

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

DHS Needs to Strengthen Controls For Remote Access to Its Systems and Data (Redacted)



Notice: The Department of Homeland Security, Office of the Inspector General, has redacted this report for public release under the Freedom of Information Act, 5 U.S.C. § 552 (b)(2).

Office of Information Technology

OIG-05-03

November 2004



**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, investigative, and special reports prepared by the OIG as part of its DHS oversight responsibility to identify and prevent fraud, waste, abuse, and mismanagement.

This report assesses the strengths and weaknesses of controls over remote access to DHS resources. It is based on interviews with employees and officials of relevant agencies and institutions, direct observations, technical scans, and a review of applicable documents.

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

A handwritten signature in black ink, appearing to read "Clark Kent Ervin".

Clark Kent Ervin
Inspector General

Contents

| | |
|---|----|
| Introduction..... | 3 |
| Results in Brief | 4 |
| Background..... | 5 |
| Findings | 6 |
| Remote Access Security Procedures Have Not Been Fully Developed And Implemented . | 6 |
| Remote Access Hosts Are Vulnerable..... | 9 |
| Miscellaneous Issue | 15 |
| Recommendations..... | 15 |
| Management Comments And Our Evaluation | 16 |

Appendices

| | | |
|-------------|---|----|
| Appendix A: | Purpose, Scope, and Methodology..... | 18 |
| Appendix B: | Management’s Response..... | 20 |
| Appendix C: | User Administration Processes | 22 |
| Appendix D: | Account Policy Settings | 23 |
| Appendix E: | Vulnerabilities Identified..... | 25 |
| Appendix F: | Major Contributors to This Report | 26 |
| Appendix G: | Report Distribution | 27 |

Abbreviations

| | |
|-----|--|
| ATL | Advanced Technology Laboratory |
| CIO | Chief Information Officer |
| CIS | Bureau of Citizenship and Immigration Services |
| DHS | Department of Homeland Security |

Contents

| | |
|----------------|---|
| DHS Handbook | DHS Sensitive Systems Handbook |
| DHS Management | DHS Management Directorate |
| EP&R | Emergency Preparedness and Response Directorate |
| FISMA | Federal Information Security Management Act of 2002 |
| FISCAM | Federal Information System Controls Audit Manual |
| GAO | Government Accountability Office |
| ICE | Bureau of Immigration and Customs Enforcement |
| ID | Identification |
| ISS | Internet Security Systems |
| ISSO | Information Systems Security Officer |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| NT | Windows New Technology (Microsoft) |
| OIG | Office of Inspector General |
| SP | Special Publication |
| TSA | Transportation Security Administration |

OIG

Department of Homeland Security Office of Inspector General

Introduction

The Office of Inspector General (OIG) audited the security program of the Department of Homeland Security (DHS) and its components¹ to control remote access to DHS networks. Insofar as remote access capabilities can significantly increase security risks to its networks, DHS must ensure strong security controls over remote access and dial-in capabilities.

Our objective was to determine whether DHS had provided system security, integrity, and control over remote access to its computer systems and data. The audit focused on wire based remote access to DHS systems and resources, including dial-in access through modems and access through the Internet.

We interviewed DHS officials, reviewed remote access policy and procedure documents, and performed technical scans of 53 remote access hosts.² Additionally, we analyzed password strength and account policy settings and performed modem discovery tests on 2,868 analog phone lines.

To perform these tests, we used three commercial, off-the-shelf products: Internet Security Systems' (ISS) Internet Scanner 7.0, @stake's L0phtCrack 5.02, and Sandstorm Enterprises' PhoneSweep 4.0. Upon completion of the tests, we provided each component with technical reports detailing the specific vulnerabilities detected on their networks and the actions needed for remediation.

Fieldwork was conducted from April through August 2004 at DHS' Office of the Chief Information Officer (CIO), five DHS components, and the OIG's Advanced Technology Laboratory (ATL).³ See Appendix A for purpose, scope, and methodology.

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

² In this report we used the term "host(s)" to refer to those servers and devices providing remote access capabilities, including Microsoft Windows New Technology (NT) and Windows 2000 domain controllers, Microsoft Exchange Servers, Cisco Systems Access Servers, and virtual private network concentrators.

³ The ATL supports DHS OIG's 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.

Results in Brief

DHS does not provide adequate or effective system security controls over remote access to its computer systems and data. While DHS has established policy governing remote access, and has developed procedures for granting, monitoring, and removing user access, these guidelines have not been fully implemented by the components because they are still developing processes or they are waiting to obtain automated tools to assist them in performing these functions. Further, DHS has not established configuration guidelines for the hosts providing remote access to its networks.

In addition, DHS components have not established effective system controls on remote access. Specifically: (1) remote access hosts do not provide strong protection against unauthorized access; (2) systems were not appropriately patched;⁴ and (3) modems that may be unauthorized were detected on DHS networks. Due to these remote access exposures, there is an increased risk that unauthorized people could gain access to DHS networks and compromise the confidentiality, integrity, and availability of sensitive information systems and resources.

Subsequent to the completion of our audit work, officials from each of the components said that they had taken or planned corrective action to address many of the vulnerabilities identified in our review. However, we did not verify that the problems had been resolved.

Our report includes three recommendations that will assist DHS in remedying the deficiencies identified. Specifically, the CIO should:

- Update the *DHS Sensitive Systems Handbook* (DHS Handbook) to include implementation procedures and configuration settings for remote access to DHS systems.
- Ensure that procedures for granting, monitoring, and removing user access are fully implemented.
- Ensure that all necessary system and application patches are applied in a timely manner.

⁴ A patch, also known as a “hotfix” or “service pack,” is a piece of software published by the manufacturer of a software application to correct errors or bugs in the software.

In response to our draft report, the DHS CIO concurred with our recommendations and stated that many of them have been incorporated into DHS' planning and are now reflected in the Department's program objectives and milestones. DHS' response is summarized and evaluated in the body of this report and included, in its entirety, as Appendix B.

Background

Within DHS remote access provides trusted computer users access to DHS networks by dialing in via modem or via the Internet. There are numerous advantages associated with the use of remote access. For example, remote access:

- Allows employees to have flexible work schedules.
- Provides teleworkers or employees on travel the ability to access the network and resources, such as email messages, files, databases, and applications.
- Permits administrators to identify and resolve network or system problems remotely.
- Increases employee productivity because of an improved work and home-life balance.
- Reduces operational overhead such as office space, infrastructure costs, and less sick leave.
- Reduces traffic congestion and commuting times.
- Provides more job opportunities and lessens the commute for disadvantaged workers.

While there are several advantages associated with providing DHS employees remote access, there are also numerous security concerns related to granting and maintaining remote access to government systems and resources. High-speed internet access technologies, such as cable modems, digital subscriber lines, satellites, and wireless devices, allow for increased transmission speed and bandwidth. These technologies make it easier for remote users to access and transfer large amounts of data, and allow users to be online for longer periods.

However, these technologies also increase the risk that unauthorized users will gain access to DHS systems and resources.

The *Federal Information Security Management Act (FISMA) of 2002*,⁵ requires each agency to develop, document, and implement an agency-wide information security program to provide security for the information and information systems that support the operation and assets of the agency. Agency policies should ensure that information security is addressed throughout the life-cycle of each agency information system and prescribe minimally acceptable system configuration requirements.

DHS Sensitive Systems Policy Publication 4300A addresses access controls, including remote access and dial-in capabilities. The policy requires that DHS components ensure that strong authentication and access controls are implemented for remote access. The department developed the DHS Handbook to provide components with specific techniques and procedures for implementing the requirements of this policy.

Findings

Remote Access Security Procedures Have Not Been Fully Developed And Implemented

DHS has not developed and implemented the security procedures necessary to control remote access to its networks adequately and effectively. While DHS has established a policy governing remote access and has developed procedures for user administration,⁶ these guidelines have not been fully implemented by the components.⁷ Further, DHS has not established implementation and configuration guidelines for the hosts providing remote access to its networks. As a result, there is greater risk that the controls implemented to protect DHS networks may not prevent unauthorized access to the department's systems and data.

⁵ Title III, E-Government Act of 2002, P.L. 107-347, December 17, 2002.

⁶ According to National Institute of Standards and Technology Special Publication 800-14, user administration incorporates: (1) user account management, including processes for requesting, establishing, issuing, and closing user accounts; tracking users and their respective access authorizations; and managing these functions; (2) audit and management reviews of user account management; and, (3) the timely modification or removal of access.

⁷ See Appendix C for a detailed description of recommended procedures for user administration, including granting, monitoring, and removing user access.

Remote Access User Administration Needs Improvement

Although DHS has developed procedures for granting, monitoring, and removing user access, these guidelines have not been implemented fully by the components. Specifically:

- [REDACTED] said that they had not implemented effective exit procedures to ensure that access is removed in a timely manner upon employee separation or transfer. DHS policy requires that components implement procedures to ensure system access is revoked for employees or contractors who either leave DHS or are reassigned to other duties. In addition, the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-14 requires that a standard set of processes be implemented governing friendly and unfriendly⁸ termination, including removal of access privileges, computer accounts, and authentication tokens.⁹ Additionally, the U.S. Government Accountability Office's (GAO) *Federal Information System Controls Audit Manual* (FISCAM) requires that exit processes ensure that security management is notified immediately of terminations and that access to the entity's resources and facilities, including passwords, is promptly removed.
- [REDACTED] had not implemented procedures to review audit trails periodically or logs of remote access activity and documenting the completion of such reviews. In addition, though officials from [REDACTED] that they conducted periodic reviews, officials from these components said that they did not document the completion of these activities. According to NIST SP 800-14, audit trails should be reviewed periodically to provide individual accountability, reconstruction of events, intrusion detection, and problem identification. Further, the

⁸ NIST SP 800-12 defines friendly termination as the removal of an employee from the organization when there is no reason to believe that the termination is other than mutually acceptable. Unfriendly termination is defined as the removal of an employee under involuntary or adverse conditions. NIST recommends that separate processes be developed for handling friendly and unfriendly terminations, including additional security controls to prevent adverse events in the cases of unfriendly terminations.

⁹ An authentication token is an object that a user possesses for the purpose of identification and authentication. Tokens can be divided into two categories: memory tokens such as bank or credit cards, which store information; and smart tokens such as Smart Cards, which contain integrated circuits.

DHS Handbook requires information systems security officers (ISSO) to review audit trails at least once per week or according to the system's security plan.

-



According to NIST SP 800-12, application managers or data owners should review each user's access level every month and sign a formal access approval list to provide a written record of authorization. In addition, FISCAM requires that system owners periodically review access authorization listings and determine whether they remain appropriate. The DHS Handbook requires that system managers or owners revalidate all accounts at least annually.

According to DHS officials, some of the user administration procedures noted above had not been implemented because the components were still developing auditing and management review processes, or waiting to obtain automated tools that would assist them in performing user administration functions.

DHS Has Not Issued Detailed Remote Access Configuration Guidance

DHS has not established detailed implementation and configuration procedures to ensure that remote access hosts provide strong protection against unauthorized access. The department plans to include detailed guidance in the DHS Handbook for the employment of remote access devices, user responsibilities, operating procedures, and other information pertaining to remote access administration. This section of the DHS Handbook has not been completed; however, DHS is still negotiating with its components to ensure that the minimum implementation requirements established in the guidelines are feasible.

FISMA requires federal agencies to develop and maintain information security policies, procedures, and control techniques to address all applicable requirements. Further, FISMA requires federal agencies to develop, document, and implement policies and procedures that ensure compliance with the minimally acceptable system configuration requirements determined by the agency.

Until effective user administration and remote access configuration procedures are established, DHS is at increased risk that remote access may not be adequately controlled and remote access devices may not be appropriately configured. As a result, the risks associated with providing remote access to DHS networks may not be adequately addressed.

Remote Access Hosts Are Vulnerable

DHS has not established effective system controls on remote access hosts. To assess the security of remote access to DHS networks, we: (1) performed vulnerability assessment scans to identify configuration weaknesses and vulnerabilities on the hosts providing remote access capabilities;¹⁰ (2) analyzed account policy settings¹¹ to verify that remote access hosts were properly configured; (3) conducted password strength analyses to determine whether the use of strong passwords was enforced; and, (4) performed modem discovery tests to locate any unauthorized modems operating on DHS networks. In assessing the effectiveness of remote access controls, we identified several problems related to remote access host configurations, system patching, and the control of modems. These control weaknesses could provide an attacker with the ability to gain inappropriate access to DHS information systems and resources.

Remote Access Hosts Were Not Appropriately Configured

Many of the hosts that we tested were not configured to protect against unauthorized access. Specifically:

- DHS components did not enforce strong identification or authentication measures according to DHS requirements, NIST guidelines, and National Security Agency (NSA) recommendations. For each network reviewed, we sampled a single remote access domain and tested for appropriate account policy parameter settings. With the exception of DHS management, each component had weak or inappropriate configuration settings:¹²

¹⁰ The tested hosts included Microsoft Windows NT and Windows 2000 domain controllers, Microsoft Exchange Servers, Cisco Systems Access Servers, and virtual private network concentrators.

¹¹ Account policy settings are a series of system security configurations that control almost every aspect of user passwords, including initial creation of the password, changing the password, and forgotten passwords. The account policy section is broken down into three different categories: (1) Password Policy, which configures the password itself, with regard to validity period, length of password, and complexity of the password; (2) Account Lockout policy, which configures how the password will react when users fail to input their correct password multiple times; and (3) Kerberos Policy, which controls the Kerberos ticketing for domain communications.

¹² See Appendix D for a detailed description of the parameter settings identified at each component, along with a discussion of the risks associated with the use of those parameter settings.



Further, [REDACTED] had several high and medium risk vulnerabilities relating to account and password administration. These vulnerabilities included:

- Administrator, user, and guest accounts with no password required.
- An administrator account with a password that was the same as the user identification (ID).
- Accounts with blank passwords.
- User accounts assigned inappropriate systems privileges that could be used to access or modify any file on the system.

The absence of adequate identification and authentication controls enabled users and administrators to create weak passwords on devices providing remote access to DHS networks. To determine the extent of the use of weak passwords, we sampled a single remote access domain at each component and ran user information, dictionary, and hybrid dictionary attacks¹⁴ to identify accounts with weak or missing passwords.

¹³ DHS has also established configuration guidelines for password reuse. However, these guidelines differ from the NIST and NSA recommendations (See Appendix D for a comparison).

¹⁴ In a user information attack, the password cracking software encrypts, i.e., hashes, data from each account's password field, such as the account's user ID, and compares it to the password to determine whether any of the accounts have a password based on this information. In a dictionary attack, the password cracking software encrypts all the words in a dictionary file and compares every result with the password hash to determine whether there are any matches. In a third type of attack, known as a hybrid dictionary attack, numbers or symbols are appended to each word in the dictionary file.

Next, we analyzed the test results to identify accounts with passwords that did not comply with DHS, NIST, and NSA password complexity requirements. Each of the components had a significant number of accounts with weak passwords.



The following table details the password test results for each of the components.

Table 1: Results Of Password Strength Analysis On Remote Access Domains

| Component | Number of Accounts Tested | Accounts with No Password (Number and Percent of total) | Passwords Cracked (Number and Percent of total) | | | Cracked passwords not meeting DHS guidelines and NIST/NSA recommended settings (Number and Percent of total) |
|-----------|---------------------------|--|--|--------------------------|-------------------------------|---|
| | | | User Info/ Dictionary Attack | Hybrid Dictionary Attack | Total | |
| | 6,579 | 23 (0.35%) | 61 (0.93%) | 523 (7.95%) | 584 (8.88%) | 461 (7.01%) |
| | 41,486 | 8 (0.02%) | 981 (2.36%) | N/A ^(a) | 981 (2.36%) ^(a) | 939 (2.26%) ^(a) |
| | 4,532 | 0 (0%) | 837 (18.47%) | 819 (18.07%) | 1,656 (36.54%) | 1,605 (35.41%) |
| | 58,287 | 34 (0.06%) | 714 (1.22%) | 4,032 (6.92%) | 4,746 (8.14%) | 4,451 (7.64%) |

^(a) Due to a technical problem involving the password auditing software and the file obtained from [REDACTED] for testing, we were not able to complete the hybrid dictionary attack portion of the password strength analysis for this component. Thus, the figures presented above for [REDACTED] are for the dictionary and user information attacks only.

DHS policy requires that system ISSOs determine and enforce appropriate measures to ensure that strong passwords are used. Further, the DHS Handbook and NIST SP 800-18 require that passwords contain a combination of alphabetic, numeric, and special characters. According to NSA, passwords should also contain upper and lowercase characters.

- DHS components did not properly configure remote access hosts.¹⁶ For example, the remote access hosts had the following configuration

¹⁵



¹⁶ See Appendix E for a detailed description of the vulnerabilities identified at each component, including those related to configuration weaknesses and those resulting from missing or inappropriately applied system patches.

weaknesses that could allow attackers to gain valuable information or compromise the integrity of the system:



Table 2 illustrates the number of hosts, by component, that contained configuration weaknesses.

Table 2: Configuration Weaknesses Identified

| Component | Number of Hosts Tested ^(a) | Number of Hosts with High or Medium Risk Configuration Weaknesses | | | | |
|-----------|---------------------------------------|---|---------------|---------------|----------------------|---------------------------------|
| | | 1 Weakness | 2 Weaknesses | 3 Weaknesses | 4 or More Weaknesses | Total With 1 or More Weaknesses |
| | 10 | 0 | 3 Hosts (30%) | 0 | 3 Hosts (30%) | 6 Hosts (60%) |
| | 14 | 1 Host (7%) | 0 | 2 Hosts (14%) | 4 Hosts (29%) | 7 Hosts (50%) |
| | 11 | 1 Host (9%) | 0 | 0 | 3 Hosts (27%) | 4 Hosts (36%) |
| | 18 | 0 | 4 Hosts (22%) | 0 | 2 Hosts (11%) | 6 Hosts (33%) |

^(a) For each network reviewed, we selected a remote access domain and conducted vulnerability scans on each of the hosts in the domain.

Because of weak account policy settings, passwords, and remote access host configurations, there is increased risk that an unauthorized person could obtain or guess a user ID and password combination to gain access to DHS networks. Passwords are often the first lines of defense against hackers or insiders who may be trying to obtain unauthorized access to a computer system. The use of weak passwords, combined with inappropriate account policy settings and system configurations, might allow unauthorized internal users and external hackers to

gain access to DHS systems. This is why it is important that DHS components have strong account policies, passwords, and system configurations.

Component officials said that several of the account and configuration weaknesses noted above were the result of changes that occurred during system migrations and were not subsequently corrected. In addition, according to a [REDACTED] [REDACTED] the creation of strong passwords had not been enforced on its network because of the likelihood that users would write down their passwords in an accessible place, which may lead to password compromise. However, security training and enforcement can decrease the risk of users' writing down their passwords in accessible locations.

System and Application Patches Were Not Applied

Hosts providing remote access capabilities to DHS systems and data were not appropriately patched. Remote access hosts at each component were vulnerable to buffer overflow attacks¹⁷ or other exploits due to missing or inappropriately applied security patches.¹⁸ Specifically, according to our tests:



According to NIST SP 800-40, patching is critical to the operational availability, confidentiality, and integrity of information technology systems. Organizations should establish a systematic, accountable, and documented process for handling patches. DHS remote access hosts were highly vulnerable to attacks because

¹⁷ A buffer overflow occurs when a program or process tries to store more data in a buffer (temporary data storage area) than it was intended to hold. Since buffers are created to contain a finite amount of data, the extra information can overflow into adjacent buffers, corrupting or overwriting the valid data held in them. Attackers can use this vulnerability to replace valid data on the system with their own code and cause the system to fail or to execute their instructions.

¹⁸ See Appendix E for the number of hosts tested and number of vulnerabilities detected at each component.

they were not appropriately patched. For example, servers at [REDACTED] were vulnerable to a buffer overflow in the Microsoft Windows Messenger service.¹⁹ By sending a [REDACTED]

Subsequent to the completion of our audit work, officials from each of the components said that they had taken or planned to take corrective action to address many of the account policy, password, configuration, and patch issues that we identified. However, we did not verify that these problems had been solved.

Modems On DHS Networks May Increase Risk Of Unauthorized Access

We detected possible unauthorized modems operating on DHS networks. During our modem discovery tests, we identified modems on the analog lines of DHS Management, EP&R, CIS, and ICE. DHS Management and EP&R provided us with information regarding the mission requirement for each of the modems that we detected on their networks or phone lines, along with some of the controls implemented to reduce the risks associated with their use.

According to an ICE official, CIS and ICE were in the process of investigating 20 modems that we identified, but they were not able to provide a business justification for 18 of them. They were not able to provide a timely response, according to an ICE official, due in part to inaccuracies in the CIS and ICE database of telecommunications management information.

An unsecured modem or other dial-in facility could provide a backdoor for internal and external unauthorized users to DHS networks. According to FISCAM, dial-in access can significantly increase the risk of unauthorized access, and its use should be limited and the associated risks weighed against the benefits. Justification for such access should be documented and approved by system owners.

¹⁹ The Windows Messenger service transmits messages between client computers and servers on a network. For example, network administrators can use the Messenger service to send administrative alerts to network users, or it can be used by Windows to inform users when a print job has been completed.

Miscellaneous Issue

CIS Needs To Monitor Systems Security Functions

CIS does not monitor sufficiently the security activities performed by ICE personnel on the systems and data supporting CIS operations. CIS and ICE were part of the former Immigration and Naturalization Service and continue to share the same network infrastructure, which is managed by ICE. However, CIS does not have a process to verify that ICE information technology staff is performing necessary security or user administration functions for CIS systems and personnel. Further, ICE officials were not able to determine whether users granted remote access to the network were CIS or ICE personnel based on system records. According to CIS and ICE officials, effective CIS oversight has not been established because the components have not completed a formal memorandum of agreement concerning their respective responsibilities.

FISMA requires that senior agency officials provide security for the information and information systems that support the operations and assets under their control. Without an established process to monitor the quality of user administration performed by ICE officials, CIS lacks assurance that sufficient security is provided for the systems and data supporting its operations.

Recommendations

To enhance DHS' guidance for remote access implementation, we recommend that the CIO:

1. Update the *DHS Sensitive Systems Handbook* to include implementation and configuration procedures for remote access to DHS systems.

To protect remote access to DHS networks effectively, we recommend that the CIO:

2. Ensure that procedures for granting, monitoring, and removing user access are fully implemented according to DHS requirements, as well as NIST and FISCAM guidelines.
3. Verify that all necessary system and application patches are applied in a timely manner to reduce the risk of system compromise or failure.

Management Comments and Our Evaluation

We obtained written comments on a draft of this report from DHS. We have incorporated the comments where appropriate and included a copy of the comments in their entirety as Appendix B. DHS generally agreed with each of our recommendations. Below is a summary of DHS' response to each recommendation and our assessment of the response.

Recommendation 1: Update the *DHS Sensitive Systems Handbook* to include implementation and configuration procedures for remote access to DHS systems.

DHS plans to update the DHS Sensitive Systems Handbook with minimum requirements and configuration guidance by February 2005. It is not DHS' intent to issue "one size fits all" procedures for the entire department. DHS agreed that exit procedures need to be clear and adhered to and access permissions should be periodically revalidated, but said that regular reviews of audit logs were not feasible due to the volumes of audit data and the lack of audit reduction tools.

We accept DHS' response to update the DHS Sensitive Systems Handbook with minimum requirements and configuration guidance. We do not agree that our findings and recommendations imply that DHS must establish "one size fits all" procedures for remote access. We maintain that procedures for granting, monitoring, and removing user access must be enforced; and the Department must establish configuration guidelines for the hosts providing remote access to its networks. In addition, we also maintain that DHS should enforce the requirements outlined in the DHS Sensitive Systems Handbook for regular reviews of audit logs. As noted in the GAO FISCAM, security software should be implemented to analyze audit trail information and selectively identify unauthorized, unusual, and sensitive access activity.

Recommendation 2: Ensure that procedures for granting, monitoring, and removing user access are fully implemented according to DHS requirements, as well as NIST and FISCAM guidelines.

DHS will continue to work to enforce DHS requirements and, where appropriate, NIST and FISCAM guidelines. DHS also plans to reduce its reliance on passwords and move to stronger authentication technologies. However, where the use of passwords is still necessary, DHS policy requires the use of strong password controls, including strict limits on the number of failed logon attempts.

We accept DHS' response to move toward stronger authentication technologies. Nonetheless, many of the hosts we tested were not configured in accordance with DHS requirements and had weak passwords and password controls, including hosts that allowed an unlimited or excessive number of failed logon attempts. Until stronger authentication technologies are employed and as long as passwords are used as an identification and authentication mechanism at DHS, strong password controls must be enforced on DHS systems.

Recommendation 3: Verify that all necessary system and application patches are applied in a timely manner to reduce the risk of system compromise or failure.

DHS indicated that it will continue to strengthen its patch management. DHS also noted that implementation of some of the patches was delayed so that the impact on their systems could be tested.

We accept DHS' response to continue to strengthen its efforts for effective patch management. We agree that it is important to test the impact of system and application patches prior to their implementation. However, we identified security patches that the vendor released over six months before our review that had not yet been implemented on some DHS systems. In addition, one host was missing patches that were released in 1999 and 2000.

Purpose, Scope, and Methodology

The objective of this audit was to determine whether DHS had provided system security, integrity, and control over remote access to its computer systems and data. Specifically, we determined whether: (1) DHS developed adequate security policies and procedures to grant and control remote access to system resources, including the administration, configuration, and use of remote access paths to networks; and, (2) security controls were properly configured on applications and systems providing remote access. For some controls, we determined their adequacy, but we did not test their effectiveness. Our focus was on testing the implementation of secure configurations on the hosts controlling remote access to DHS networks.

The audit focused on wire-based remote access to DHS systems and resources, including dial-in access through modems and access through the internet. We did not examine wireless remote access, including satellite and microwave-based access, during this audit. We conducted fieldwork at the following locations:

- DHS Management
- Emergency Preparedness and Response (EP&R)
- Bureau of Citizenship and Immigration Services (CIS)
- Bureau of Immigration and Customs Enforcement (ICE)
- Transportation Security Administration (TSA)

During the audit, we used three software tools to conduct internal and external security tests to evaluate the effectiveness of controls implemented for remote access. NIST SP 800-42 identifies the following as common testing tools:

- Internet Security Systems' (ISS) Internet Scanner 7.0, which is a component of the ISS Dynamic Threat Protection platform, was used to detect and analyze vulnerabilities on DHS systems, including servers and infrastructure devices.
- @stake's L0phtCrack 5.02, which is a password auditing and recovery application, was used to analyze passwords that control remote access to DHS systems and resources. We analyzed encrypted system passwords to test for compliance with agency password policies or security best practices.
- Sandstorm Enterprises' PhoneSweep 4.0, which is a telephone scanner, was used for modem discovery and analysis, also known as

“war dialing.”²⁰ PhoneSweep was used to dial a range of numbers, provided by the selected components, to identify modems and computers running remote access software to bypass the corporate firewall. Once an active modem was identified, we did not use PhoneSweep to establish a connection with the modem using standard user ID and password combinations.

Before the creation of DHS, both CIS and ICE were part of the former Immigration and Naturalization Service; these components continue to share the same infrastructure, which is managed by ICE. As a result, the technical scans for CIS and ICE were combined. Upon completion of testing, we provided each component the technical reports detailing the specific vulnerabilities detected on their networks and the actions needed for remediation.

We conducted our audit between April and August 2004 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.

The principal OIG 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.

²⁰ Also synonymous with demon dialing, is a technique by which a computer would repeatedly dial a large number of telephone numbers to find test tones, computers, voice mailboxes, private branch exchanges, and government offices.


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



October 28, 2011

**Homeland
Security**

MEMORANDUM FOR: Clark Kent Ervin
Inspector General

FROM: Steve Cooper 
Chief Information Officer

SUBJECT: CIO Comments on Draft Audit Report – *DHS Needs to Strengthen Controls For Remote Access to Its Systems and Data* (OIG-IT-04-008)

Thank you for the opportunity to review and comment on your draft report *DHS Needs to Strengthen Controls For Remote Access to Its Systems and Data*. After reviewing your report, I am in support of your recommendations and appreciate the work done by your team to assist us in identifying opportunities for improvement. Many of the recommendations made have now been incorporated into our planning, and are now reflected in our program objectives and milestones.

I would like to address comments in some of your findings which do not seem to be supported by our understanding of your audit results. I believe these findings may not fully take into consideration the diverse nature of the Department's operations.

FINDING - Remote Access Security Procedures Have Not Been Fully Developed And Implemented

The policy, as noted, has been developed, but it is not our intent to issue "one size fits all" procedures for the entire department. There are valid operational reasons for the range of risk acceptance policies throughout the department. To mandate a single explicit procedure for remote access ignores the reality that even within a single organization there will be applications and systems that will have diverse operational requirements. The only viable strategy in this environment is to establish policy as a baseline for our expectations. It is recognized that Organizational Elements are not yet in complete alignment with Department information security policies, and we are aggressively working to bring them into compliance.

I fully concur that exit procedures need to be clear and adhered to and access permissions should be periodically revalidated, but current practice and policy make the exhaustive review of audit material an inappropriate use of resources. It should be noted that the Department must depend on firewalls and intrusion detection systems, as well as other alarms, to alert us to potential problems. We

www.dhs.gov

then review audit files for event reconstruction on a case-by-case basis. The volumes of audit data and the lack of effective audit reduction tools make it impossible to review every log in real time. DHS policy also mandates that Information Systems Security Officers review audit logs on a reoccurring basis for these same reasons.

FINDING - Remote Access Hosts Are Vulnerable

The reality is that given the sophistication of current tools, if access is given to the password file, such as was provided to the OIG, every password should be broken, regardless of complexity. By way of illustration, the tool used by the auditors reported the finding of accounts with no password, or equivalent password and account names, yet none of the reported accounts could be accessed when remediation was attempted. The department has made a conscious decision to minimize and reduce the reliance on passwords and move to stronger authentication technologies. Where the use of passwords is still required, DHS policy is to strictly limit the number of logon attempts, and DHS policy also focuses on protection of the password file. As we complete the transition to Windows 2003 on most of our networks, it will be impossible to have a password that does not comply with DHS complexity requirements.

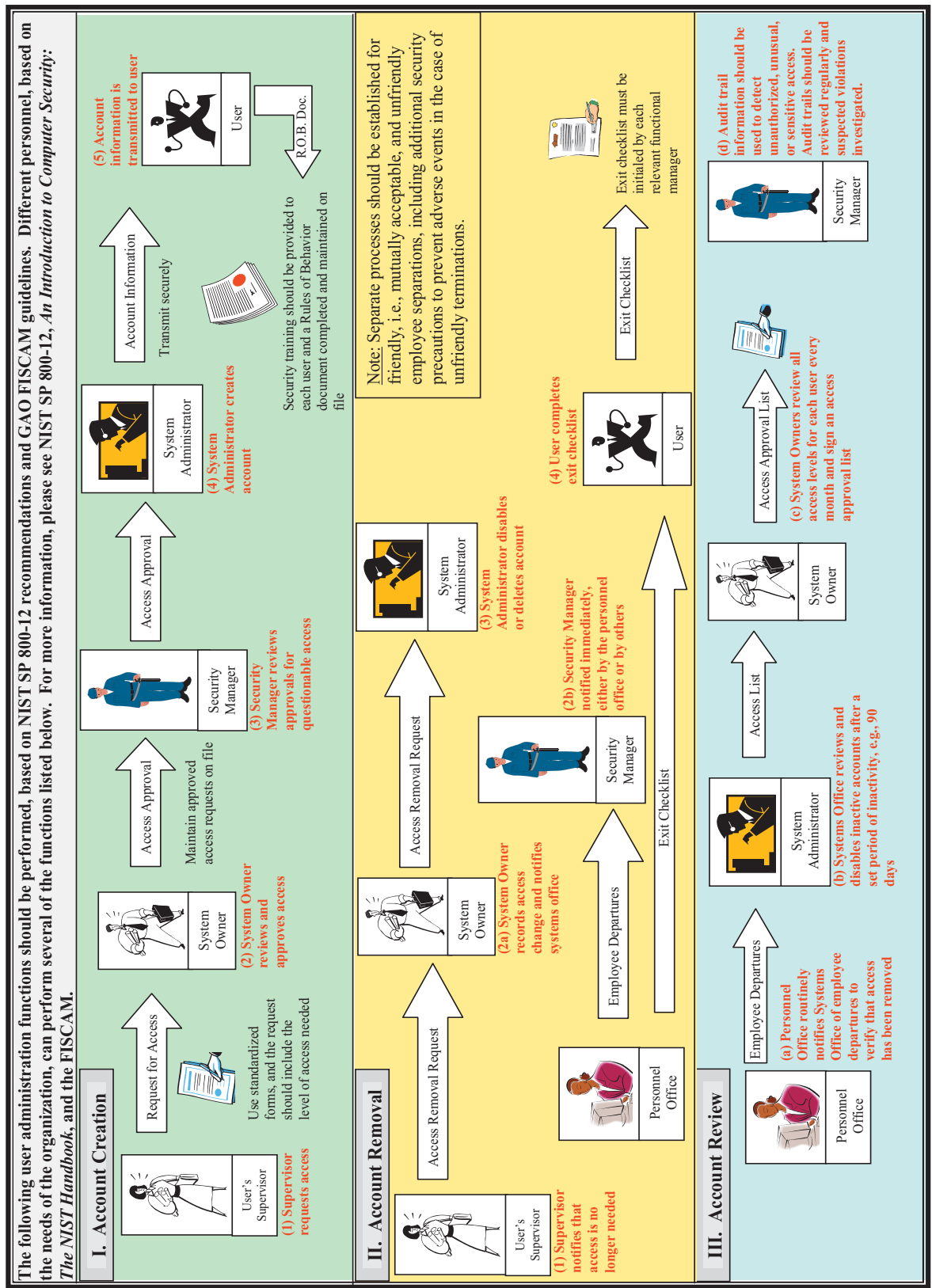
FINDING - System and Application Patches Were Not Applied

Again, based on extrapolating my experience with the DHS Management System, my concerns are mitigated by the fact that all of the patches identified were in testing to be implemented. It is not good practice to deploy patches without testing the impact on our essential systems. I support strong patch management and will continue to work to ensure effective implementation. I appreciate any feedback your office may have on our continuing efforts in this area.

CIO Response to OIG Recommendations

1. Update DHS Sensitive Systems Handbook - Planned for February 2005, will provide minimum requirements and configuration guidance as opposed to proscriptive uniform procedures.
2. Ensure that procedures for user access are implemented – DHS will continue to work to enforce DHS requirements and where appropriate NIST and FISCAM guidelines.
3. Verify Patch Management – DHS will continue and strengthen its efforts for effective Patch Management while working to reduce the time required for pre-deployment testing.

Again, I thank you for the opportunity to provide our comments. If you should have any questions, please do not hesitate to contact my office.



| Parameter | Risk Associated with Weak Policy Setting | NIST and NSA Recommended Setting | DHS Required Setting | Actual Setting | | | |
|---|--|---|----------------------------|--------------------|-----------------------------|-----------------------------|-----------------------------|
| | | | | | | | |
| <u>Maximum password age:</u> The period of time that a user is allowed to have a password before being required to change it. | Limiting password life reduces the likelihood of unauthorized access | Less than 90 days | Less than 90 days | 90 days | Passwords never expire | Passwords never expire | 45 days |
| <u>Minimum password age:</u> Specifies how long a user must wait after changing a password before changing it again. | If changes are allowed immediately, a user could change their password, then immediately change it back to what it was before. | At least 1 day | At least 1 day | 14 days | Changes allowed immediately | Changes allowed immediately | Changes allowed immediately |
| <u>Minimum password length:</u> The minimum number of characters a password must contain | Blank passwords and shorter length passwords are easily guessed by password cracking tools. | High risk environments: 12 characters Other environments: 8 characters | 8 characters | 8 characters | 6 characters | 5 characters | 8 characters |
| <u>Password uniqueness/history:</u> Prevents users from toggling among their favorite passwords | Forcing users to change their passwords reduces the likelihood that a hacker or password cracker will discover passwords. | 24 passwords | 4 to 6 passwords | 24 passwords | 5 passwords | 10 passwords | 24 passwords |
| <u>Account lockout after # of bad logon attempts:</u> Specifies the number of bad logon attempts that can be made before an account is locked out. | Establishing an account lockout threshold helps prevent password cracking or guessing attacks on the system. | 3 invalid attempts or less | 3 invalid attempts or less | 3 invalid attempts | No account lockout | 12 invalid attempts | 3 invalid attempts |

Appendix D Account Policy Settings

| | | | | | | | |
|---|---|--|---------------|------------|--------------------|------------|------------|
| <u>Reset lockout counter after # of minutes:</u> Specifies the number of minutes until the bad logon count is reset. | Setting the number of minutes too low may reduce the effectiveness of the account lockout control | 15 minutes or more | Not specified | 15 minutes | No account lockout | 30 minutes | 15 minutes |
| <u>Lockout duration:</u> Sets the number of minutes an account will be locked out. | Setting the number of minutes too low may reduce the effectiveness of the account lockout control | 15 minutes or more, but not forever ^(a) | Forever | 15 minutes | No account lockout | Forever | 15 minutes |

(a) According to NSA, setting the lockout duration to forever may lead to a denial of service attack, i.e., a form of attacking another computer to prevent legitimate users of a system from using the computer or its services.

| Component | Number of Hosts Tested | Number of Vulnerabilities Detected ^(a) | | | Total | | |
|---|------------------------|---|-----------------------------|--------------|--------------|----------------------|----------------------|
| | | High Risk Vulnerabilities | Medium Risk Vulnerabilities | | | | |
| | 10 | 13 | 12 | | 25 | | |
| | 14 | 21 | 52 | | 73 | | |
| | 11 | 4 | 14 | | 18 | | |
| | 18 | 8 | 10 | | 18 | | |
| Number of Hosts with High or Medium Risk Vulnerabilities ^(a) (Number and Percent) | | | | | | | |
| Component | Number of Hosts Tested | Number of Hosts with High or Medium Risk Vulnerabilities ^(a) (Number and Percent) | | | | | Total with 1 or More |
| | | No Weaknesses | 1 Weakness | 2 Weaknesses | 3 Weaknesses | 4 or More Weaknesses | |
| | 10 | 3 (30%) | 1 (10%) | 0 | 3 (30%) | 3 (30%) | 7 (70%) |
| | 14 | 7 (50%) | 1 (7%) | 0 | 1 (7%) | 5 (36%) | 7 (50%) |
| | 11 | 7 (64%) | 0 | 1 (9%) | 0 | 3 (27%) | 4 (36%) |
| | 18 | 11 (61%) | 1 (6%) | 4 (22%) | 0 | 2 (11%) | 7 (39%) |

^(a) Includes configuration weaknesses and patch-related vulnerabilities

Information Security Audits Division

Edward G. Coleman, Director
Patrick Nadon, Audit Manager
Chiu-Tong Tsang, Audit Team Leader
Jason Bakelar, Auditor
Pedro Calderon, Auditor
Evan Portelos, Associate
Anthony Nicholson, Referencer

Advanced Technology Division

Jim Lantzy, Director
Chris Hablas, Senior Security Engineer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
General Counsel
Under Secretary, Management
DHS OIG Liaison
DHS Chief Information Security Officer
DHS Public Affairs
CIO Audit Liaison
DHS Office of Security
Director, Compliance and Oversight Program, OCIO

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 Department of Homeland Security, Washington, DC 20528, Attn: Office of Inspector General, Investigations Division – Hotline. The OIG seeks to protect the identity of each writer and caller.