Technology Audits, at (202) 254-4100.


Appendix B Management Comments to the Draft Report

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



MAY 21 2012

MEMORANDUM FOR: Charles K. Edwards
Acting Inspector General
Department of Homeland Security

FROM: David J. Kaufman 
Director
Office of Policy and Program Analysis

SUBJECT: OIG Draft Report: *Progress Has Been Made in Securing Laptops and Wireless Networks at FEMA* - For Official Use Only
OIG Project No. 11-151-ITA-FEMA

The Federal Emergency Management Agency (FEMA) appreciates the Department of Homeland Security (DHS) Office of the Inspector General's evaluation of our laptop security controls and wireless networks. The evaluation has been very helpful in identifying areas requiring improvement and prioritizing work to implement the recommendations.

FEMA concurs with the auditor's recommendations in the above referenced draft report. The FEMA Office of the Chief Information Officer (OCIO) is resolute in directing these audit recommendations be effectively implemented. Plans of Action and Milestones (POA&Ms) are being developed to ensure the recommendations are implemented in a timely manner. FEMA's OCIO Audit Remediation Team meets weekly with Action Officers to review the status of planned remediation milestones and address issues that are impeding progress. Branch Chiefs receive weekly reports reflecting the status of their organization's assigned actions and are working to correct findings. Implementation of corrective actions is a performance goal for each Branch Chief in the OCIO.

In reviewing the report, we noted that the number of laptops reported as lost or stolen was incorrect on page 8. The number should be changed from 13 to 25. Attachment 1 lists the related security incidents.

Regarding your recommendations, FEMA's response to each follows:

Recommendation #1: Implement appropriate management controls to ensure that all government-purchased laptops are accounted for in the Logistics Information Management System (LIMS) in accordance with applicable policy.

Response: FEMA Manual 119-7-1, *Personal Property* (Attachment 2), has established standards regarding accounting for laptops in LIMS. Property Management Officers (PMO) and Accountable Property Officers (APO) are required to follow this Manual. Conference calls with PMOs and APOs

Appendix B

Management Comments to the Draft Report

are routinely held that stress the importance of property accountability. Measures will be put in place to ensure that any discovery of laptops not being accounted for in LIMS is escalated to ensure that non-compliance is appropriately addressed. Policy regarding this control is already established. Compliance with policy will be tested in July after the annual inventory is completed.

This recommendation will remain open until it is tested and found to be effective. The expected completion date is July 2012.

Recommendation #2: Work with the Chief Information Officer to establish a process to ensure that the loss or theft of laptops is reported timely as security incidents to the DHS EOC.

Response: The FEMA Security Team aggressively investigates all reports of stolen laptops and other computer equipment. The Rules of Behavior (Attachment 3) that users sign when issued accountable property includes the requirement to report lost or stolen property to the FEMA Security Operations Center (SOC). Measures will be put in place to ensure that accountable property reported as missing during inventories are reconciled with the incident reports received by the SOC to ensure that the missing property was reported to the SOC promptly upon discovery. Instances where the incident was not reported will be escalated and appropriately addressed. Policy regarding this control is already established. Compliance with policy will be tested in July after the annual inventory is completed.

This recommendation will remain open until it is tested and found to be effective. The expected completion date is July 2012.

Recommendation #3: Accelerate the implementation schedule to deploy full hard drive encryption for all laptops to prevent unauthorized access information.

Response: Accelerating the upgrade from Windows XP to the current Windows 7 image would satisfy this requirement because the WinMagic agent is included on this image. The established timeline for completing this upgrade is November 30, 2012.

This recommendation is considered resolved and open until the upgrade is completed.

Recommendation #4: Ensure that all required USGCB configuration settings are implemented on FEMA laptops.

Response: All Windows laptops meet required USGCB configuration settings at this time.

FEMA requests that this recommendation be resolved and closed.

Recommendation #5: Ensure that security and software patches are deployed in a timely manner to all FEMA laptops.

Response: Patchlink and Windows Server Update Services (WSUS) are being phased out; Altiris, the centralized patching mechanism, will be fully deployed by September 30, 2012 provided receipt of follow-on funding. Agency-wide implementation of Altiris will correct this issue.

Appendix B

Management Comments to the Draft Report

FEMA considers this recommendation resolved and open until implementation of the above action.

Recommendation #6: Implement appropriate management controls to ensure that laptop sanitization procedures, including documentation, are followed at all FEMA facilities.

Response: *Electronic and Hard Copy Media Sanitization and Release* Standard Operating Procedure (SOP) standardizes the media sanitization process to include the usage of FEMA Form 137-1-1 to certify. The SOP was signed and published September 2, 2011 and is included as Attachment 4. The OCIO will re-socialize this SOP FEMA-wide and establish a process to monitor its enforcement by July 31, 2012. To address the issue on password policy not being enforced for local users described in the report, FEMA will update its group policy to address the password vulnerabilities. This action is planned for completion by June 30, 2012.

FEMA considers this recommendation resolved and open until implementation of the above action.

Recommendation #7: Account for all wireless networks within a recognized IT system and implement management controls to ensure that annual wireless security assessments are conducted.

Response: The CIO is requiring that all wireless devices/networks be enrolled into the FEMA Network Operations Center for management and monitoring. The Chief Information Security Officer will establish controls to ensure that wireless security assessments are conducted annually. These actions are scheduled to be completed by September 30, 2012.

FEMA considers this recommendation resolved and open until implementation of the above action.

Again, we thank you for the opportunity to review your draft report. If you have any questions, please have your staff contact Brad Shefka, FEMA's OIG and GAO Liaison, at 202-646-1308.

Attachment 1 – *Listing of Incident Reports for Lost or Stolen Laptops*

Attachment 2—FEMA Manual 119-7-1, *Personal Property*

Attachment 3—DHS 4300A, *Sensitive Systems Handbook*, Attachment G, Rules of Behavior

Attachment 4 – FEMA Standard Operating Procedures, *Electronic and Hard Copy Media Sanitization and Release*

Appendix C
Major Contributors to this Report

Chiu-Tong Tsang, Director
Mike Horton, IT Officer
Amanda Strickler, Team Lead
Bridget Glazier, IT Auditor
David Bunning, IT Specialist
Gregory Wilson, Management/Program Assistant
Matthew Worner, Referencer

Appendix D

Report Distribution

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Deputy Chief of Staff
General Counsel
Executive Secretariat
Assistant Secretary for Office of Policy
Assistant Secretary for Office of Public Affairs
Assistant Secretary for Office of Legislative Affairs
Administrator, FEMA
Chief Information Officer, DHS
Chief Information Security Officer, DHS
Chief Information Officer, FEMA
Chief Administrative Officer, FEMA
Chief Information Security Officer, FEMA
Associate Administrator, Response and Recovery, FEMA
Director, Compliance and Oversight, DHS OCISO
Director, GAO/OIG Liaison Office
Audit Liaison, CIO, DHS
Audit Liaison, CISO, DHS
Audit Liaison, FEMA
IT Audit Liaison, FEMA

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, please call the Office of Inspector General (OIG) at (202)254-4100, fax your request to (202)254-4305, or e-mail your request to our OIG Office of Public Affairs at DHS-OIG.OfficePublicAffairs@dhs.gov. For additional information, visit our OIG website at www.oig.dhs.gov or follow us on Twitter @dhsOIG.

OIG HOTLINE

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

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

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