

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Security Weaknesses Increase Risks to Critical Emergency Preparedness and Response Database (Redacted)



Notice: The Department of Homeland Security, Office of Inspector General, has redacted this report for public release. The redactions are identified as (b)(2), comparable to 5 U.S.C. § 552(b)(2). A review under the Freedom of Information Act will be conducted upon request.

Office of Information Technology

OIG-05-43

September 2005



**Homeland
Security**

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 DHS oversight responsibilities to promote economy, effectiveness, and efficiency within the department.

This report assesses the strengths and weaknesses of database security controls over Emergency Preparedness and Response (EP&R) resources. It is based on interviews with EP&R officials, direct observations, technical scans, 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.

A handwritten signature in cursive script that reads "Richard L. Skinner".

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Executive Summary	1
Background	3
Results of Audit	5
Strengthening of Database Security Procedures Is Needed	5
Recommendations	9
Management Comments and OIG Analysis	9
NEMIS Servers Are Vulnerable	10
Recommendations	18
Management Comments and OIG Analysis	18

Appendices

Appendix A: Purpose, Scope, and Methodology	20
Appendix B: Management's Response	22
Appendix C: Vulnerabilities Identified and Addressed	28
Appendix D: FISMA Metrics	29
Appendix E: NEMIS Architecture	31
Appendix F: Major Contributors to this Report	32
Appendix G: Report Distribution	33

Abbreviations

ATL	Advanced Technology Laboratory
C&A	Certification and Accreditation
CIO	Chief Information Officer
DBMS	Database Management System
DHS	Department of Homeland Security
DHS Handbook	DHS Sensitive Systems Handbook
DHS Policy	DHS Sensitive Systems Policy Publication 4300A
EP&R	Emergency Preparedness and Response Directorate
FISMA	Federal Information Security Management Act of 2002
ISS	Internet Security Systems

Table of Contents/Abbreviations

IT	Information Technology
NACS	NEMIS Access Control System
NEMIS	National Emergency Management Information System
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
-----	-----
SP	Special Publication

OIG

*Department of Homeland Security
Office of Inspector General*

Executive Summary

We audited the Department of Homeland Security (DHS) and its organizational components' security program to evaluate the security and integrity of select sensitive but unclassified mission critical databases.¹ This audit included a review of access controls, continuity of operations, and change management policies and procedures. This report assesses the strengths and weaknesses of security controls over Emergency Preparedness and Response (EP&R) database resources.

Our objective was to determine whether EP&R had implemented adequate and effective controls over sensitive data contained in its National Emergency Management Information System (NEMIS). We interviewed EP&R officials, reviewed database security documents, and performed technical tests of six [REDACTED] servers and two domain controllers.

EP&R has not established adequate or effective database security controls for NEMIS. EP&R has developed and implemented many essential security controls for the NEMIS system, including the establishment of a change management process and the development of a NEMIS Information Technology (IT) contingency plan. However, additional work remains to implement the access controls and continuity of operations safeguards necessary to protect sensitive NEMIS data adequately. Specifically, EP&R has not (1) implemented effective procedures for granting, monitoring, and removing user access;

¹ DHS "organizational components" are defined as directorates, including organizational elements and bureaus, and critical agencies.

(2) maintained and reviewed adequate [redacted] or (3) conducted NEMIS IT contingency training or testing. In addition, vulnerabilities existed on NEMIS servers related to access rights and password administration, configuration management, [redacted]. Due to these database security exposures, there is an increased risk that unauthorized individuals could gain access to critical EP&R database resources and compromise the confidentiality, integrity, and availability of sensitive NEMIS data. In addition, EP&R may not be able to recover NEMIS following a disaster.

Subsequent to the completion of our audit work, officials from EP&R stated that they had taken or planned to take corrective action to address [redacted] of the [redacted] vulnerabilities identified during our technical testing. As our fieldwork was complete, we did not verify that the vulnerabilities had been remedied. EP&R did not provide a corrective action plan for the remaining 56 vulnerabilities. See Appendix C for an overview of the vulnerabilities we identified.

We are recommending that the EP&R Under Secretary direct the Chief Information Officer (CIO) to:

- Ensure that adequate controls for granting, monitoring, and removing user access to NEMIS are implemented.
- Develop and implement an IT contingency training and testing program for NEMIS.
- [redacted]
- Develop and implement corrective action plans to address all identified NEMIS vulnerabilities and configuration weaknesses.

In addition, to comply with the Office of Management and Budget's (OMB) *Federal Information Security Management Act of 2002* (FISMA) reporting requirements, we evaluated the effectiveness of EP&R's information security program and practices as implemented for NEMIS.³ EP&R has not aligned

[redacted]

³ FISMA is included under Title III of the E-Government Act of 2002 (Public Law 107-347).

fully its security program with DHS' overall policies, procedures, or practices. For example, security controls had not been tested in over a year; a contingency plan has not been tested; security control costs have not been integrated into the life cycle of the system; and, system and database administrators have not obtained specialized security training. Appendix D summarizes the results of our FISMA evaluation.

Fieldwork was conducted from December 2004 through January 2005 at the EP&R Office of the CIO; Mount Weather Facility in Bluemont, VA; regional offices in Atlanta, GA and Philadelphia, PA; and the Office of Inspector General's (OIG) Advanced Technology Laboratory (ATL).⁴ See Appendix A for our purpose, scope, and methodology.

In response to our draft report, the EP&R CIO generally concurred with our recommendations and is in the process of implementing corrective measures. In addition, based on the results of our review, the CIO plans to implement an independent annual security assessment of NEMIS. EP&R's response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

A database is one or more large structured sets of data (fields, records, and files) organized so that the data can be easily accessed, managed, and updated. Most often, databases are associated with software used to update and query the data, called a database management system (DBMS). The DBMS can be an extremely complex set of software programs that controls the organization, storage, and retrieval of data in a database. In addition, the DBMS, in conjunction with its host operating system, controls access to the data and ensures the security and integrity of the database. DBMS' can be classified according to their architectural model (e.g., relational, hierarchical, or network), and can be centralized on one platform or distributed across multiple servers.

Databases and DBMS' have become a more frequent target of attack for malicious users. Such an attack can result in financial loss, loss of privacy, or a breach of national security as well as the many other varieties of corruption that result from unauthorized access to sensitive data. To counter this threat, a

⁴ The ATL supports our capability to perform effective and efficient technical assessments of DHS information systems and 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.

number of security options are available to protect the data housed in databases. For these measures to be effective, however, DBMS security controls must be properly configured and maintained. In addition, as database products have become more complex and the attacks against them have increased, a number of vulnerabilities have been identified that could be exploited by attackers. DBMS vendors have responded by issuing patches or fixes for discovered vulnerabilities. These patches must be applied—quickly and appropriately—to ensure that critical data is protected adequately.

NEMIS is a component-wide system of hardware, software, telecommunications, and applications that provide an information technology base to EP&R and its partners for carrying out the organization’s emergency management mission. Since the system became operational in late 1998, NEMIS has allowed EP&R to manage responses to disasters, public and congressional activities, financial activities, presidential disaster declarations, response programs, and state government recovery projects more effectively. For example, NEMIS provides incident tracking and coordination activities, allows individuals and small businesses to apply for assistance, and processes requests from the states for funding of hazard mitigation projects.

NEMIS utilizes a three-tiered client/server architecture based on a [REDACTED] database, server-based applications, and individual user workstations.⁵ The system requires significant utilization of [REDACTED] on geographically dispersed dedicated servers with corresponding requirements for system and database administration. NEMIS consists of many integrated subsystems that are distributed over as many as [REDACTED] separate servers in the production environment and accessed by thousands of client workstations. See Appendix E for an overview of the NEMIS architecture.

DHS Sensitive Systems Policy Publication 4300A (DHS Policy) provides direction to DHS components regarding the management and protection of sensitive systems. Also, this policy outlines the management, operational, and technical controls necessary for ensuring confidentiality, integrity, availability, and authenticity within the DHS IT infrastructure and operations. DHS Policy requires that its components ensure that strong access controls, IT contingency planning safeguards, and change and configuration management procedures are

[REDACTED]

implemented for all systems processing sensitive but unclassified information. The department developed the DHS Sensitive Systems Handbook (DHS Handbook) to provide components with specific techniques and procedures for implementing the requirements of this policy. Further, in November 2004, DHS published a series of secure baseline configuration guides for certain software applications, such as [REDACTED].

The National Institute of Standards and Technology (NIST) has issued several publications related to database system access controls, change and configuration management, and IT contingency planning. Specifically, NIST Special Publication (SP) 800-12, *An Introduction to Computer Security: The NIST Handbook*, provides guidance for establishing adequate access controls for sensitive government systems, including the use of strong passwords, encryption, and user administration practices. Also, NIST SP 800-12 provides guidance on effectively controlling changes to sensitive information systems. Further, NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, provides instructions, recommendations, and considerations for government IT contingency planning.

Results of Audit

Strengthening of Database Security Procedures Is Needed

EP&R has not developed and implemented the security controls necessary to protect NEMIS and its data. In assessing the procedures governing sensitive data contained in NEMIS, we identified user administration, auditing, and IT contingency planning weaknesses. As a result, there is significant risk that the security procedures protecting EP&R's critical databases may not prevent unauthorized access to its systems and data. In addition, EP&R may not be able to recover NEMIS operations following a disaster or disruption.

User Administration Procedures Are Incomplete

EP&R has implemented a process for granting, monitoring, and removing NEMIS user access that includes many of the controls necessary to protect access to the system and its data. For example, EP&R has established a process to document user access authorizations in a standard format and maintain these authorizations on file. Further, EP&R has implemented a process to disable automatically user accounts that have not been utilized in 90 days, and NEMIS

officials conduct weekly reviews of [REDACTED]. However, additional work remains to implement the access control procedures needed to limit system access to the appropriate personnel adequately and effectively. Specifically:

- [REDACTED]

- EP&R has not implemented procedures for performing periodic revalidations of NEMIS access authorizations. NEMIS officials do not perform regular reviews of all accounts with access to the system to ensure that the access granted remains appropriate. These reviews are not being performed because of the large number of user accounts on the system (15,503 at the time of our review).

DHS Policy requires that components ensure that user access is controlled and limited based on positive user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity.⁶ The policy also requires that:

- [REDACTED]
- System managers or owners revalidate all accounts at least annually.

Because NEMIS user administration procedures have not been fully implemented, there is greater risk that [REDACTED], while current users may have more access to the system than needed to fulfill their job responsibilities. As a result, the sensitive information in NEMIS may not be adequately protected.

⁶ The principle of least privilege requires that users be granted the most restrictive set of privileges needed to perform authorized tasks.

NEMIS Auditing Is Inadequate

EP&R does not [REDACTED] for NEMIS. Specifically:

- EP&R has not developed sufficient procedures to [REDACTED] for NEMIS. EP&R maintains [REDACTED] pertinent information related to [REDACTED]. However, audit trail records are [REDACTED]. In addition, only two and a half years of historical [REDACTED] exists for NEMIS, as the earlier [REDACTED] had been deleted.
- None of the database servers we examined had [REDACTED]. According to NEMIS officials, [REDACTED] due to the concern that it would negatively impact system performance.

According to DHS Policy, audit trails must contain sufficient information to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. Further, DHS Policy requires that Information Systems Security Officers review audit trail information weekly or in accordance with the system security plan, and that audit trail information be retained for seven years.

Audit trails help ensure individual accountability by providing the ability to track a user's activities while accessing an automated system. However, to be effective, significant security events must be recorded and the audit trails must be reviewed and retained. According to the DHS Handbook, the review of audit trail information is essential because unauthorized access, modification, or destruction of data may only be discovered through the review process. As a result of the lack of database auditing and adequate audit review and retention procedures, inappropriate access to sensitive data or malicious changes to NEMIS may not be detected and investigated.

IT Contingency Training and Testing Has Not Been Accomplished

EP&R has established an IT contingency plan for NEMIS that outlines the procedures to recover the system following a disruption in services as a result of an emergency or a disaster. However, EP&R has not provided training to key personnel on its NEMIS IT contingency plan, and an annual test of the NEMIS IT contingency plan has not been conducted. According to the NEMIS Contingency Plan Coordinator, a scheduled tabletop exercise of the plan was delayed due to the resources needed to respond to the 2004 hurricane season.

Further, we identified the following issues related to NEMIS data backup, restoration procedures, and environmental controls:

- The backup tapes used for onsite and offsite storage of NEMIS data are not stored in fireproof and waterproof containers.
- EP&R has not conducted a formal test of data backup and restoration procedures for NEMIS.
- Cleaning supplies were stored in one of the server rooms housing NEMIS computer equipment, and another server room had regular carpeting installed, rather than anti-static carpet.

According to NEMIS system administrators, some of the data backup and environmental control weaknesses have not been addressed due to the cost associated with procuring the proper equipment. Further, formal tests of the NEMIS data restoration procedures have not been performed because some data is occasionally restored for operational purposes, and the officials felt that this provided sufficient assurance that the procedures were adequate.

According to DHS Policy and NIST guidelines, each element of an IT contingency plan must be tested annually to confirm the accuracy of individual recovery procedures and the overall effectiveness of the plan. DHS and NIST also require that all personnel involved in IT contingency planning efforts be identified and trained in the procedures and logistics of IT contingency planning and implementation. According to NIST, this training should be provided at least annually. Further, DHS requires that quarterly tests of data backup and restoration procedures be performed, and that adequate environmental controls be established for sensitive systems and data.

IT contingency testing and training are essential to ensuring that contingency planning is successful. Testing enables deficiencies to be identified and

addressed, and helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. Formal tests of established data restoration procedures are an integral part of testing the overall contingency plan, and help ensure that all necessary data can be recovered in the event of a disaster. In addition, contingency plan personnel should be trained to execute their respective recovery procedures without the aid of the actual document, in the event that paper or electronic versions of the plan are unavailable for the first few hours after a disaster. As a result of the lack of IT contingency plan training and testing, including tests of the NEMIS data restoration process, EP&R lacks assurance that the component will be able to resume operations in a timely manner following a disaster.

Recommendations

To protect sensitive NEMIS data effectively, we recommend that the EP&R Under Secretary direct the CIO to:

1. Ensure that adequate controls for granting, monitoring, and removing NEMIS user access are implemented according to DHS requirements as well as NIST guidelines.
2. Develop and implement an IT contingency training and testing program for NEMIS to ensure that key personnel are trained on the plan annually, and that an annual test of the NEMIS IT contingency plan is conducted.

Management Comments and OIG Analysis

EP&R concurs with recommendation 1. EP&R plans to adopt additional measures to improve NEMIS user administration and access control, including [redacted]; staggered annual revalidation of all user accounts; and, an automated method to notify system administrators and information system security officers of individuals who no longer require access. In addition, EP&R plans to implement [redacted] on all NEMIS platforms, including [redacted]. However, the implementation of [redacted] is pending the completion of the NEMIS continuity of operations site, which is planned to become operational by the end of fiscal year 2005. Further, EP&R plans to archive NEMIS audit logs for seven years, as required by DHS Policy.

We accept EP&R's response to implement additional NEMIS user administration and access controls, as well as [REDACTED]. However, we maintain that EP&R should implement [REDACTED], and the component should establish a process to [REDACTED]. Also, EP&R should establish a timeline for the implementation of these additional NEMIS controls.

EP&R concurs with recommendation 2. EP&R plans to establish a NEMIS continuity of operations site by the end of fiscal year 2005. As part of this process, EP&R will conduct IT contingency training for NEMIS personnel. In addition, EP&R plans to develop a standard tabletop exercise for testing IT contingency plans by October 2005. Further, EP&R has instituted [REDACTED] backup capability for NEMIS, and has conducted data restoration tests using this functionality.⁷

We accept EP&R's response to train NEMIS personnel on the system's IT contingency plan as well as to conduct a tabletop test of the NEMIS IT contingency plan. Also, we accept EP&R's response to test NEMIS data restoration procedures using [REDACTED]. However, EP&R did not indicate that annual IT contingency plan testing or training would be completed, or that quarterly data restoration tests would be performed. We maintain that EP&R should ensure that periodic contingency testing and training are conducted.

NEMIS Servers Are Vulnerable

EP&R has not established effective database security controls for NEMIS. To assess the security of NEMIS databases, we performed vulnerability assessment scans to identify configuration weaknesses and vulnerabilities on NEMIS servers; and, conducted manual checks of the security settings on the central NEMIS database server to identify additional configuration weaknesses as well as to verify the results of our vulnerability assessment scans. In assessing the effectiveness of database controls, we identified issues related to access rights and password administration, configuration management, [REDACTED]. These control weaknesses could provide an attacker with the ability to gain inappropriate access to NEMIS and its data.

Access Privileges Were Not Appropriately Restricted

EP&R did not enforce strong identification and authentication measures for NEMIS. Many of the servers we tested did not appropriately restrict access to the system. For example:

- [Redacted]
- [Redacted]
- [Redacted]
- [Redacted]

According to NEMIS officials, several of these access rights and password vulnerabilities are the result of weaknesses in the NEMIS Access Control System (NACS) application. EP&R is in the process of implementing an upgrade to the NACS application that will enforce stronger identification and

[Redacted]

authentication controls for NEMIS. The implementation of the new system was scheduled for February 2005.

Table 1 illustrates the number of access rights and password management vulnerabilities that we identified for the NEMIS database servers and related hosts, along with the number of corrective actions that EP&R has planned or already taken to address these weaknesses.

Table 1: Access Rights and Password Vulnerabilities Identified and Addressed

	Number of Vulnerabilities Identified			Number That Have Been Addressed			Number For Which No Corrective Action Plan Was Provided
	High Risk	Medium Risk	Total	Corrected	Planned	Total	
[REDACTED]	2	7	9	2 (22%)	1 (11%)	3 (33%)	6 (67%)
[REDACTED]	1	4	5	1 (20%)	1 (20%)	2 (40%)	3 (60%)
[REDACTED]	1	6	7	1 (14%)	2 (29%)	3 (43%)	4 (57%)
[REDACTED]	1	4	5	1 (20%)	1 (20%)	2 (40%)	3 (60%)
[REDACTED]	0	0	0	N/A	N/A	N/A	N/A
[REDACTED]	2	9	11	1 (9%)	7 (64%)	8 (73%)	3 (27%)
[REDACTED]	0	0	0	N/A	N/A	N/A	N/A
[REDACTED]	3	9	12	2 (17%)	7 (58%)	9 (75%)	3 (25%)
Total	10	39	49	8 (16%)	19 (39%)	27 (55%)	22 (45%)
(a) Manual security parameter tests were only conducted on the NEMIS [REDACTED] Database Server.							

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

DHS Policy requires that its components ensure that user access is controlled and limited based on user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity. Further, the DHS Handbook and secure baseline

configuration guidelines provide specific requirements related to system security settings, including [REDACTED]

Often, passwords are the first lines of defense against hackers or insiders who may be trying to obtain unauthorized access to a computer system. The use of weak password controls, combined with inappropriate account policy settings and access rights, might allow unauthorized internal users or external hackers to gain access to EP&R networks and systems.

NEMIS Servers Are Not Configured Appropriately

EP&R did not configure network services and security parameters to protect NEMIS data and files. For example:

- [REDACTED]
- [REDACTED]

Table 2 illustrates the number of configuration management vulnerabilities that we identified for the NEMIS database servers and related hosts, along with the number of corrective actions that EP&R has planned or already taken to address these weaknesses.

[REDACTED]

Table 2: Configuration Management Vulnerabilities Identified and Addressed

Server	Number of Vulnerabilities Identified			Number That Have Been Addressed			Number For Which No Corrective Action Plan Was Provided
	High Risk	Medium Risk	Total	Corrected	Planned	Total	
[REDACTED]	1	15	16	0	1 (6%)	1 (6%)	15 (94%)
[REDACTED]	2	2	4	1 (25%)	1 (25%)	2 (50%)	2 (50%)
[REDACTED]	2	0	2	1 (50%)	0	1 (50%)	1 (50%)
[REDACTED]	1	1	2	0	0	0	2 (100%)
[REDACTED]	0	2	2	0	0	0	2 (100%)
[REDACTED]	1	5	6	0	1 (17%)	1 (17%)	5 (83%)
[REDACTED]	0	0	0	N/A	N/A	N/A	N/A
[REDACTED]	1	5	6	0	1 (17%)	1 (17%)	5 (83%)
Total	8	30	38	2 (5%)	4 (11%)	6 (16%)	32 (84%)

(a) Manual security parameter tests were only conducted on the NEMIS [REDACTED] Database Server.

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

According to NEMIS officials, some of the configuration weaknesses noted above are required for the proper functioning of the system. Specifically, EP&R officials stated that [REDACTED]. However, we determined that it would be possible to allow [REDACTED] without allowing [REDACTED].

NEMIS Had Not Been [REDACTED]

EP&R had not [REDACTED]. We examined each of the eight servers to determine if all of the appropriate [REDACTED].

Also, we reviewed the master database server to determine if all of the appropriate . Although EP&R had each of the servers we tested, the component had not . Specifically, we identified

In addition, EP&R officials stated that because they were planning to upgrade the NEMIS servers and transition to a new operating system, which occurred in February 2005.

Table 3 illustrates the number of vulnerabilities that we identified for the NEMIS database servers and related hosts, along with the number of corrective actions that EP&R has planned or already taken to address these weaknesses.

Table 3: Vulnerabilities Identified and Addressed

Server	Number of Vulnerabilities Identified			Number That Have Been Addressed		
	High Risk	Medium Risk	Total	Corrected	Planned	Total
	1	1	2	2 (100%)	0	2 (100%)
(a) Manual security parameter tests were only conducted on the NEMIS Database Server, and weaknesses were only identified on this server.						

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

DHS Policy requires that IT security in accordance with configuration management plans or direction from higher authorities. According to

----- is critical to the operational availability, confidentiality, and integrity of information technology systems. NIST recommends that organizations have an explicit and documented ----- policy as well as a systematic, accountable, and documented process for -----.

Because EP&R officials have not ----- the master NEMIS database server, a malicious user could ----- . In addition, critical vulnerabilities likely to exist in the system are not being addressed -----.

NEMIS Data And Files Were Not []

NEMIS was not configured to protect sensitive data and files through the use of ----- . Specifically:

- -----
- -----
- -----

EP&R officials stated that the implementation of some of the ----- protections noted above was pending the completion of an upcoming operating system upgrade. The upgrade was scheduled to be completed in June 2005.

Table 4 illustrates the number of ----- vulnerabilities that we identified for the NEMIS database servers and related hosts, along with the number of corrective actions that EP&R has planned or already taken to address these weaknesses.

Table 4: [REDACTED] Vulnerabilities Identified and Addressed

Server	Number of Vulnerabilities Identified			Number That Have Been Addressed			Number For Which No Corrective Action Plan Was Provided
	High Risk	Medium Risk	Total	Corrected	Planned	Total	
[REDACTED]	1	3	4	0	2 (50%)	2 (50%)	2 (50%)
[REDACTED]	0	0	0	N/A	N/A	N/A	N/A
[REDACTED]	1	1	2	0	2 (100%)	2 (100%)	0
[REDACTED]	1	1	2	0	2 (100%)	2 (100%)	0
[REDACTED]	1	0	1	0	1 (100%)	1 (100%)	0
[REDACTED]	1	1	2	0	2 (100%)	2 (100%)	0
[REDACTED]	1	0	1	0	1 (100%)	1 (100%)	0
[REDACTED]	1	1	2	0	2 (100%)	2 (100%)	0
Total	7	7	14	0	12 (86%)	12 (86%)	2 (14%)

(a) Manual security parameter tests were only conducted on the NEMIS [REDACTED] Database Server.

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

According to the DHS Handbook, [REDACTED] a reliable and achievable way to ensure confidentiality for sensitive data. DHS Policy requires that the department’s components identify IT systems transmitting sensitive information that may require protection, and develop [REDACTED] for their sensitive IT systems. In addition, NIST recommends that [REDACTED] tools be implemented to protect the integrity and confidentiality of critical data and software programs. As a result of these [REDACTED]

[REDACTED]

Subsequent to the completion of our review, EP&R officials stated that they have taken or plan to take steps to address many of the access rights and password administration, configuration management, [REDACTED] weaknesses we identified. We did not verify that the problems have been resolved. EP&R did not provide a corrective action plan for the remaining vulnerabilities.

Recommendations

To protect sensitive NEMIS data, we recommend that the EP&R Under Secretary direct the CIO to:

3. [REDACTED]
4. Develop and implement corrective action plans to address all identified NEMIS vulnerabilities and configuration weaknesses to reduce the risk of system compromise or failure.

Management Comments and OIG Analysis

EP&R concurs with recommendation 3. EP&R plans to [REDACTED]. However, certain database servers cannot be [REDACTED] due to the use of a commercial product [REDACTED]. EP&R will need to engineer the software product out of NEMIS and replace it with another product prior to [REDACTED] on these servers. Also, EP&R plans to establish a process to [REDACTED] for the NEMIS system.

We accept EP&R's response to [REDACTED], and to [REDACTED]. EP&R should establish a process for [REDACTED] in addition to a timeline for the implementation of these changes.

EP&R concurs with recommendation 4. EP&R stated that the component has taken or plans to take action to address the vulnerabilities identified during the review. However, the remediation of some weaknesses is pending the completion of NEMIS system upgrades. In addition, EP&R is determining the feasibility of acquiring [REDACTED].

However, EP&R estimates that implementation will cost approximately \$10,000 per connected computer.

We accept EP&R's response to address the vulnerabilities identified during our review. In addition, we recommend that EP&R determine the feasibility of using the software-licensing contract under negotiation between DHS and ----- . Once finalized, this contract is projected to reduce the cost of obtaining ----- , by 85 percent.

Purpose, Scope, and Methodology

The objective of this audit was to determine whether DHS has implemented adequate and effective controls over sensitive data contained in its mission critical databases. As part of our audit of DHS database security, we conducted reviews of critical databases at the following DHS components:

- Emergency Preparedness and Response
- United States Citizenship and Immigration Services
- United States Coast Guard
- United States Secret Service

For each of the databases included, we determined whether the component had implemented effective access controls, continuity of operations capabilities, and change management processes. Our focus was to test the implementation of secure configurations on the hosts controlling access to sensitive DHS data. In addition, we obtained FISMA information required for our annual independent evaluation.

To identify EP&R's critical database systems, we analyzed the DHS Enterprise Architecture inventory of the Department's IT assets as of October 2004. We supplemented this information with NIST SP 800-26 Security Self-Assessments, where available. Based on our analysis, we selected NEMIS for inclusion in our review.

We used two software tools to conduct internal security tests to evaluate the effectiveness of controls implemented for NEMIS:

- Internet Security Systems (ISS) Internet Scanner 7.0 was used to detect and analyze vulnerabilities on DHS servers. NIST SP 800-42, *Guideline on Network Security Testing*, identifies ISS Internet Scanner as a common testing tool.
- ISS Database Scanner 4.3 was used to analyze the configurations of the databases and DBMS' selected for review.

In addition, we performed extensive manual security parameter checks on the master NEMIS database server to confirm the results of our scans and identify any additional security weaknesses. Upon completion of the tests, we

provided EP&R with technical reports detailing the specific vulnerabilities detected on the NEMIS system and the actions needed for remediation.

We conducted fieldwork at the EP&R Office of the CIO in Washington, DC; Mount Weather Facility in Bluemont, VA; regional offices in Atlanta, GA and Philadelphia, PA; and the OIG's ATL. We conducted our audit between December 2004 and January 2005 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 F.

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.

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



August 10, 2005

MEMORANDUM FOR: Frank Deffer
Assistant Inspector General for Information Technology
Department of Homeland Security

THROUGH: Michael D. Brown *M. Brown*
Under Secretary
Emergency Preparedness and Response Directorate

FROM: *for* Barry C. West *B. West*
Chief Information Officer/Director
Information Technology Services Division

SUBJECT: Comments on the Draft Audit Report Entitled "Security Weaknesses Increase Risks to Critical Emergency Preparedness and Response Database," dated June 2005

FEMA staff continues to work to strengthen the protection of the National Emergency Management Information System (NEMIS) database. The work started prior to the audit, and incorporates recommendations where they can be applied.

I appreciate the efforts of your audit team and am pleased to report that 71 of the 100 suggested security enhancements have been implemented. Attachment B documents those that have been implemented and explains why each of the 29 left has not yet been implemented (the majority of which are dependent on [REDACTED] within DHS and EP&R). I know that we have a highly skilled motivated staff supporting NEMIS, however, it is clear that staff is fully employed with day-to-day activities (especially in times like the fall of 2004, when everyone in EP&R was focused on disaster responses). I believe your report has demonstrated how useful an independent assessment of NEMIS security can be. Starting in FY 2006, I intend to have an independent security assessment of NEMIS done annually.

Unfortunately, as discussed with your audit team, for technical reasons not all of your recommendations can be immediately applied. In particular, we cannot [REDACTED] due to limitations imposed by currently having a [REDACTED]

Appendix B
Management's Response

commercial product (used for viewing application documentation). First, we need to engineer that product out of the system. Second, replace it with another product. And, finally, [REDACTED]. A second recommendation that we cannot, for technical reasons, immediately implement is [REDACTED]. Again, as we discussed with your team, we have tried that in the past but had to [REDACTED] for performance reasons (our systems could not [REDACTED]). However, when we get the NEMIS COOP site up and activated, we may be able to implement your recommendation.

Our detailed comments are in the Attachments. If you have any questions or wish to discuss further any of the points in this memorandum, please ask a member of your staff to contact Deborah Moradi, Chief, Policy and Compliance Section, at (202) 646-3154.

Attachments

cc: IT
IT-SE-CS
IT-IR
IT-IR-PC

ATTACHMENT A

Comments on Draft Inspector General Report:

*“Security Weaknesses Increase Risks
To Critical Emergency Preparedness and Response Database”
(A-IT-05-003)*

These comments are organized according to their locations in the report, from beginning to end, with bolded captions in the draft audit report as markers. The four recommendations in the draft audit report, found on pages 9 and 17, are inserted in the comments at pertinent points.

Database Access Control and Continuity Procedures Have Not Been Fully Implemented

NEMIS User Administration Procedures Are Incomplete

DHS OIG Recommendation #1: Ensure that adequate controls for granting, monitoring, and removing user access are implemented according to DHS requirements as well as NIST guidelines.

In April 2001, the EP&R Chief Information Officer issued a memorandum addressed to senior EP&R officials entitled “NEMIS Management and Access Controls Policy” which stated, in part, [REDACTED]

A draft FEMA instruction entitled [REDACTED] is expected to be signed by the Under Secretary imminently. The instruction broadens the policy quoted in the previous paragraph and more specifically assigns responsibility for ensuring [REDACTED]

[REDACTED] This instruction is an interim solution to improving user administration and access control.

In conjunction with this instruction, EP&R plans to adopt staggered annual revalidation of all user accounts, synchronized with annual Security Awareness Training.

EP&R is planning to identify an automated method that can be used to notify system administrators and Information System Security Officers of individuals who no longer require access.

NEMIS Auditing Was Inadequate

Regarding the OIG finding that EP&R has not [redacted] [redacted] EP&R informed the OIG upon receipt of the draft version of the report that [redacted] the NEMIS environment at this time would cause a major negative impact of [redacted] based on experiences when tried with previous versions of NEMIS and [redacted]. To [redacted] without causing that problem, EP&R is [redacted] [redacted]

After researching documentation on [redacted] capabilities (which were not available in previous [redacted] releases), EP&R management has decided to [redacted] [redacted] across all NEMIS platforms. This [redacted] will [redacted]

In response to the OIG finding that EP&R has not developed sufficient procedures to review and retain operating system audit trail information, EP&R intends to implement Oracle Database Auditing in the near future, as discussed previously. These audit logs, along with system, Oracle Listener, Apache and application logs, will be stored in a central location and will be archived for 7 years, in accordance with DHS policy.

IT Contingency Training and Testing Has Not Been Accomplished

DHS OIG Recommendation #2: Develop and implement an IT contingency training and testing program for NEMIS to ensure that key personnel are trained on the plan annually and that an annual test of the NEMIS IT contingency plan is conducted.

EP&R received funding in FY 2005 to establish a COOP site for NEMIS. The initial operational capability for this site is planned for the end of FY 2005. It will include adequate training for NEMIS personnel and testing of the plan. EP&R is developing a standard tabletop exercise to enable us to test our contingency plans. This tabletop testing capability is planned to be available in October 2005. This site is planned to be a hot COOP and also function as the primary NEMIS site when updates are being performed on the main NEMIS system. This utilization will ensure that the COOP failover works and that the COOP site is constantly upgraded to match the main site.

In response to the OIG finding that EP&R has not conducted a formal test of data backup and restoration procedures for NEMIS, EP&R wishes to inform the OIG that contingencies at three levels are specified in the NEMIS IT Contingency Plan and that contingencies are exercised at two of the levels. Level 1 is continuously exercised on a daily basis as part of NEMIS standard operating procedures. (Since the time of this audit, EP&R has successfully restored the NEMIS [redacted] NPSC servers from backups. We also have instituted [redacted] and we have run [redacted]

[REDACTED] Level 2 is exercised for major system upgrades. Level 3 will be part of the COOP development activity.

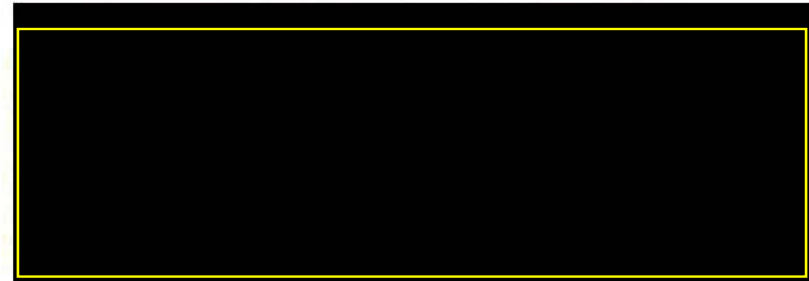
NEMIS Servers Are Vulnerable

Access Privileges Were Not Appropriately Restricted

DHS OIG Recommendation #3: Update the NEMIS database software to a version that is currently supported by the vendor, and ensure that all necessary patches are installed.



NEMIS Servers Are Not Configured Appropriately



NEMIS Had Not [REDACTED]





NEMIS Data and Files Were Not [redacted],

EP&R is determining the feasibility of acquiring [redacted].
[redacted] If determined to be feasible, resources will be requested to implement this recommendation. Implementation of [redacted] is tied to initiation of [redacted] [redacted] which began in June 2005. The approach planned is to use [redacted] [redacted] will need to be purchased in order to [redacted]. The estimate of cost for this is \$10,000.00 per CPU. **All** machines [redacted] will need to be configured to [redacted].

DHS OIG Recommendation #4: Develop and implement corrective action plans to address all identified vulnerabilities and configuration weaknesses to reduce the risk of system compromise or failure.

The CIO develops corrective actions plans to ensure tracking, assignment of responsibility, and correction of deficiencies identified during reviews and audits.

Appendix C
Vulnerabilities Identified and Addressed

Server	Number of Vulnerabilities Identified			Number of Vulnerabilities That Have Been Addressed			Number For Which No Corrective Action Plan Was Provided
	High Risk	Medium Risk	Total	Corrected	Planned	Total	
Password and Access Rights	10	39	49	8 (16%)	19 (39%)	27 (55%)	22 (45%)
Configuration Management	8	30	38	2 (5%)	4 (11%)	6 (16%)	32 (84%)
	1	1	2	2 (100%)	0	2 (100%)	0
	7	7	14	0	12 (86%)	12 (86%)	2 (14%)
Total	26	77	103	12 (12%)	35 (34%)	47 (46%)	56 (54%)

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

FISMA Requirements

Title III of the E-Government Act, entitled FISMA, provides a comprehensive framework to ensure the effectiveness of security controls over information resources that support federal operations and assets.¹³ The agency's security program should 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.

To comply with OMB's FISMA reporting requirements, we evaluated the major applications selected for this audit to determine whether DHS continues to make progress in implementing its agency-wide information security program. We collected information related to certification and accreditation (C&A), system impact level determination, NIST SP 800-26 annual assessment, security control costs integrated into the life cycle of the system, assessment of E-authentication risks, specialized security training, and plan of action and milestones (POA&M).¹⁴

Our evaluation of NEMIS shows that EP&R has not implemented certain security management practices into its information security program, as required by FISMA.

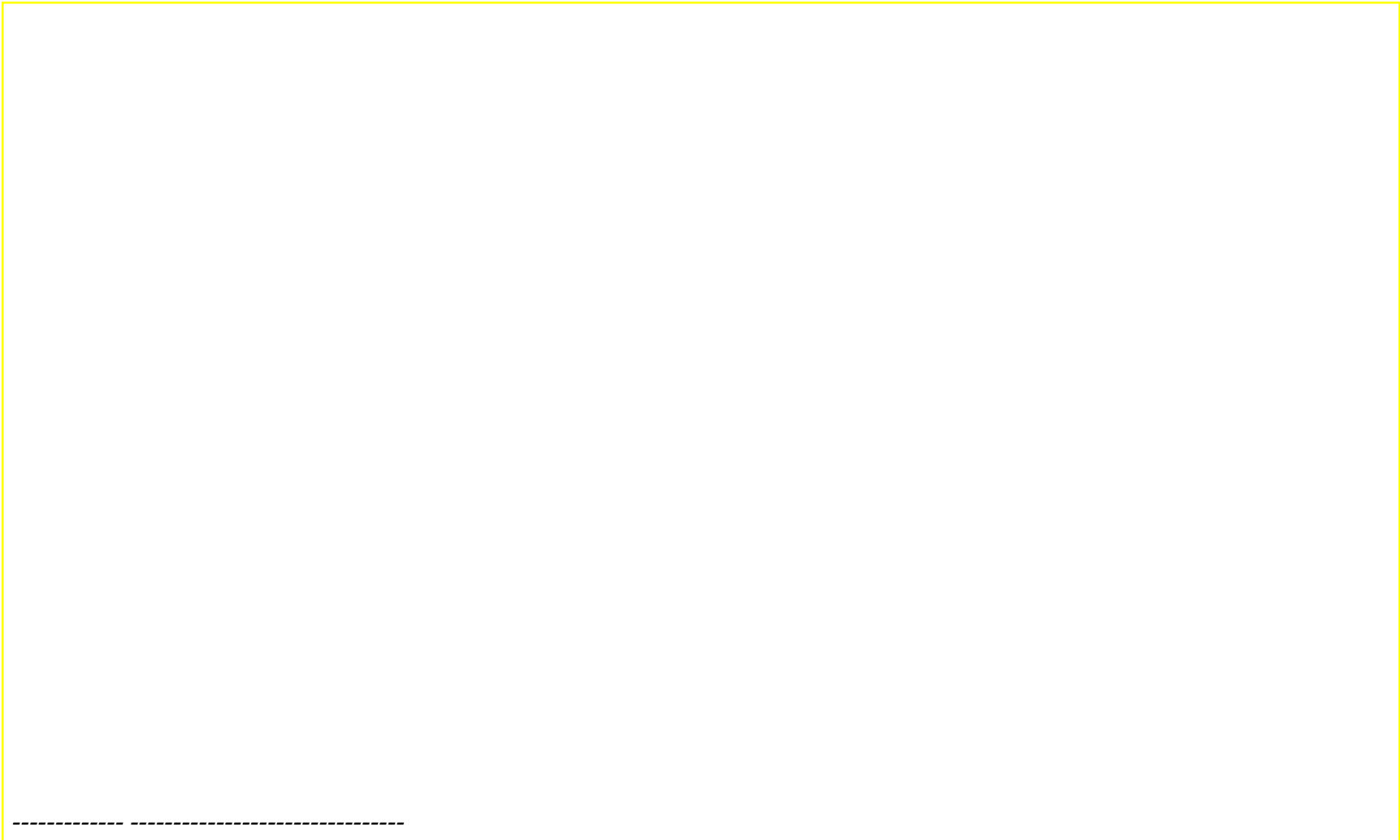
¹³ The E-Government Act of 2002 (Public Law 107-347), signed into law by the President on December 17, 2002, recognized the importance of information security to the economic and national security interests of the United States.

¹⁴ As required by: OMB M-04-04, *E-Authentication Guidance for Federal Agencies*, and NIST 800-63, *Electronic Authentication Guideline*.

Table 2: FISMA Compliance Metrics

FISMA Reporting Requirements	EP&R (NEMIS)	Notes
Does the major application have a complete and current C&A, including a risk assessment and security plan?	Yes	The system has a current authority to operate, and the C&A documentation includes a security plan and a risk assessment
Has the major application's impact level been determined according to Federal Information Processing Standard 199 criteria?	Yes	The loss of confidentiality, availability or integrity of NEMIS would have an overall high impact on EP&R's mission.
Does the major application have a complete and current NIST SP 800-26 annual assessment?	Yes	A NEMIS assessment was completed on August 13, 2004.
Does the assessment indicate that security controls have been tested and evaluated in the last year?	No	The assessment indicated that security controls had been routinely tested. However, security controls had not been tested in over a year.
Does the assessment indicate that a contingency plan has been established and tested?	No	The assessment indicated that the IT contingency plan had not been tested.
Have security control costs been integrated into the life cycle of the system?	No	EP&R plans to incorporate security control costs into the life cycle for upcoming version releases.
Has an assessment of E-Authentication risk been performed for the major application?	Yes	The NEMIS applications that are publicly accessible have been assessed for E-Authentication risk, though some assessments were in draft at the time of our review.
Have the system and database administrators obtained specialized security training?	No	System and operations personnel were not being provided specialized security training due to funding limitations.
Does the major application have any existing POA&Ms?	Yes	As of September 23, 2004, there were POA&Ms for five NEMIS weaknesses.

Source: OIG table based on interviews with EP&R personnel and analysis of database documentation.



Information Security Audits Division

Edward G. Coleman, Director

Patrick Nadon, Audit Manager

Jason Bakelar, Audit Team Leader

Chris Udoji, Auditor

Pedro Calderon, Referencer

Advanced Technology Division

Jim Lantzy, Director

Michael Goodman, Security Engineer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Emergency Preparedness and Response, Under Secretary
Executive Secretary
General Counsel
Chief Information Officer
Chief Information Security Officer
Public Affairs
Emergency Preparedness and Response, Chief Information Officer
Emergency Preparedness and Response, Audit Liaison
Director, Departmental GAO/OIG Liaison Office
Director, Compliance and Oversight Program
Chief Information Officer Audit Liaison
Office of Security

Office of Management and Budget

Chief, Homeland Security Branch
DHS OIG Budget Examiner

Congress

Appropriate Congressional Oversight and Appropriations Committees

Additional Information and Copies

To obtain additional copies of this report, call the Office of Inspector General (OIG) at (202) 254-4100, fax your request to (202) 254-4285, 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 the OIG Hotline at 1-800-323-8603; write to DHS Office of Inspector General/MAIL STOP 2600, Attention: Office of Investigations – Hotline, 245 Murray Drive, SW, Building 410, Washington, DC 20528; fax the complaint to (202) 254-4292; or e-mail DHSOIGHOTLINE@dhs.gov. The OIG seeks to protect the identity of each writer and caller.