DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Security Weaknesses Increase Risks to Critical DHS Databases (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-06-17 **December 2005**

Office of Inspector General

U.S. Department of Homeland Security
Washington, DC 20528

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 DHS database resources. It is based on interviews with DHS officials, direct observations, technical tests, and a review of applicable documents.

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

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Appendices

Abbreviations

ATL	Advanced Technology Laboratory
C&A	Certification and Accreditation
CIO	Chief Information Officer
Coast Guard	United States Coast Guard
DBMS	Database Management System
DHS	Department of Homeland Security
DHS Handbook	DHS Sensitive Systems Handbook
DHS Policy	DHS Sensitive Systems Policy Publication 4300A
DISA	Defense Information Systems Agency
EP&R	Emergency Preparedness and Response
FISMA	Federal Information Security Management Act of 2002

Table of Contents/Abbreviations

ISS	Internet Security Systems
IT	Information Technology
MISLE	Marine Information for Safety and Law Enforcement
NEMIS	National Emergency Management Information System
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
USCIS	United States Citizenship and Immigration Services
Secret Service	United States Secret Service
SP	Special Publication
SSWeb	Secret Service Web

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] The audit included reviews of access controls, change management, and continuity of operations policies and procedures. This report assesses the strengths and weaknesses of security controls over DHS database resources.

Our objective was to determine whether DHS had implemented adequate and effective controls over sensitive data contained in its mission critical database systems. We interviewed DHS officials, reviewed database security documents, and performed technical tests of the operating system and database management system (DBMS) security controls for the Emergency Preparedness & Response (EP&R) National Emergency Management Information System (NEMIS); the U.S. Citizenship and Immigration Services (USCIS) Central Index System; the United States Coast Guard (Coast Guard) Marine Information for Safety and Law Enforcement (MISLE) system; and the United States Secret Service (Secret Service) Secret Service Web (SSWeb) system. 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 DHS' information security program as implemented for the systems included in our review.[2]

DHS components have implemented security program requirements that have improved DHS' security posture. Specifically, each of the components have certified and accredited the systems we reviewed; determined the system impact

[1] DHS "organizational components" are defined as directorates, including organizational elements and bureaus, and critical agencies.
[2] FISMA is included under Title III of the E-Government Act of 2002 (Public Law 107-347).

level; and, completed National Institute of Standards and Technology (NIST) Special Publication (SP) 800-26 assessments.[3] In addition, three of the four components have documented plans of action and milestones (POA&M) for system weaknesses.[4] Further, DHS has established policies, procedures, and baseline configuration guidelines related to database security, and DHS components have implemented many of the essential security controls for their mission critical database systems. For example, each of the components has implemented physical security and environmental controls to protect their systems and data. Also, the components have established policies and procedures to control routine and emergency changes to their database systems.

DHS components have not aligned fully their security programs with FISMA requirements. Specifically, security controls are not routinely tested or evaluated; contingency plans have not been established and tested; security control costs have not been integrated into the life cycle of the systems; and, system and database administrators have not obtained specialized security training. Although DHS has established secure baseline configuration guidelines for certain software applications, these guidelines are not sufficiently detailed; and, DHS has not established configuration guidelines for other software applications used by the department's database systems. Further, additional work remains for DHS components to implement the user administration, auditing, configuration management, and continuity of operations procedures necessary to protect sensitive data effectively.[5]

Due to these database security weaknesses, individuals could gain access to critical DHS database resources and compromise the confidentiality, integrity, and availability of sensitive data. Further, DHS may not be able to recover critical database systems following a disaster.

We are recommending that the Chief Information Officer (CIO):

- Strengthen DHS' existing baseline configuration guides, and implement guidelines for other commonly used software applications.
- Ensure that components adhere to DHS information security procedures and database configuration guidelines.

[3] System impact level determination according to Federal Information Processing Standard (FIPS) 199 criteria.
[4] Appendix E summarizes the results of our FISMA evaluation.
[5] Audit trails maintain a record of system activity both by system and application processes and by users of the systems and applications. The audit trail is the evidence that demonstrates how a specific transaction was initiated, processed, and summarized. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.

Fieldwork was conducted from November 2004 through May 2005 at DHS and contractor facilities in Washington, DC; ---------- ---------- MD; ---------- , VA; ---------- , WV; ----------, PA; -------- , GA; ------- , TX; and, the Office of Inspector General's (OIG) Advanced Technology Laboratory (ATL).[6] See Appendix A for our purpose, scope, and methodology, as well as a description of each of the database systems included in our review.

In response to our draft report, DHS concurred with our recommendations and is in the process of implementing corrective measures. For example, DHS issued configuration guidance for ---------- software in October 2005, and plans to revise other existing guidance. In addition, DHS has implemented a review process for verifying that the components are complying with DHS certification and accreditation (C&A) requirements and implementing such requirements as configuration guidance. DHS also provided suggestions for clarifying the scope and findings of our review. Where appropriate, changes were made to more accurately present the issues in this report. DHS' 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 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 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 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

[6] 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.

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.

DHS Sensitive Systems Policy Publication 4300A (DHS Policy) provides direction to DHS components regarding the management and protection of sensitive systems. In addition, this policy outlines the management, operational, and technical controls necessary for ensuring confidentiality, integrity, availability, and authenticity within the DHS information technology (IT) infrastructure and operations. DHS Policy requires that its components ensure that strong access controls, IT contingency planning safeguards, and change as well as configuration management procedures are implemented for all systems processing sensitive but unclassified information. The department developed the DHS Sensitive Systems Handbook (DHS Handbook) to provide 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 --------- DBMS.

NIST has issued several publications related to database system access controls, change and configuration management, and IT contingency planning. Specifically, NIST 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. 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.

The *Federal Information Security Management Act of 2002* requires each agency to develop, document, and implement an agency-wide information security program to provide security for the information and information systems, including wireless systems, that support the operations and assets of the agency. Policies should ensure that information security is addressed throughout the life cycle of each agency information system and determine minimally acceptable system configuration requirements.

Results of Audit

Database Security Procedures Need Strengthening

While DHS has issued security policies and procedures for user administration, auditing, configuration management, and IT contingency planning, the organizational components have not implemented these procedures fully. Specifically, none of the components have implemented effective procedures for granting, monitoring, and removing user access for the systems we reviewed. Although each component has implemented controls to protect database access, additional work remains to implement the control procedures to ensure that access to sensitive data is granted appropriately. For example, EP&R had not ---------- ---------- ; USCIS had not ---------- ; the Coast Guard has not ---------- ; and, the Secret Service had not ---------- [7]

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.[8] The DHS Handbook also provides requirements related to granting, monitoring, and removing user access. Because user administration procedures were not fully implemented, there is greater risk that individuals may have inappropriate access to these systems.

Further, none of the components have implemented effective procedures for recording, reviewing, and retaining audit trail information for the systems we reviewed, as illustrated in Table 1:

[8] The principle of least privilege requires that users be given the most restrictive set of privileges that will still enable them to perform authorized tasks.

Table 1: Audit Trail Procedures Implemented by Component and Type

	EP&R NEMIS	USCIS Central Index System	Coast Guard MISLE	Secret Service SSWeb
Operating System Auditing				
Audit Trail Recorded	-----	-----	----	-----
Audit Trail Reviewed	- -	-----	----	- -
Audit Trail Retained	- -	- -	----	- -
Database Auditing				
Audit Trail Recorded	- -	-----	- -	- -
Audit Trail Reviewed	- -	- -	- -	- -
Audit Trail Retained	- -	-----	- -	- -

Source: OIG table based on the results of technical testing and interviews with component officials

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, the DHS Handbook 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. Because DHS components have not implemented adequate audit procedures, inappropriate access to sensitive data or malicious changes to database systems may not be detected or investigated.

None of the components have implemented effective procedures for ensuring that the database systems we audited are configured appropriately and system changes are controlled. EP&R, the Coast Guard, and Secret Service did not configure appropriately the servers supporting their respective database systems.[9] In addition, USCIS did not control sufficiently an upgrade to the Central Index System DBMS, and the Secret Service does not have a SSWeb configuration management plan or documented configuration management procedures for the system.

DHS Policy requires that organizational components establish, implement, and enforce change management and configuration management controls on all IT systems and networks; and, that organizational components prepare configuration management plans for all IT systems and networks. Further, the DHS Handbook requires that the initial configuration of a system be

[9] See Appendix C for an overview of the vulnerabilities identified during our review.

documented in detail, and that all subsequent changes to any components of the system be controlled through a complete and robust change management process. Until change and configuration management plans and procedures are implemented adequately and effectively, there is greater risk that routine and emergency changes to the system will not be controlled.

Finally, we determined that none of the components have implemented effective procedures for developing and testing IT contingency safeguards for the systems we reviewed, as illustrated in Table 2:

Table 2: IT Contingency Planning Procedures Established by Component and Type

	EP&R NEMIS	USCIS Central Index System	Coast Guard MISLE	Secret Service SSWeb
IT Contingency Plan Developed	Yes	**No**	**No**	**No**
IT Contingency Plan Tested	**No**	**No**	**No**	**No**
Key Personnel Trained on the Plan	**No**	**No**	**No**	**No**
Backup Data Retained and Stored Appropriately	**No**	**No**	Yes	**No**
Data Restoration Procedures Tested Quarterly	**No**	**No**	Yes	**No**

Source: OIG table based on the results of technical testing and interviews with component officials

DHS Policy requires that comprehensive IT contingency plans be developed, tested, exercised, and maintained for critical major applications and general support systems. Also, DHS and NIST 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. Further, DHS requires that components implement and enforce backup procedures for all Sensitive IT systems and data; data backups be stored both on-site and off-site in a secure facility, in fireproof and waterproof containers; and, quarterly tests of data backup and restoration procedures be performed. As a result of the lack of adequate contingency planning and testing, including proper retention and storage of backup media as well as tests of the data restoration process, the components lack assurance that they will be able to resume operations following a disaster.

According to component officials, many of these security procedures have not been implemented because equipment or software tools have not been obtained. For example, the Coast Guard plans to[redacted] as part of an upcoming system upgrade. Also, EP&R and the Secret Service are not [redacted]. In addition, component officials stated that they have taken or plan to take actions to address several of the weaknesses noted above, including the development and testing of IT contingency plans for the NEMIS, MISLE, and SSWeb systems.

DHS Configuration Guidelines Require Additional Detail

DHS has not established adequate configuration guidelines for operating system and DBMS software applications. Although DHS has issued secure configuration guidelines for seven software applications, these guidelines do not contain sufficient information to ensure that DHS database systems are configured appropriately.[10] We compared the DHS secure configuration guidelines for the DBMS and operating system software products used by NEMIS, the Central Index System, MISLE, and SSWeb to configuration guidelines issued by the National Security Agency (NSA), Defense Information Systems Agency (DISA), and the Center for Internet Security (CIS).[11] The DHS configuration guides failed to address critical security issues or did not provide sufficient information to ensure that the software could be configured appropriately. For example:

- The DHS [redacted] *Database Management System Secure Baseline Configuration Guide* does not address database auditing, the protection of critical DBMS files and [redacted], or many specific operating issues such as[redacted] In addition, several areas addressed by the guide do not provide sufficient information regarding correct configuration settings. For instance, [redacted]

[10] DHS has issued secure baseline configuration guidelines for [redacted]

[11] These guidelines were obtained from the NIST Computer Security Resource Center, http://csrc.nist.gov/pcig/index.html

[redacted] See Appendix D for the results of our detailed analysis of the DHS secure configuration guidelines for [redacted] DBMS.

- The DHS [redacted] *Secure Baseline Configuration Guide* does not address critical areas, such as requiring the use of role-based access controls and the configuration of certain security settings. For instance, the guide does not address [redacted], which if properly configured can help prevent denial of service attacks.[13]
- The DHS [redacted] *Secure Baseline Configuration Guide* does not address monitoring network access attempts and the configuration of certain security settings. For instance, the guide does not address [redacted].
- The DHS [redacted] *Secure Baseline Configuration Guide* provides sufficient information regarding a basic installation of [redacted] software. However, the guide does not contain information regarding the implementation of specific types of [redacted].

Further, DHS has not issued configuration guides for other DBMS and operating system software products used by the database systems included in our review. For example, DHS has not issued configuration guidelines for [redacted], which is employed by the MISLE and SSWeb systems. DHS had not issued guidance for [redacted]

[redacted]

[13] A denial of service attack is a form of attacking another computer to prevent legitimate users of a system from using the computer or its services.

[redacted]

-------- software because the department did not consider it a standard DBMS platform. However, following the completion of our review, DHS issued specific configuration guidance for ----- -------- ---------- software as part of the guidance updates issued in October 2005.

Until DHS issues detailed secure baseline configuration guidelines for database software applications, DHS components will not have adequate guidance on the appropriate configuration of the department's database systems. The database configuration weaknesses we identified during our review were largely the result of default system settings that were not changed at the time the software was installed. The issuance and enforcement of secure baseline configuration guidelines could help ensure that database servers and devices are appropriately configured prior to being placed into operation.

Recommendations

To enhance DHS' security guidance for database systems, we recommend that the CIO:

1. Strengthen DHS' existing DBMS and operating system configuration guides, and implement guidelines for other commonly used software products.

To protect sensitive data housed in the department's critical database systems, we recommend that the CIO:

2. Ensure that components adhere to DHS information security procedures and database configuration guidelines.

Management Comments and OIG Analysis

DHS concurs with recommendation 1. In response to the OIG's draft report, DHS plans to update the existing configuration guides and has issued three additional guides. For example, DHS published configuration guidance for ---------- ---------- software in October 2005. However, DHS stated that the comparison of the DHS configuration guide for --------- DBMS to configuration guides published by NIST/DISA and NSA/CIS (see Appendix D) did not account for the tailoring needed for a diverse department such as DHS. DHS designed its configuration guides to not be comprehensive, so as not to establish requirements that would disable legacy applications, and the guides do not preclude system owners from emplacing controls that are more stringent. In addition, DHS indicated that the report did not adequately consider network

security controls implemented as part of the department's defense-in-depth strategy, which would mitigate many of the vulnerabilities that may result from inappropriately configured operating system and DBMS software.

We accept DHS' response to update the existing configuration guides and to issue additional guidance based on current or expected needs. Also, we agree that any configuration guidance issued by DHS should be tailored to the department's operating environment. However, we maintain that, rather than publishing non-comprehensive guidance and relying on the components to implement the necessary controls, DHS should establish comprehensive guidance and implement a process for components to be granted a waiver in situations where compliance with the requirements would have a significant negative affect on the operation of legacy systems. In addition, we agree with DHS on the importance of strong perimeter and network security controls. However, we believe that even in the presence of strong network security controls, operating system and DBMS controls are still necessary to provide sufficient security for mission critical DHS systems, particularly against insider attacks.

DHS concurs with recommendation 2. DHS components are responsible for ensuring the quality of system security as part of their C&A activities, and the configuration guidance is a key element in this process. Following the completion of the audit, DHS implemented a review process for verifying that the components are complying with DHS C&A requirements and are properly implementing such requirements as configuration guidance. This process includes a high-level review of all key C&A elements, as well as a more detailed review of a subset of systems.

We accept DHS' response to implement a review process to ensure that components are complying with DHS information security procedures and database configuration guidelines.

DHS also provided suggestions for clarifying the scope and findings of our review. For example, DHS stated that by only using red and green in the color coding system of the chart in Appendix C, the report did not provide credit to those components that had addressed most, but not all, of the identified vulnerabilities. In response to DHS' comments, we provided additional clarification for our technical findings, and we modified Appendix C to illustrate those components that had addressed most of the identified vulnerabilities.

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:

Component	System	Purpose
Emergency Preparedness and Response	National Emergency Management Information System	NEMIS provides an information technology base to EP&R and its partners for carrying out the organization's emergency management mission. NEMIS allows EP&R to manage better responses to disasters, public and congressional activities, financial activities, presidential disaster declarations, response programs, and state government recovery projects. 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.
United States Citizenship and Immigration Services	Central Index System	The Central Index System assists in the enforcement of the immigration laws of the United States. The system contains information on the status of approximately 55 million individuals, including permanent residents, naturalized citizens, border crossers, and other individuals of interest to the federal government. The system provides DHS field offices, ports of entry, and examination and inspection sites access to biographical and status information on individuals seeking legal entry to or residence in the United States. The Central Index System also assists the department in the identification of individuals who violate the terms of their stay, who enter the United States illegally, or who are otherwise not entitled to entry or benefits.
United States Coast Guard	Marine Information for Safety and Law Enforcement	MISLE is used to track marine safety and law-enforcement activities involving commercial and recreational vessels. MISLE is comprised of two main components: the Marine Safety Network and the Vessel Documentation System. The Marine Safety Network allows Coast Guard personnel to input and obtain information on Coast Guard marine safety activities, such as waterway details, inspection information (vessel and facility), and incident investigation data. The Vessel Documentation System, which supports the marine banking community, is used by the National Vessel Documentation Center to assist in processing vessel registrations and tracking vessel ownership information.
United States Secret Service	Secret Service Web	SSWeb serves as the secure corporate intranet for the Secret Service. The SSWeb system consists of eight applications, including: [redacted]

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 the OIG's annual independent evaluation.

To identify 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.

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

- 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 select database servers to confirm the results of our scans and identify any additional security weaknesses. Upon completion of the tests, we provided component officials with technical reports detailing the specific vulnerabilities detected on their system and the actions needed for remediation. We also issued separate reports to each of the components describing the weaknesses identified and recommendations for improvement.

We conducted fieldwork at DHS and contractor facilities in Washington, DC; ---------- --- ---------- , MD; ---------- , VA; ---------- --, WV; ----------, PA; -------- , GA; ------ -, TX; and, the OIG's ATL. We conducted our audit from November 2004 through July 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, DC 20528

NOV 15 2005

Homeland Security

MEMORANDUM TO: Richard L. Skinner, Inspector General

FROM: Scott Charbo, Chief Information Officer

SUBJECT: Response by the DHS Office of the CIO to the Draft Audit Report - Security Weaknesses Increase Risks to Critical DHS Databases (OIG-05-XXX)

General Comments

Thank you for the opportunity to comment on the subject report. The results provided in the draft report comprise both observations and recommendations. The observations are valuable to our program improvement efforts and the recommendations are generally consistent with our plans and activities.

The Component-level compliance observations were extremely valuable and will prove instrumental in helping to refine the FY06 information security program goals. The ongoing efforts by the Office of the CIO (OCIO) and the Office of the Inspector General (OIG) will help ensure that the security of information systems and data supporting the Department's mission are achieved.

OIG Recommendations

The report offered two recommendations:

1. Strengthen DHS' existing DBMS and operating system configuration guides, and implement guidelines for other commonly used software products.
2. Ensure that components adhere to DHS information security procedures and database configuration guidelines.

CIO Response

The OCIO concurs with the recommendations from OIG and has implemented actions to address these issues in FY06. The following actions have been initiated by the OCIO to address the issues identified in the OIG recommendations.

Recommendation 1: The OCIO releases additional/revised configuration guidance based on current or expected needs at least annually. For example, the specific [redacted] configuration guidance mentioned in the OIG Findings was released as part of the 4th Quarter FY05 configuration guidance updates in October 2005.

www.dhs.gov

The existing guidance will be revised and any necessary new guidance will be released as the Department identifies opportunities for improvement.

- Clarification: The initial guidance which was used as part of this OIG review was issued in November 2004. At that time [redacted] Server was not considered a standard DBMS platform under either [redacted] or DHS rules. (Page 9, Paragraph 4). The OIG report has helped emphasize the more prevalent use of such products in the current DHS environment.

Recommendation 2: The Department has implemented a series of checks and balances to help ensure that a quality control process is implemented at both the Component and Department level to ensure system and data security.

- Components are responsible for ensuring the quality of system security as part of their overall certification and accreditation (C&A) process with management accepting residual risk for each of their systems. The professional judgment and system risks are best understood at this level. Configuration guidance is one key element of this process and reviewed and approved for implementation by the Designated Approving Authority.
- The Department works with the Components to document and publish these requirements as mentioned in the OIG report. In FY06, the Department has implemented a Compliance Review process for verifying that the components are complying with DHS C&A requirements and properly implementing such requirements as configuration guidance. The Department implements both a high-level review on all key C&A elements and a more detailed review on a subset of systems to most effectively leverage available funding.
- As part of the Departments FY06 C&A Remediation Plan, the Department has identified eleven (11) key elements that comprise the minimum acceptable effort associated with complying with DHS policy and procedures. The Compliance Review team will use these elements to help ensure that all DHS inventory systems are adequately protected based on artifact review of individual Component submissions.

In addition to the specific recommendation mentioned above, several clarifications regarding the OIG report are provided below.

1. **PURPOSE** – The report lists in Appendix D several settings that compare the DHS Baseline Guidance with the NSA and DISA comprehensive checklists for security. Both of these documents are guidelines that are designated by NIST under 800-26 to be TAILORED to fit the operational needs and security needs by the department they service. The OIG report suggests through Appendix D that the DHS Security Configuration Checklist is in gross non-compliance without consideration of the tailoring necessary for a department as wide and diverse as Homeland Security. Although the comparison highlights the differences, the fact that neither the NSA nor DISA checklists are applicable to the DHS environment is disregarded.

2. **SCOPE** - The hardening guides for DHS platforms, as directed, are not meant to be inclusive in their scope of the prescribed platforms. They were specifically written to be "widely applicable" guidance so as not to disable many legacy applications through a broad stroke of general policy. This does not and should not be perceived to preclude the platform and application owners from taking measures above the guidance to secure their assets. In fact, the risk assessment process defined by NIST, and mandated by DHS policy, requires that this tailoring should be conducted at the system level. The configuration guides also indicate that they are not comprehensive for their respective platforms. This scope falls in line directly with NIST 800-70 guidance on checklists and its FAQ found at http://csrc.ncsl.nist.gov/checklists/faq-general.html#f1 that state that:

   "While the use of security configuration checklists can greatly improve overall levels of security in organizations, no checklist can permit a system or a product to become 100% secure. However, use of checklists that emphasize hardening of systems against flaws or bugs inherent in software will typically result in greater levels of product security and protection from future threats." (800-70)

   Since the draft audit was made available to the DHS Office of the CIO the CISO's office has undertaken an update of all the guides as well as the addition of [redacted] to address the requests from the office of the IG to provide guidance.

   This guidance has been increased properly and fine tuned to represent optimum settings that can be applied to the core DHS security domain with the least specialization in role and taking compensating controls into consideration.

3. **DEFENSE IN DEPTH CONSIDERATION** – DHS employs many common controls beyond those offered at the DBMS or operating system that mitigate many of the issues cited in the document. Because the report only takes into account database and operating system controls in isolation, the additional controls employed at the system level were obviously not considered. If the report had the opportunity to take into consideration all controls such as quarantine networks that are using firewall devices to protect database services, intrusion detection and protection mechanisms, and n-tier application design that would only allow access through a firewall, network isolation, or some other form of network stateful inspection a more comprehensive perspective would be achieved. Without such a comprehensive approach it is understood that this report represents one perspective of the overall security approach.

   NIST 800-26 states the following in support of considering all defenses:

   "An important element of the assessment will be determining the effectiveness of the boundary controls when the information system is part of a network. The boundary controls must protect the defined system or group of systems from unauthorized intrusions.

   If such boundary controls are not effective, then the security of the systems under review will depend on the security of the other systems connected to it.

In the absence of effective boundary controls, the assessor should determine and document the adequacy of security controls related to each system that is connected to the system under review. " (800-26, 12)

General Comments

Page 15 - chart of addressed weaknesses contains no mention or consideration of risk level of findings. A component that is addressing 86%, 95%, 88%, and 95% is meeting the first recommendation of strengthening cited by the OIG. By only giving green for 100% the report could be viewed as setting unrealistic or impractical levels of compliance.

We modified Appendix C to illustrate those components that had addressed most of the identified vulnerabilities.

Technical Comments

Page 1, Paragraph 3 – the NIST 800-26 Checklist did not publish the control mappings indicated by the list in Appendix D until April of 2005 under NIST 800-53. The guidance provided by the OCIO was published months prior to the 800-53 release and has since been incorporated into DHS tools.

We determined whether DHS components had completed NIST 800-26 self-assessments as required by FISMA. NIST 800-26 was not used as criteria in the evaluation of DHS configuration guidelines.

Page 2, Paragraph 4 – the existing guidelines for platforms considered common were measured against a standard that came out in April 2005, several months after the DHS Guidance under evaluation in this report was delivered (November 2004). DHS issued guidance for ALL commonly used software applications identified in at the time it was published. DHS annually reviews hardening guidance for appropriate adjustments, and includes additional common software applications as needed or mandated by OMB guidance. For example guidance documents were issued in August 2005 as a result of these platforms being identified by the OIG as "common".

We included DHS' explanation for why additional configuration guidelines had not been issued.

Page 4, Paragraph 1 to 3 - The findings in the document focus exclusively on controls within the DHS Hardening Guides as prescriptive for control and assurance of the systems cited. At the DHS Department level it is impractical and exceedingly difficult to provide guidance that will fit all platforms and applications. The guides attempt to address core issues and provide a building block for components to leverage and to tailor as is the intent stated in NIST 800-26. Since the draft report was delivered the department has increased the number of controls to more prescriptive levels.

We noted DHS' progress in the report.

Page 4, Paragraph 4 - The issues cited in page 5 while relevant do not have to do with technical controls as much as human controls in areas of user provisioning, de-provisioning, that must be assessed through the DHS Office of Security in conjunction with the Office of the CIO. Each example is something that cannot be controlled entirely through information technology or OCIO and must be delivered in conjunction with the human resource processes and physical security CSO of the department and each component. The OCIO works with these other areas as necessary to help refine the approach.

We believe that DHS should coordinate with the Office of Human Resources, the Office of Security, or other DHS Management offices or functions as appropriate to ensure adequate enforcement of the implementation of the IT security policies and procedures outlined in DHS Sensitive Systems Policy Publication 4300A and the Sensitive Systems Handbook.

Page 9, Paragraph (Bullet) 2 – The term "mandatory role-based access control" is technically inaccurate. Mandatory control (MAC) and Role Based Access Control (RBAC) are not the same thing.

While they can be used in conjunction with one another the use of MAC in the context of assumes that the guidance was not written for nor does DHS use exclusively for its

This bullet also describes settings that depending upon the application are more specific than baseline guidance can practically be provided. In addition to prevent denial of service are commonly protected by network based IDS, host based IDS, and perimeter firewall systems. This setting must also be closely reviewed for application worthiness and should not be considered baseline guidance.

In our draft report we used the term "mandatory" to indicate that the use of role-based access controls should be required. We revised the sentence to eliminate any ambiguity. In addition, while we agree with DHS on the importance of strong perimeter and network security controls, we believe that even in the presence of strong network security controls, operating system and DBMS controls are still necessary to provide sufficient security for mission critical DHS systems, particularly against insider attacks.

Page 9, Paragraph (Bullet) 3 – The comments are very unique to the installation and support of specific attack scenarios for which network based compensating controls are more effective than host based controls and more efficient to manage. As an example, the on the host is usually not necessary due to the network and IDS systems deployed on the platform that are easier to manage at an enterprise level than system based parameters. This type of configuration can be detrimental for application systems within the same subnet without complex configuration across the board on all systems.

While the hardening guidance could implement these requirements if based solely on system security as the only line of defense, it is considered outside the scope of common usage when the system is on the core network. It is impractical for operational management to consider this level of control of the host network configuration during the initial deployment of DHS configuration guidance and must be closely tailored to the servicing applications of the platform.

As noted above, we maintain even in the presence of strong network security controls, operating system and DBMS controls are still necessary to provide sufficient security for mission critical DHS systems, particularly against insider attacks.

	EP&R NEMIS	USCIS Central Index System	Coast Guard MISLE	Secret Service SSWeb
Number of Servers Tested	8	1[(a)]	7	2
Passwords and Access Rights				
Number of Weaknesses Identified	49	0	33	17
Number of Weaknesses Addressed	**27 (55%)**	N/A	**33 (100%)**	**17 (100%)**
Configuration Management				
Number of Weaknesses Identified	38	0	21	19
Number of Weaknesses Addressed	**6 (16%)**	N/A	**20 (95%)**	**19 (100%)**
[redacted]				
Number of Weaknesses Identified	2	0	17	2
Number of Weaknesses Addressed	**2 (100%)**	N/A	**9 (53%)**	**2 (100%)**
[redacted]				
Number of Weaknesses Identified	14	0	3	3
Number of Weaknesses Addressed	**12 (86%)**	N/A	**3 (100%)**	**2 (67%)**
Total				
Number of Weaknesses Identified	103	0	74	41
Number of Weaknesses Addressed	**47 (46%)**	N/A	**65 (88%)**	**40 (98%)**

[(a)] The Central Index System resides on a mainframe computer.

Source: Based on the results of technical testing and interviews with component officials.

Evaluation of DHS' DBMS Configuration Guide

The *Federal Information Security Management Act of 2002* requires federal agencies to establish minimum acceptable configuration requirements for the information systems that support the operations and assets of the agency. On November 22, 2004, DHS issued secure baseline configuration guidelines for seven commonly used software applications: -- ---------- ---------- - ---------- ------ ---------- ---------- ---

To evaluate the adequacy of the DHS ---------- *Database Management System Secure Baseline Configuration Guide*,[15] we compared the DHS guide to configuration guidelines issued by NIST/DISA[16] and NSA/CIS.[17] Based on our review, as well as input from DHS Management, we identified the following three categories of configuration requirements:

- Core: Those security requirements necessary for all implementations of --------- DBMS, whether on a standalone system or a system connected to the DHS network.
- Networked Systems: Additional security requirements applicable to all ---- ----- DBMS implementations on systems connected to the DHS network.
- Best Practices: Security best practices that should be applied where possible.

As illustrated in Tables 3-5 below, there are a number of areas covered by the other configuration guides that DHS' guide does not address.

[15] The --------- guide was selected for review because it is the only DBMS configuration guideline DHS has issued.
[16] The DISA configuration guidelines are identified on the NIST security best practices website.
[17] ---------- -------- ---- - --------- ---------- ------ - --------- ---- --------- ---------- ----------

Table 3: Core Requirements

SETTINGS ADDRESSED IN GUIDE	DHS	NIST/DISA	NSA/CIS
_----------	No	Yes	Yes
Access Permissions to Stored Passwords/Keys	No	Yes	Yes
--------- -------- --- ----- - ----	No	Yes	Yes
Application Software Ownership	No	Yes	Yes
Application Users Assigned Least Privileges	Yes	Yes	Yes
Audit Data Retention	No	Yes	No
Audit Data Review	No	Yes	Yes
Audit Table Ownership	No	Yes	Yes
Audit Table Permissions	No	Yes	Yes
---------- ---------- -	No	Yes	Yes
---------- ----- - ---------- ---------- --	No	Yes	Yes
Auditing of Commands	No	Yes	Yes
---------- ----- ----------	No	Yes	Yes
---------- ---------- ------- - ----------	No	Yes	Yes
Changes to Database Objects	No	Yes	Yes
---------- ------- --- ---- ---	No	Yes	Yes
COTS Software Modification	No	Yes	Yes
---------- ----------	Yes	Yes	Yes
---------- ---------- -- - ---------	No	Yes	Yes
---------- ---------- -	No	Yes	No
Database Passwords Stored in Unencrypted Format	No	Yes	Yes
DBA Includes Non-default Account	No	Yes	Yes
Default Accounts and Passwords	Partially	Yes	Partially
---------- ----------	Partially	Yes	Yes
---------- ---- - ---	No	Yes	Yes
Display of Unencrypted Password	No	Yes	Yes
Encrypted Remote Administration Connections	No	Yes	Yes
--- - ----- ------- - - --- --------- ---------	No	No	Yes
Failed Login Attempts ---------- -----	No	Yes	Yes
---------- - --- ---------- --------- --- ---	No	Yes	Yes
--- -- --------- ------ ---------	Yes	Yes	Yes
---------- ----------	No	No	Yes
---------- ---	No	Yes	Yes
---------- ---------- - ----	No	Partially	Yes
---------- ------- ---------- ----	No	No	Yes
---------- - ----------	No	No	Yes
---------- - ----------	No	No	Yes
--------- ----------	No	No	Yes
---------- ----------	No	No	Yes
----------	No	Yes	No

SETTINGS ADDRESSED IN GUIDE	DHS	NIST/DISA	NSA/CIS
----------	No	Yes	Yes
----------	No	Yes	Yes
----------	No	Yes	Yes
----------	No	Yes	Yes
----------	No	Yes	Yes
----------	No	Yes	Yes
----------	No	Yes	Yes
Password File Protection	No	Yes	Yes
----------	No	Yes	No
----------	Yes	Yes	Yes
Regularly purge the audit trail	No	No	Yes
----------	Partially	Yes	Yes
----------	Partially	Yes	Yes
----------	Yes	Yes	Yes
----------	No	No	Yes
----------	No	Yes	Yes
----------	No	Yes	Yes
Temporary Passwords for New Accounts	No	Yes	No
The Production System is Protected from Software Development	No	Yes	Yes
Third party default passwords	No	No	Yes
----------	No	No	Yes
----------	No	No	Yes
----------	No	No	Yes
----------	No	No	Yes
Unauthorized Application Software Access	No	Yes	Yes
Unauthorized Object Owner	No	Yes	Yes
Unused Database Components and Database Applications	No	Yes	Yes
----------	No	Yes	Yes
----------	No	Yes	Yes
Verify permissions of all associated application files	No	No	Yes
----------	No	No	Yes
----------	No	No	Yes
----------	No	No	Yes
----------	No	No	Yes
----------	No	No	Yes
----------	No	No	Yes
----------	No	No	Yes
----------	No	No	Yes
Total Number of Areas Partially or Fully Addressed	**9**	**55**	**73**

Table 4: Requirements for Systems Connected to the DHS Network

SETTINGS ADDRESSED IN GUIDE	DHS	NIST/DISA	NSA/CIS
Access to System Tables/DBA Views	No	Yes	Yes
Account Permissions	No	Yes	Yes
----------	No	Yes	Yes
----------	No	No	Yes
Change standard ports	No	No	Yes
Check Network IP Addresses	Yes	Partially	Yes
Configuration Management Policy for Database Software	No	Yes	No
----------	No	No	Yes
----------	No	No	Yes
Data Dictionary Accessibility	Yes	Yes	Yes
----------	No	Yes	Yes
----------	No	Yes	Yes
----------	No	Yes	Yes
----------	No	Yes	Yes
Database Software Baseline	No	Yes	Yes
Database Source Code Object Encryption/Encoding	No	Yes	Yes
----------	No	Yes	No
DDL Statements Used in Database Applications	No	Yes	Yes
----------	No	Yes	Yes
Developer Privileges on Shared Systems	No	Yes	Yes
----------	No	No	Yes
----------	No	No	Yes
----------	No	No	Yes
----------	No	Yes	Yes
----------	No	Yes	Yes
Individual Database User Accounts	No	Yes	No
----------	No	Yes	No
Limit the number of operating system users	Yes	No	Yes
----------	No	No	Yes
----------	No	Yes	No
----------	No	Yes	Yes
----------	No	Yes	Yes
----------	No	Yes	Yes
----------	No	Yes	Yes
----------	No	Yes	Yes
----------	No	Yes	Yes
----------	No	Yes	Yes
Password Life Time (---------- ----------	No	Yes	Yes

Table 4: Requirements for Systems Connected to the DHS Network (continued)

SETTINGS ADDRESSED IN GUIDE	DHS	NIST/DISA	NSA/CIS
Password Reuse ---------- ----------	No	Yes	Yes
---------- - ---------- ---------- -------	No	Yes	Yes
---------- - -------	No	No	Yes
---------- - ---------- --	No	Yes	Yes
---------- ----- ---------- -----	No	Yes	Yes
----------	No	Yes	No
---------- ------- ---------- --- - ---	No	Yes	No
------- --- ---------- ---------- - ----- -- ----	Yes	No	No
---------- - ---- --------- -	No	Yes	Yes
--- -------- ------ ---------- -- ---- ---	No	No	Yes
Shared/N-Tier Connection/Non-Interactive Database Accounts	No	Yes	No
----------	No	Yes	No
- ---------- -- -- ---	No	Yes	Yes
----- -- ----- ------ --	No	Yes	Yes
---------- - --- - ---------- -- - ----------	Yes	Yes	Yes
---------- - ----------	No	Yes	Yes
---------- ---------- -------	No	Yes	No
Total Number of Areas Partially or Fully Addressed	**5**	**42**	**43**

Table 5: Security Best Practices

SETTINGS ADDRESSED IN GUIDE	DHS	NIST/DISA	NSA/CIS
Account Lock Time	No	Yes	Yes
Ad-hoc queries on production databases	No	No	Yes
-------- ---------- ---------- ----------	No	Yes	Yes
Audit data Location	No	Yes	Yes
---------- ------ -----	No	Yes	Yes
---------- ----------	No	No	Yes
---------- ---------- ----------	No	Yes	Yes
----------	No	No	Partially
---- ------ -- ---------- -- --- --	No	Yes	Yes
---------- --- ----------	No	No	Yes
---------- --------- ------	No	No	Yes
---------- ----------	Partially	Yes	Yes
---------- -- ------ -	Partially	No	Partially
---------- -- -- ----- --	No	Yes	No
---------- ---------- -----	No	Yes	Yes
---------- --- -- ------ -	No	No	Yes
---------- ---------- ----- -	No	Yes	Yes
---------- ---------- ----------	No	No	Yes
---------- ---------- ---------- -	No	Yes	Yes
----------	No	Yes	Yes
----------	No	No	Yes
PKI Database Authentication	No	Yes	No
- - ---------- -- ---- ---------- ---	No	No	Yes
----------	No	No	Yes
----------	No	Yes	Yes
---- - -------- --- --------- ---	No	No	Yes
---------- -------- -------- ------ ----------	No	Partially	Yes
---------- ------ - -----	No	No	Yes
---------- ------ - --- -----	No	No	Yes
Use triggers to implement row level auditing	No	No	Yes
-- --------- --------	No	Yes	Yes
Total Number of Areas Partially or Fully Addressed	**2**	**16**	**29**
Overall Total (Core, Network, and Best Practices)	**16**	**113**	**145**

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.[18] 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 relative to 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 POA&Ms.[19]

Our evaluation of the DHS database systems shows that the department has not implemented certain security management practices into its information security program, as required by FISMA. Table 3 illustrates FISMA metrics for each of the components included in our audit, as implemented for the systems we reviewed. Specific information regarding each of the systems and metrics is included in the reports addressed to each of the components.[20]

[18] The E-Government Act of 2002 (Public Law 107-347), signed into law on December 17, 2002, recognized the importance of information security to the economic and national security interests of the United States.
[19] As required by: OMB M-04-04, *E-Authentication Guidance for Federal Agencies*, and NIST 800-63, *Electronic Authentication Guideline.*
[20] See OIG-05-35, *Security Weaknesses Increase Risks to Critical United States Coast Guard Database*; OIG-05-37, *Security Weaknesses Increase Risks to Critical United States Secret Service Database*; OIG-05-42, *Security Weaknesses Increase Risks to Critical United States Citizenship and Immigration Services Database*; and, OIG-05-43, *Security Weaknesses Increase Risks to Critical Emergency Preparedness and Response Database*.

Table 3: FISMA Compliance Metrics by Component

FISMA Reporting Requirements	EP&R NEMIS	USCIS Central Index System	Coast Guard MISLE	Secret Service SSWeb
Does the major application have a complete and current C&A, including a risk assessment and security plan?	Yes	Yes	Yes	Yes
Has the major application's impact level been determined according to Federal Information Processing Standard 199 criteria?	Yes	Yes	Yes	Yes
Does the major application have a complete and current NIST SP 800-26 annual assessment?	Yes	Yes	Yes	Yes
Does the assessment indicate that security controls have been tested and evaluated in the last year?	**No**	**No**	**No**	Yes
Does the assessment indicate that a contingency plan has been established and tested?	**No**	**No**	**No**	**No**
Have security control costs been integrated into the life cycle of the system?	**No**	Yes	**No**	**No**
Has an assessment of E-authentication risk been performed for the major application?	Yes	Not Applicable	Not Applicable	Not Applicable
Have the system and database administrators obtained specialized security training?	**No**	**No**	**No**	**No**
Does the major application have any existing POA&Ms?	Yes	Yes	**No**	Yes

Source: OIG table based on interviews with DHS 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
Charles Twitty, Referencer

Advanced Technology Division
Jim Lantzy, Director
Michael Goodman, Security Engineer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
Executive Secretary
General Counsel
Chief Information Officer
Chief Information Security Officer
Under Secretary, Management
Assistant Secretary, Public Affairs
Assistant Secretary, Legislative Affairs
Assistant Secretary, Policy
Director, Departmental GAO/OIG Liaison Office
Director, Compliance and Oversight Program
Chief Information Officer Audit Liaison

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.