

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Security Weaknesses Increase Risks to Critical United States Coast Guard 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-05-35

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

This report assesses the strengths and weaknesses of database security controls over United States Coast Guard (Coast Guard) resources. It is based on interviews with Coast Guard 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 black ink 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..... | 8 |
| Management Comments and OIG Analysis | 8 |
| MISLE Servers Are Vulnerable..... | 10 |
| Recommendations..... | 19 |
| Management Comments and OIG Analysis | 19 |

Appendices

| | |
|---|----|
| Appendix A: Purpose, Scope, and Methodology | 21 |
| Appendix B: Management’s Response..... | 23 |
| Appendix C: Vulnerabilities Identified and Addressed..... | 27 |
| Appendix D: FISMA Metrics..... | 28 |
| Appendix E: MISLE Architecture | 30 |
| 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 |
| DISA | Defense Information Systems Agency |

Table of Contents/Abbreviations

| | |
|-------------|---|
| Coast Guard | United States Coast Guard |
| FISMA | Federal Information Security Management Act of 2002 |
| ID | Identifier |
| ISS | Internet Security Systems |
| IT | Information Technology |
| MISLE | Marine Information for Safety and Law Enforcement |
| NIST | National Institute of Standards and Technology |
| <hr/> | |
| OIG | Office of Inspector General |
| OMB | Office of Management and Budget |
| OSC | Operations Systems Center |
| POA&M | Plan of Action and Milestones |
| SP | Special Publication |
| <hr/> | |

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 reviews of access controls, continuity of operations, and change management policies and procedures. This report assesses the strengths and weaknesses of security controls over United States Coast Guard (Coast Guard) database resources.

Our objective was to determine whether the Coast Guard had implemented adequate and effective controls over sensitive data contained in its Marine Information for Safety and Law Enforcement (MISLE) system. We interviewed Coast Guard officials; reviewed database security documents; and, performed technical tests of one [REDACTED] database server, one [REDACTED] database server, three application and authentication servers, and two domain controllers.

The Coast Guard has not established adequate or effective database security controls for MISLE. The Coast Guard has developed and implemented many essential security controls for the MISLE system, including a process to control routine changes to the system and a process to maintain and review an audit trail of operating system level security events.² However, additional work remains to implement the access controls and continuity of operations safeguards

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

² 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.

necessary to protect sensitive MISLE data effectively. Specifically, the Coast Guard has not 1) implemented effective procedures for granting, monitoring, and removing user access; 2) maintained and reviewed adequate [REDACTED]; or 3) developed and tested an adequate Information Technology (IT) contingency plan. In addition, vulnerabilities existed on MISLE servers related to access rights and password administration, configuration management, [REDACTED], and encryption. Due to these database security exposures, there is an increased risk that unauthorized individuals could gain access to critical Coast Guard database resources and compromise the confidentiality, integrity, and availability of sensitive MISLE data. In addition, the Coast Guard may not be able to recover MISLE following a disaster.

Subsequent to the completion of our audit work, officials from the Coast Guard stated that they had taken or planned to take corrective action to address 65 of the 74 vulnerabilities identified during our technical testing. The Coast Guard did not provide a corrective action plan for the remaining nine vulnerabilities. As our fieldwork was complete, we did not verify that the vulnerabilities had been remedied. See Appendix C for an overview of the vulnerabilities we identified.

We recommend that the Chief Information Officer (CIO):

- Ensure that adequate controls for granting, monitoring, and removing user access to MISLE are implemented.
- Maintain and review MISLE [REDACTED].
- Develop an IT contingency plan for MISLE.
- Implement corrective action plans to address all identified MISLE vulnerabilities and configuration weaknesses.
- Examine methods to expedite the implementation of [REDACTED].
- Ensure that corrective actions for the above recommendations are applied to all Coast Guard database systems.

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 the Coast Guard's information security program and practices as implemented for MISLE.³ The Coast Guard

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

has not yet fully aligned its security program with DHS' overall policies, procedures, or practices. For example: 1) security controls have not been tested and evaluated in the last year; 2) a contingency plan has not been established and tested; 3) security control costs have not been integrated into the life cycle of the system; 4) system and database administrators have not obtained specialized security training; and, 5) MISLE does not have any existing plan of action and milestones (POA&M). Appendix D summarizes the results of our FISMA evaluation.

Fieldwork was conducted from January through February 2005 at the Coast Guard headquarters in Washington, DC; the Coast Guard Operations Systems Center (OSC) facility in Martinsburg, WV; 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 Coast Guard Chief of Staff concurred with our recommendations and is in the process of implementing corrective measures. In addition, POA&Ms will be created and tracked for the vulnerabilities we identified. The Coast Guard'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

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.

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 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.

MISLE is a web-based, mission critical database system that is used to track marine safety and law-enforcement activities involving commercial and recreational vessels. The system provides ad hoc query, reporting, and file downloading capabilities to the Coast Guard Marine Safety and Law Enforcement operating programs. 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. Certain vessel data in the Vessel Documentation System is also accessible to personnel accessing the Marine Safety Network.

MISLE utilizes a multi-tiered architecture based on database servers, web and application servers, and individual user workstations. The Marine Safety Network utilizes [REDACTED], and [REDACTED], while the Vessel Documentation System employs [REDACTED]. According to a Coast Guard official, the Marine Safety Network provides approximately 90 percent of the MISLE system's functionality. There are approximately [REDACTED] registered Marine Safety Network users and [REDACTED] registered Vessel Documentation System users.

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

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

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

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

User Administration Procedures Are Incomplete

The Coast Guard has implemented a process for granting, monitoring, and removing MISLE user access that includes controls to protect access to the system and its data. For example, the Coast Guard has established a process to control emergency and temporary access for privileged MISLE users. However, additional work remains to implement the access control procedures

needed to limit system access to appropriate personnel adequately and effectively. Specifically:

- The Coast Guard has not established sufficient controls over account creation for Marine Safety Network users. [REDACTED]
[REDACTED]
[REDACTED]. Further, there is no process to document Marine Safety Network user access authorizations, and there is [REDACTED]. MISLE officials stated that the implementation of [REDACTED] was pending the completion of an upcoming system upgrade. The Coast Guard plans to complete the upgrade by December 2005.
- The Coast Guard has not implemented procedures to ensure that regular reviews of all accounts with access to MISLE are performed. Periodic revalidations ensure that access granted to users remain appropriate. According to Coast Guard officials, the capability to perform periodic revalidations exists, but they were not aware of a policy requiring that such reviews be performed.
- The Coast Guard has not conducted annual security training or completed rules of behavior documents for Vessel Documentation System users, including several with privileged access to the MISLE system. According to MISLE officials, informal security training is provided to new Vessel Documentation System users. Users are orally briefed on their security responsibilities during orientation. However, there is no annual refresher training, and completion of the initial security training is not documented.

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:

- A user's supervisor or project manager determines the systems the user needs to access as well as the levels of access the user needs to do his or

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

her job, and that the program official or designated representative approve user access privileges.

- System managers or owners revalidate all accounts at least annually.
- DHS personnel and contractors accessing DHS IT systems receive initial and annual training in security awareness, and sign rules of behavior documents.

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

MISLE Auditing Is Inadequate

The Coast Guard does not [REDACTED] for MISLE. The Coast Guard maintains audit logs of pertinent information related to [REDACTED]. These audit logs are reviewed on a daily basis using [REDACTED]. Further, a historical record of audit trail information has been maintained since the implementation of the system. [REDACTED]

[REDACTED] According to MISLE officials, [REDACTED] because they were not aware of any requirement for [REDACTED].

According to DHS Policy, audit trails must contain sufficient information to facilitate the reconstruction of events if compromise or malfunction occurs or is suspected. Audit trails help ensure individual accountability by providing the ability to track a user's activities while accessing an automated system.

[REDACTED]. As a result of the lack of [REDACTED], inappropriate access to sensitive data or malicious changes to MISLE [REDACTED].

An IT Contingency Plan Has Not Been Developed and Tested

The Coast Guard has created an IT contingency plan for MISLE, but the plan does not contain all of the information necessary to ensure that the system can be recovered. For example, the current MISLE IT contingency plan [REDACTED]

Coast Guard officials stated that they are aware of the deficiencies in the current MISLE IT contingency plan, and that they are in the process of developing comprehensive IT contingency plans for all major applications housed at the OSC. However, the development and testing of the updated MISLE IT contingency plan is pending completion of the new Coast Guard disaster recovery site [REDACTED]

According to the Coast Guard, the disclosure, inaccuracy, or non-availability of sensitive information processed and stored by MISLE could have a significant impact on the component's ability to complete its mission. Consequently, it is critical that the system be able to operate effectively without excessive interruption. Contingency planning supports this requirement by establishing thorough plans, procedures, and technical measures that can enable a system to be recovered quickly and effectively following a service outage or disaster. IT contingency plan testing enables deficiencies to be identified and addressed, and helps evaluate the ability of the recovery staff to implement the plan quickly and effectively. As a result of the lack of adequate contingency planning and testing for the system, there is greater risk that MISLE officials may not be able to restore the system in a timely manner following a disaster.

Recommendations

To protect sensitive MISLE data, we recommend that the Coast Guard Commandant direct the CIO to:

1. Ensure that adequate controls for granting, monitoring, and removing MISLE user access are implemented according to DHS requirements and NIST guidelines.
2. [REDACTED]
3. Develop and implement a MISLE IT contingency plan and ensure that an annual test of the plan is conducted.

Management Comments and OIG Analysis

The Coast Guard concurs with recommendation 1. The Coast Guard plans to verify user access via the Coast Guard's [REDACTED] environment. The Coast Guard will require that [REDACTED] before access is granted to the system. These changes will adhere to DHS requirements. In addition, by 4th Quarter FY 2006, the Coast Guard will comply with NIST guidelines for access control, auditing, and user authentication.

We accept the Coast Guard's response to align its controls for granting, monitoring, and removing user access with DHS requirements and NIST guidelines.

The Coast Guard concurs with recommendation 2. The Coast Guard plans to implement [REDACTED] in accordance with DHS requirements. However, because DHS has not issued guidelines for [REDACTED], configuration settings will be reviewed in accordance with the Defense Information Systems Agency (DISA) Database Secure Technical Implementation Guide. These changes will be in place by 2nd Quarter FY 2006.

We accept the Coast Guard's response to implement [REDACTED], as well as additional [REDACTED] in accordance with DISA guidelines.

The Coast Guard concurs with recommendation 3. The Coast Guard has a new, NIST compliant contingency plan under draft, which will be tested and reported in MISLE's FISMA TAF tool. The MISLE disaster recovery site is scheduled to be in place by September 2005.

We accept the Coast Guard's plan of action to develop and test a NIST compliant contingency plan. However, the Coast Guard did not indicate that an annual test of the plan would be completed. We maintain that the Coast Guard should have a process to ensure that an annual test of the contingency plan is conducted.

MISLE Servers Are Vulnerable

The Coast Guard has not established effective database security controls for MISLE. To assess the security of MISLE databases, we performed vulnerability assessment scans to identify configuration weaknesses on MISLE servers; and, conducted manual checks of the security settings on a central MISLE database server to identify additional configuration weaknesses and verify the results of the vulnerability assessment scans. In assessing the effectiveness of database controls, we identified issues related to access rights and password administration, configuration management, [REDACTED] and encryption. These control weaknesses could enable an attacker to gain inappropriate access to MISLE and its data.

Access Privileges Were Not Appropriately Restricted

The Coast Guard did not enforce strong identification or authentication measures for MISLE. Six of the seven servers we tested did not appropriately restrict access to the system. For example:

- [REDACTED]
- [REDACTED]
- [REDACTED]

[REDACTED]

[Redacted]

Several of the access rights and password vulnerabilities we identified are the result of default operating system and DBMS settings that were not changed at the time the software was installed. [Redacted]. Unless this default setting is changed [Redacted].

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

[Redacted]

Table 1: Access Rights and Password Vulnerabilities Identified and Addressed

| Server | Number of Vulnerabilities Identified | | | Number That Have Been Addressed | | |
|------------|--------------------------------------|-------------|-------|---------------------------------|--------------|--------------|
| | High Risk | Medium Risk | Total | Corrected | Planned | Total |
| [REDACTED] | 0 | 5 | 5 | 0 | 5 (100%) | 5 (100%) |
| [REDACTED] | 0 | 0 | 0 | N/A | N/A | N/A |
| [REDACTED] | 3 | 8 | 11 | 0 | 11 (100%) | 11 (100%) |
| [REDACTED] | 0 | 3 | 3 | 0 | 3 (100%) | 3 (100%) |
| [REDACTED] | 1 | 0 | 1 | 0 | 1 (100%) | 1 (100%) |
| [REDACTED] | 2 | 5 | 7 | 7 (100%) | 0 | 7 (100%) |
| [REDACTED] | 1 | 5 | 6 | 6 (100%) | 0 | 6 (100%) |
| Total | 7 | 26 | 33 | 13 (39%) | 20 (61%) | 33 (100%) |

(a) Manual security parameter tests were only conducted on the Marine Safety Network database server.

Source: OIG table based on the results of technical testing and interviews with Coast Guard 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. The DHS Handbook also forbids [REDACTED]. Further, NIST and the National Security Agency provide specific guidelines related to certain operating system and database security settings, including [REDACTED].

Often, passwords are the first line of defense against hackers or insiders who may try to obtain unauthorized access to a computer system. The use of weak password controls, combined with inappropriate access rights, might allow unauthorized internal users or external hackers to gain access to Coast Guard networks and systems.

MISLE Servers Are Not Configured Appropriately

The Coast Guard did not configure network services and security parameters to protect MISLE data and files. For example:

- [Redacted]
- [Redacted]

Table 2 illustrates the number of configuration management vulnerabilities that we identified for the MISLE database servers and related hosts, along with the corrective actions that the Coast Guard 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 | 4 | 5 | 0 | 4 (80%) | 4 (80%) | 1 (20%) |
| [REDACTED] | 0 | 1 | 1 | 0 | 1 (100%) | 1 (100%) | 0 |
| [REDACTED] | 0 | 1 | 1 | 0 | 1 (100%) | 1 (100%) | 0 |
| [REDACTED] | 0 | 2 | 2 | 0 | 2 (100%) | 2 (100%) | 0 |
| [REDACTED] | 0 | 2 | 2 | 0 | 2 (100%) | 2 (100%) | 0 |
| [REDACTED] | 0 | 5 | 5 | 3 (60%) | 2 (40%) | 5 (100%) | 0 |
| [REDACTED] | 0 | 5 | 5 | 3 (60%) | 2 (40%) | 5 (100%) | 0 |
| Total | 1 | 20 | 21 | 6 (29%) | 14 (67%) | 20 (95%) | 1 (5%) |

(a) Manual security parameter tests were only conducted on the Marine Safety Network database server.

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

The configuration weaknesses noted above are largely the result of default operating system and DBMS settings that were not changed at the time the software was installed. These configuration weaknesses had not been identified or corrected by Coast Guard personnel, in part, because [REDACTED] of the MISLE system are not performed.

MISLE Has Not Been [REDACTED]

The Coast Guard has not [REDACTED]. We examined each of the seven servers to determine if all of the [REDACTED]. Also, we reviewed the Marine Safety Network database

server to determine if all of the appropriate [REDACTED]. Although the Coast Guard had [REDACTED], the component has [REDACTED], including those running [REDACTED].

Some [REDACTED] because Coast Guard officials did not believe [REDACTED] were needed for the MISLE operating environment. However, according to the vendor of the operating system software, [REDACTED] are relevant to the software version running on the MISLE servers. The vendor has indicated that [REDACTED]. In addition, some of [REDACTED] because the systems administrators had previously attempted [REDACTED]. However, the installation had not been successful because [REDACTED] had not been previously installed.

Table 3 illustrates the number of [REDACTED] that we identified for the MISLE database servers and related hosts, along with the corrective actions that the Coast Guard has planned or already taken to address these weaknesses.

Table 3: [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 | 0 | 1 | 0 | 1 (100%) | 1 (100%) | 0 |
| [REDACTED] | 0 | 0 | 0 | N/A | N/A | N/A | N/A |
| [REDACTED] | 0 | 0 | 0 | N/A | N/A | N/A | N/A |
| [REDACTED] | 0 | 0 | 0 | N/A | N/A | N/A | N/A |
| [REDACTED] | 0 | 0 | 0 | N/A | N/A | N/A | N/A |
| [REDACTED] | 5 | 3 | 8 | 4 (50%) | 0 | 4 (50%) | 4 (50%) |
| [REDACTED] | 5 | 3 | 8 | 4 (50%) | 0 | 4 (50%) | 4 (50%) |
| Total | 11 | 6 | 17 | 8 (47%) | 1 (6%) | 9 (53%) | 8 (47%) |

(a) Manual security parameter tests were only conducted on the Marine Safety Network database server.

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

DHS Policy requires that IT security [REDACTED] in accordance with configuration management plans or direction from higher authorities. According to [REDACTED] [REDACTED] is critical to the operational availability, confidentiality, and integrity of information technology systems. NIST recommends that organizations have an explicit and documented [REDACTED] policy as well as a systematic, accountable, and documented process for [REDACTED].

Because Coast Guard officials [REDACTED], the system was [REDACTED]. [REDACTED]

MISLE Data and Files Were Not Encrypted

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

- [REDACTED]
- [REDACTED]

Coast Guard officials stated that they are examining the implementation of [REDACTED]. However, the implementation of [REDACTED] is still in the planning stage because it will require extensive system changes. MISLE officials anticipate that it will take two years to implement these changes.

Table 4 illustrates the number of encryption vulnerabilities that we identified for the MISLE database servers and related hosts, along with the corrective actions that the Coast Guard has planned or already taken to address these weaknesses.

[REDACTED]

Table 4: Encryption Vulnerabilities Identified and Addressed

| Server | Number of Vulnerabilities Identified | | | Number That Have Been Addressed | | |
|------------|--------------------------------------|-------------|-------|---------------------------------|-------------|-------------|
| | High Risk | Medium Risk | Total | Corrected | Planned | Total |
| [REDACTED] | 0 | 1 | 1 | 0 | 1 (100%) | 1 (100%) |
| [REDACTED] | 0 | 0 | 0 | N/A | N/A | N/A |
| [REDACTED] | 1 | 1 | 2 | 0 | 2 (100%) | 2 (100%) |
| [REDACTED] | 0 | 0 | 0 | N/A | N/A | N/A |
| [REDACTED] | 0 | 0 | 0 | N/A | N/A | N/A |
| [REDACTED] | 0 | 0 | 0 | N/A | N/A | N/A |
| [REDACTED] | 0 | 0 | 0 | N/A | N/A | N/A |
| Total | 1 | 2 | 3 | 0 | 3 (100%) | 3 (100%) |

(a) Manual security parameter tests were only conducted on the Marine Safety Network database server.

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

According to the DHS Handbook, encryption is 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 encryption plans for their sensitive IT systems. NIST recommends that cryptographic tools be implemented to protect the integrity and confidentiality of critical data and software programs [REDACTED]

[REDACTED]

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

Recommendations

To protect sensitive MISLE data, we recommend that the Coast Guard Commandant direct the CIO to:

4. Develop and implement corrective action plans to address all identified MISLE vulnerabilities and configuration weaknesses to reduce the risk of system compromise or failure.
5. Examine methods to expedite the implementation of [REDACTED] [REDACTED] to ensure that sensitive data is adequately protected.
6. Ensure that corrective actions for the above recommendations are applied to all Coast Guard database systems.

Management Comments and OIG Analysis

The Coast Guard generally concurs with recommendation 4. The Coast Guard will develop and implement corrective action plans for the MISLE vulnerabilities we identified. However, the Coast Guard disagreed with the severity categorizations of three of the findings identified during our review. Specifically, Coast Guard officials stated that, due to the presence of mitigating controls, three findings categorized as medium risk only pose a low risk to MISLE operations. Nonetheless, the Coast Guard plans to take action to address these weaknesses.

We accept the Coast Guard's plan to develop and implement corrective action plans for all of the identified MISLE vulnerabilities.

The Coast Guard concurs with recommendation 5. The MISLE team will examine ways to expedite the implementation of [REDACTED]

[REDACTED]

We agree that the action the Coast Guard plans to take satisfies the intent of the recommendation.

The Coast Guard concurs with recommendation 6. The Coast Guard indicated that lessons and best practices learned from the MISLE audit would be considered for all major application with a comparable FIPS 199 sensitivity level as they are scheduled for C&A.

We agree that the action the Coast Guard plans to take satisfies the intent of the recommendation.

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 the Coast Guard'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 MISLE for inclusion in our review.

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

- 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 Marine Safety Network database server to confirm the results of our scans and identify any additional security weaknesses. Upon completion of the tests, we provided the Coast Guard with technical reports detailing the specific

vulnerabilities detected on the MISLE system and the actions needed for remediation.

We conducted fieldwork at the Coast Guard headquarters in Washington, DC; the Coast Guard OSC facility in Martinsburg, WV; and, the OIG's ATL. We conducted our audit between January and February 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
United States
Coast Guard




Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: CG-823
Phone: (202) 267-2294
Fax: (202) 267-4850
Email: mark.kulwicki@uscg.dhs.gov

7501

MEMORANDUM

15 AUG 2005

From: 
T.W. Allen, VADM
Chief of Staff, U.S. Coast Guard

Reply to: CG-823
Attn of: Mark Kulwicki
202-267-2294

To: Assistant Inspector General for Information Technology
Subj: Security Weaknesses Increase Risks to Critical United States Database
Ref: (a) Draft Report dated June 28, 2005

1. This letter transmits our comments to the Department of Homeland Security Inspector General draft report findings and recommendations contained in reference (a).
2. We have reviewed the draft report and generally concur with the findings and recommendations. We have provided some technical comments and clarifications for your consideration.
3. The Coast Guard also requests that none of the subject report get posted to the DHSIG internet site. The entire report is classified For Official Use Only (FOUO) and contains security related vulnerabilities that others can use to compromise Sensitive But Unclassified (SBU) information contained in the MISLE system.
4. The Coast Guard appreciates the opportunity to comment on this report and will continue its work to improve the security of its databases. If you have any questions, please contact Mark Kulwicki at (202)-267-2294.

#

Enclosure: U.S. Coast Guard Comments on Draft Report

**UNITED STATES COAST GUARD
STATEMENT ON INSPECTOR GENERAL REPORT**

TITLE: "Security Weaknesses Increase Risks to Critical United States Coast Guard Database" (Draft Report dated June 28, 2005)

The Coast Guard concurs with the principal findings included in this report and appreciates the efforts of DHS IG in documenting areas for improvement in the MISLE database. All validated vulnerabilities will be entered into the system Plan of Action and Milestones (POA&M) and recorded and tracked in the Federal Information Security Management Act (FISMA) Test Automation Framework (TAF) tool, along with the official results of the full system Security Test and Evaluation (ST&E) scheduled to begin in January 2006. The Coast Guard also agrees with the high-level recommended actions and is in the process of implementing corrective measures. The following comments are provided in response to the findings of the report.

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

Concur. The current MISLE account validation and monitoring process was put in place out of necessity to facilitate the time-critical establishment of over 5000 accounts during MISLE start-up in a post 9-11 (December 2001) operations tempo. [REDACTED]

[REDACTED]

[REDACTED] which provides an opportunity to correct shortcomings in this area. Planned improvements include: verifying the unit to which a user is assigned [REDACTED]

These changes will bring MISLE into alignment with DHS requirements. The National Institute of Standards and Technology (NIST) guidelines for access control, auditing, and user authentication have been updated as recently as April 2005. The new NIST guidelines will be thoroughly reviewed to ensure appropriate changes are made to meet compliance. These changes will be in place by Quarter 4, FY 2006.

Recommendation: [REDACTED]

Concur. MISLE has historically conducted routine structural integrity checks to document changes and compare production data structures against known good structures maintained in the code repository. MISLE is not aware of DHS guidelines defining [REDACTED]. For the reason, MISLE [REDACTED] configuration settings will be reviewed in accordance with Defense [REDACTED]

Information Systems Agency (DISA) Database Secure Technical Implementation Guide. These changes will be in place by Quarter 2, FY 2006.

Recommendation: Develop and implement an IT contingency plan and ensure that an annual test of the plan is conducted.

Concur. A new, NIST compliant contingency plan is under draft and will be tested and reported in MISLE's FISMA TAF entry. MISLE has been designated as a Gold Service Level disaster recovery (DR) system and is scheduled to be in place at the DR site by September 2005.

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

Concur with the recommendations, with the following clarifications of the findings:

1. On page 9 of the report, the Auditor reported that [REDACTED]
[REDACTED] **Clarification.** [REDACTED]
[REDACTED]
2. On page 10 of the report, the Auditor reported that [REDACTED]
[REDACTED] This data may indeed be accessed by users who can log on to the device; however this group is limited to Domain Administrators and Account operators only. Additionally, the data in [REDACTED] is only updated during the creation/update [REDACTED] An inspection of the properties on the file in question indicates the file was created the day the machine was created in 2003 and has never been modified since then. OSC rates this as a low risk.
3. On page 12 of the report, the Auditor reported that five of the seven servers tested [REDACTED]
[REDACTED] and in an internet environment is a security risk. However, MISLE is part of a screened network, the Coast Guard Data Network Plus (CGDN+) and not exposed to the internet. The Coast Guard Computer Incident Response Team (CGCIRT) and OSC regard this as a low risk. Nonetheless, the OIG-recommended [REDACTED] will be tested and implemented if feasible.

Corrective action plans will be developed and implemented for the remaining identified vulnerabilities. These items will be included in a Plan of Actions and Milestones (POA&M) that will be prepared during the certification and accreditation (C&A) scheduled for Quarter 2 FY06.



Recommendation: Examine methods to expedite the implementation of [REDACTED] [REDACTED] to ensure that sensitive data is adequately protected.

Concur. The MISLE team will examine ways to expedite the implementation of [REDACTED] [REDACTED] Options will be reviewed by Quarter 2, FY 2006.

Recommendation: Ensure that corrective actions for the above recommendations are applied to all Coast Guard database systems.

Concur. Lessons and best practices learned from this MISLE audit will be considered for all major applications with a comparable Federal Information Processing Standards (FIPS) 199 sensitivity level as they are scheduled for C&A.

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 | |
| Access Rights and Passwords | 7 | 26 | 33 | 13 (39%) | 20 (61%) | 33 (100%) | 0 |
| Configuration Management | 1 | 20 | 21 | 6 (29%) | 14 (67%) | 20 (95%) | 1 (5%) |
|  | 11 | 6 | 17 | 8 (47%) | 1 (6%) | 9 (53%) | 8 (47%) |
|  | 1 | 2 | 3 | 0 | 3 (100%) | 3 (100%) | 0 |
| Total | 20 | 54 | 74 | 27 (36%) | 38 (51%) | 65 (88%) | 9 (12%) |

Source: OIG table based on the results of technical testing and interviews with Coast Guard 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.¹⁶ 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 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 POA&Ms.¹⁷

Our evaluation of MISLE shows that the Coast Guard has not implemented certain security management practices into its information security program, as required by FISMA.

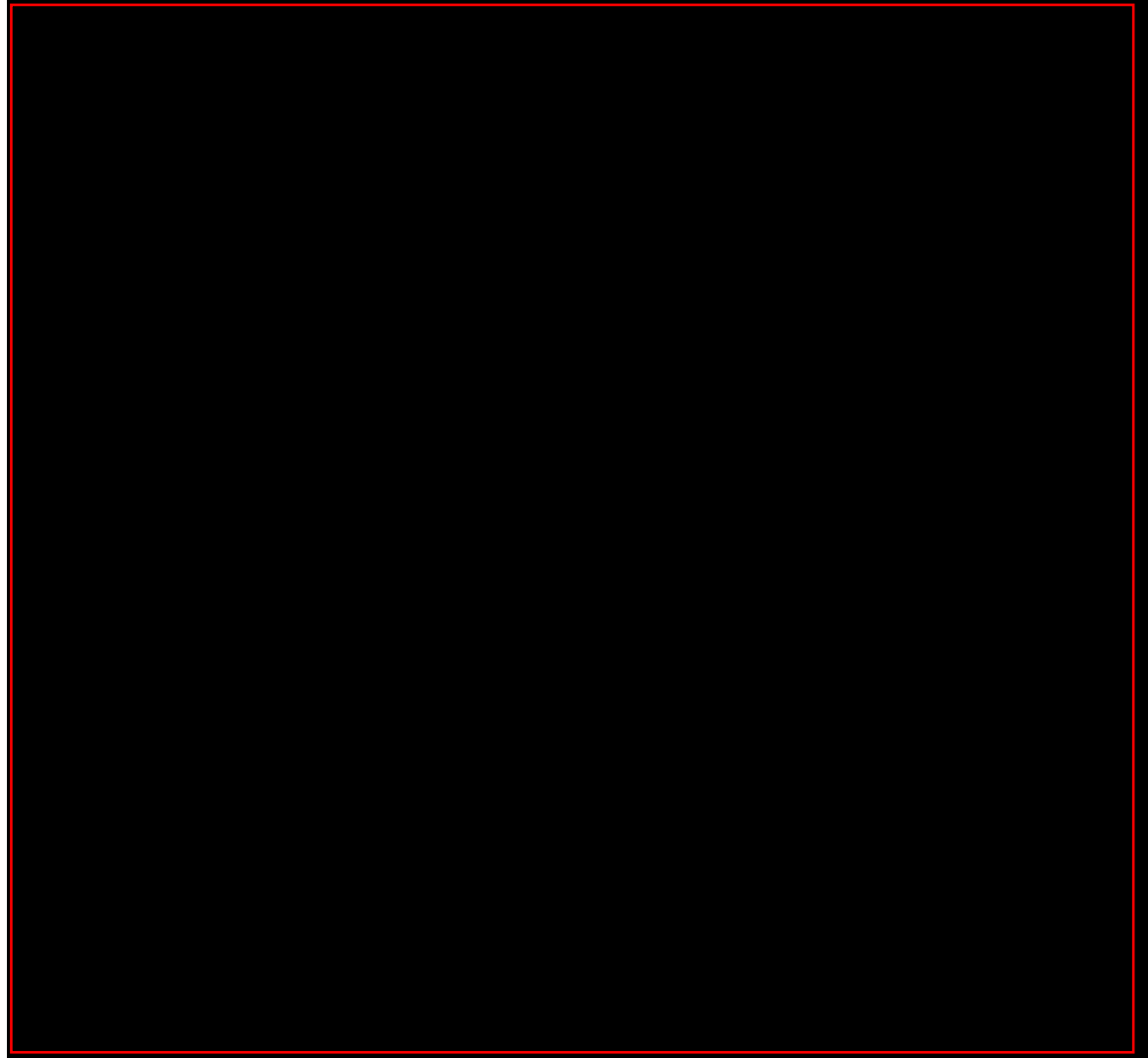
¹⁶ The E-Government Act of 2002 (Public Law 107-347), signed into law on December 17, 2002, recognized the importance of information security to the economic and national security interests of the United States.

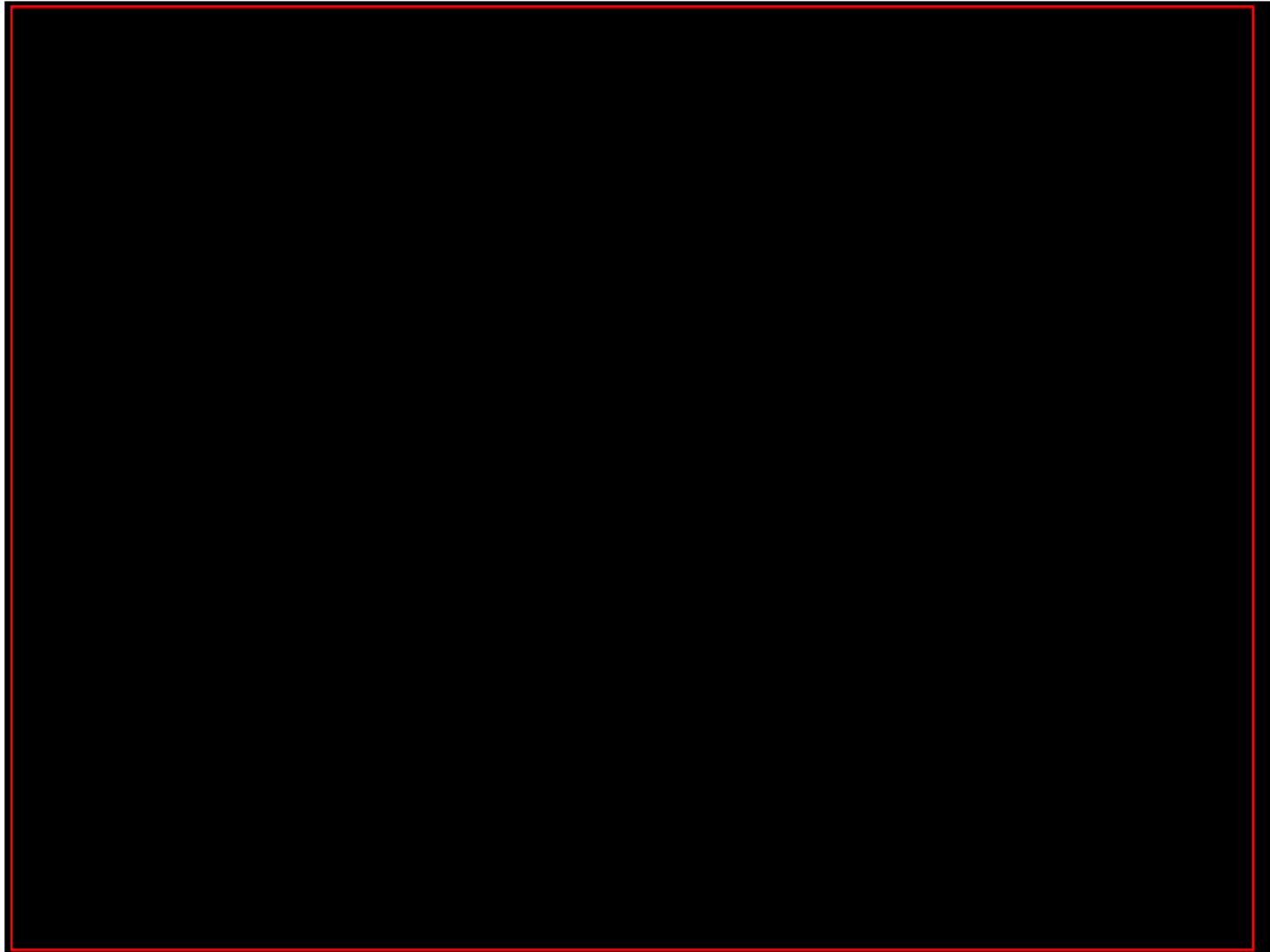
¹⁷ As required by: OMB M-04-04, *E-Authentication Guidance for Federal Agencies*, and NIST SP 800-63, *Electronic Authentication Guideline*.

Table 5: FISMA Compliance Metrics

| FISMA Reporting Requirements | Coast Guard (MISLE) | 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 MISLE would have a high impact on the Coast Guard's mission. |
| Does the major application have a complete and current NIST SP 800-26 annual assessment? | Yes | A MISLE assessment was completed on October 11, 2004. |
| Does the assessment indicate that security controls have been tested and evaluated in the last year? | No | Although vulnerability assessments are conducted quarterly, the MISLE system has not undergone a detailed configuration review in the past year. |
| Does the assessment indicate that a contingency plan has been established and tested? | No | The assessment indicated that an IT contingency plan has been established and tested. However, the MISLE contingency plan is lacking key information and has not been tested in the past year. |
| Have security control costs been integrated into the life cycle of the system? | No | Security control costs are being integrated into the life cycle for systems currently under development or undergoing certification and accreditation. |
| Has an assessment of E-Authentication risk been performed for the major application? | Not Applicable | The MISLE system is only used by Coast Guard personnel. |
| Have the system and database administrators obtained specialized security training? | No | The Coast Guard provides training opportunities to MISLE systems and database administrators, but does not provide mandatory, specialized security training for these personnel. |
| Does the major application have any existing POA&Ms? | No | At the time of our review, POA&Ms had not been entered into the Trusted-Agent FISMA application. |

Source: OIG table based on interviews with Coast Guard personnel and analysis of database documentation.





Appendix F
Major Contributors to This Report

Information Security Audits Division

Edward G. Coleman, Director

Patrick Nadon, Audit Manager

Jason Bakelar, Audit Team Leader

Chris Udoji, Auditor

Steven Staats, Referencer

Advanced Technology Division

Jim Lantzy, Director

Michael Goodman, Security Engineer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
United States Coast Guard, Commandant
Executive Secretary
General Counsel
Chief Information Officer
Chief Information Security Officer
Public Affairs
United States Coast Guard, Chief Information Officer
United States Coast Guard, 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.