

DEPARTMENT OF HOMELAND SECURITY

Office of Inspector General

Security Weaknesses Increase Risks to Critical United States Secret Service 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-05-37

September 2005



**Homeland
Security**

Preface

The Department of Homeland Security (DHS) Office of Inspector General (OIG) was established by the Homeland Security Act of 2002 (Public Law 107-296) by amendment to the Inspector General Act of 1978. This is one of a series of audit, inspection, and special reports prepared as part of our DHS oversight responsibilities to promote economy, effectiveness, and efficiency within the department.

This report assesses the strengths and weaknesses of database security controls over United States Secret Service (Secret Service) resources. It is based on interviews with Secret Service officials, direct observations, technical scans, and a review of applicable documents.

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

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

Richard L. Skinner
Inspector General

Table of Contents/Abbreviations

Executive Summary	1
Background	3
Results of Audit	5
Strengthening of Database Security Procedures Is Needed	5
Recommendations	9
Management Comments and OIG Analysis	10
SSWeb Servers Are Vulnerable	11
Recommendation	18
Management Comments and OIG Analysis	18

Appendices

Appendix A: Purpose, Scope, and Methodology	19
Appendix B: Management’s Response	21
Appendix C: Vulnerabilities Identified and Addressed	26
Appendix D: FISMA Metrics	27
Appendix E: SSWeb Architecture	29
Appendix F: Major Contributors to this Report	30
Appendix G: Report Distribution	31

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
FISMA	Federal Information Security Management Act of 2002

Table of Contents/Abbreviations

ISS	Internet Security Systems
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan of Action and Milestones
Secret Service	United States Secret Service
SP	Special Publication
SSWeb	Secret Service Web

OIG

*Department of Homeland Security
Office of Inspector General*

Executive Summary

We audited the Department of Homeland Security (DHS) and its organizational components' security program to evaluate the security and integrity of select sensitive but unclassified mission critical databases.¹ This audit included reviews of access controls, change management, and continuity of operations policies and procedures. This report assesses the strengths and weaknesses of security controls over United States Secret Service (Secret Service) database resources.

Our objective was to determine whether the Secret Service had implemented adequate and effective controls over sensitive data contained in its Secret Service Web (SSWeb) system, which houses sensitive information concerning protective operations. We interviewed Secret Service officials, reviewed database security documents, and performed technical tests of one [REDACTED] database server as well as one application server.

The Secret Service has not established adequate or effective database security controls for SSWeb. Although the Secret Service has developed and implemented many essential security controls—including a process to ensure that system access is removed upon employee separation as well as a change management policy for implementing routine and emergency changes—additional work remains to implement the access controls, configuration management procedures, and continuity of operations safeguards necessary to protect sensitive SSWeb data effectively. Specifically, the Secret Service has not 1) implemented effective procedures for user administration; 2) maintained

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

and reviewed adequate audit trail information;² 3) established a configuration management plan; or, 4) developed and tested an Information Technology (IT) contingency plan. In addition, vulnerabilities existed on the SSWeb ----- database server related to access rights and password administration, configuration management, ----- . Due to these database security exposures, there is an increased risk that unauthorized individuals could gain access to critical Secret Service database resources and compromise the confidentiality, integrity, and availability of sensitive SSWeb data. Further, the Secret Service may not be able to recover SSWeb following a disaster.

Following our audit work, Secret Service officials stated that they had taken or planned to take corrective action to address 40 of the 41 vulnerabilities identified during our technical testing. Secret Service officials stated that they did not intend to address the remaining vulnerability due to resource limitations and competing priorities. 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 are recommending that the Secret Service Director instruct the Chief Information Officer (CIO) to:

- Ensure that adequate controls for granting, monitoring, and removing SSWeb user access are implemented.
- Maintain and review ----- information.
- Complete a configuration management plan for the SSWeb system.
- Develop and test a SSWeb IT contingency plan.
- Implement corrective action plans to address all identified SSWeb vulnerabilities and configuration weaknesses.
- Examine methods to implement -----
-----.

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 Secret Service's information

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.

security program and practices as implemented for SSWeb.³ The Secret Service has not yet fully aligned its security program with DHS' overall policies or procedures. For example: a contingency plan has not been established and tested; security control costs have not been integrated into the life cycle of the system; and, system and database administrators have not obtained specialized security training. Appendix D summarizes the results of our FISMA evaluation.

Fieldwork was conducted from December 2004 through March 2005 at the Secret Service headquarters in Washington, DC; the Secret Service alternate operating facility in [REDACTED]; 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 Secret Service generally concurred with our recommendations and is in the process of implementing corrective measures. The Secret Service also indicated that the recommendations we provided would be used to strengthen security on other component systems. The Secret Service did not agree with recommendation 6. The Secret Service does not plan to

[REDACTED]

[REDACTED] The Secret Service'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.

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

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.

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

SSWeb is a database system that serves as the secure corporate intranet for the Secret Service. The SSWeb system consists of eight applications, including:

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

SSWeb utilizes a multi-tiered architecture based on database servers, web servers, and individual user workstations. The SSWeb system consists of:

- A database server [REDACTED]
- A database server [REDACTED]
- An application server [REDACTED]

Although all Secret Service personnel use the SSWeb system, access to the [REDACTED] is restricted. There are approximately 150 Secret Service personnel that are regular [REDACTED] though the number of users may double during national special security events.

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 [REDACTED] DBMS.

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 Secret Service has not implemented the security controls necessary to protect the SSWeb system and its data. In assessing the procedures governing the security of sensitive data contained in SSWeb, we identified user administration, auditing, configuration management, and IT contingency

planning weaknesses. As a result, there is significant risk that the security procedures protecting the Secret Service's critical databases may not prevent unauthorized access to its systems and data. In addition, the Secret Service may not be able to recover SSWeb operations following a disaster or disruption.

User Administration Procedures Are Incomplete

The Secret Service has implemented a process for granting, monitoring, and removing SSWeb and [REDACTED] that includes controls to protect access to the system and its data. For example, the Secret Service has established a process to control emergency and temporary access for privileged SSWeb users, as well as a process to ensure that system access is removed upon employee separation. However, additional work remains to implement the access control procedures needed to limit system access to appropriate personnel adequately. Specifically:

- The Secret Service has not ensured that privileged access is removed upon transfer or reassignment of administrators. We identified an active administrator account that belonged to a former SSWeb database administrator. This account was not disabled or removed following the official's transfer.
- The Secret Service has not required SSWeb users to complete rules of behavior documents. According to the Secret Service Information Systems Security Manager, SSWeb users are expected to be aware of agency policies, but the component has not implemented rules of behavior documents for Secret Service information systems. The Secret Service plans to develop a component-wide rules of behavior document by September 2005.
- The Secret Service has not developed a process to document and maintain a record of [REDACTED]. The Secret Service official responsible for [REDACTED] stated that he is able to keep track of the appropriate access privileges for each of the [REDACTED] database users without written records.

DHS Policy requires that user access be controlled and limited based on user identification and authentication mechanisms that support the minimum requirements of access control, least privilege, and system integrity.⁵ Also, the policy requires that access be revoked upon employee transfer and that rules of behavior be developed for each DHS system. The rules of behavior must

⁵ The principle of least privilege requires that users be given the most restrictive set of privileges needed to perform authorized tasks.

clearly delineate responsibilities and the expected behavior of all individuals with access to the system, and must be made available for each user to read and sign before access is granted to the system. Further, DHS and NIST require that user access rights be reviewed periodically to ensure that the types and levels of access granted remain appropriate. To facilitate this process, user access authorizations should be documented in a standard format and maintained on file.

Because SSWeb user administration procedures have not been fully implemented, there is greater risk that individuals who no longer require access to the system will continue to access sensitive data. In addition, SSWeb users may not fully understand their security responsibilities or the penalties associated with security violations. As a result, sensitive SSWeb information may not be adequately protected.

SSWeb Auditing Is Inadequate

The Secret Service does not have procedures to capture, review, or retain audit trail information for SSWeb. Specifically:

- The Secret Service has not developed sufficient procedures to review and retain [redacted] information for SSWeb. The Secret Service maintains an [redacted] of pertinent information related to a certain number of operating system level security events, including [redacted]. However, [redacted] audit trail records are usually reviewed [redacted]. In addition, only three months of historical [redacted] information exists for SSWeb, due to a shortage of backup media.
- The [redacted] database server did not have [redacted]

Secret Service officials stated that they are in the process of reviewing several auditing software packages that will increase the SSWeb system's auditing capabilities, including [redacted]. The component plans to implement the selected software package by August 2005.

[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. However, to be effective, significant security events must be recorded and the audit trails must be reviewed and retained. According to the DHS Handbook, the review of audit trail information is essential because unauthorized access, modification, or destruction of data may be discovered only through the review process. ----- and retention procedures, inappropriate access to sensitive data or malicious changes to SSWeb may not be detected or investigated.

A SSWeb Configuration Management Plan Has Not Been Completed

The Secret Service has developed and implemented a change management policy for implementing routine and emergency changes to the SSWeb system. However, the Secret Service does not have a SSWeb configuration management plan or documented configuration management procedures for the system. Configuration management plans and procedures help ensure that the configuration of a system or network is consistent with its security certification and accreditation (C&A); and, any subsequent changes have been approved, including an analysis of any potential security implications. Secret Service officials stated that it is working to develop and implement a configuration management plan and new configuration management procedures. The Secret Service expects to complete implementation of the new plan and procedures by August 2005.

DHS Policy requires that organizational components prepare configuration management plans for all IT systems and networks. The DHS Handbook also requires that the initial configuration of a system be documented in detail, and that change control procedures be documented and implemented for all proposed configuration changes to the system. Until adequate and effective configuration management plans and procedures are implemented, there is greater risk that routine and emergency changes to the system will not be controlled adequately.

An IT Contingency Plan Has Not Been Developed and Tested

The Secret Service has not established a SSWeb IT contingency plan or conducted a formal test of data backup and restoration procedures for the system. The Secret Service has developed a continuity of operations template, and is currently in the process of creating a draft IT contingency plan for the

system. According to Secret Service officials, the plan will be completed by December 2005. Following the completion of our review, Secret Service officials stated that they have begun conducting quarterly tests of the system's data backup and restoration procedures.

DHS Policy requires that comprehensive IT contingency plans be developed, tested, exercised, and maintained for critical major applications and general support systems. Also, DHS requires that quarterly tests of data backup and restoration procedures be performed.

According to NIST, contingency planning is essential because it establishes the plans, procedures, and technical measures necessary to recover a system quickly and effectively following a service outage or disaster. IT contingency plan testing enables deficiencies to be identified and addressed. Formal tests of established data restoration procedures are an integral part of testing the overall contingency plan, and help ensure that all necessary data can be recovered in the event of a disaster. As a result of the lack of adequate contingency planning and testing for the system, including tests of the SSWeb data restoration process, the Secret Service lacks assurance that the component will be able to resume operations following a disaster.

Recommendations

To protect sensitive SSWeb data, we recommend that the Secret Service Director instruct the CIO to:

1. Ensure that adequate controls for granting, monitoring, and removing SSWeb user access are implemented according to DHS requirements and NIST guidelines.
2. Maintain and review ----- to facilitate the detection and investigation of inappropriate access or malicious changes to SSWeb and its applications.
3. Complete an SSWeb configuration management plan and documented configuration management procedures to ensure that routine and emergency changes to the system are adequately controlled.
4. Develop an IT contingency plan for SSWeb, and ensure that annual tests of the plan and quarterly tests of data restoration procedures are conducted.

Management Comments and OIG Analysis

The Secret Service concurs with recommendation 1. The Secret Service recognizes the need for better controls to ensure removal of access privileges is no longer needed, as well as to maintain better records of accesses granted and removed. The Secret Service is currently working to improve its "Profile Request" system to address the user administration weaknesses identified. The Secret Service plans to complete the system enhancements by October 2005. In addition, the Secret Service has developed and implemented a Rules of Behavior policy directive.

We accept the Secret Service's response to enhance its controls for granting, monitoring, and removing user access and the implementation of Rules of Behavior for Secret Service systems.

The Secret Service concurs with recommendation 2. The Secret Service has been investigating software-based solutions to facilitate the review of audit trail information, and plans to implement the selected product by December 2005.

We accept the Secret Service's response to implement regular reviews of [REDACTED]. However, the Secret Service did not indicate that [REDACTED] will be recorded, or that [REDACTED] will be retained in accordance with DHS requirements. We maintain that [REDACTED] must be recorded and retained to ensure that suspicious activity is detected and investigated.

The Secret Service generally concurs with recommendation 3. The Secret Service recognizes the need for a robust configuration management program. The Secret Service is developing policies, procedures, and guidelines for configuration management plans, which it plans to complete by October 2005. Once these guidelines are complete, the Secret Service will develop a configuration management plan for the SSWeb system. The target date for the completion of the SSWeb configuration management plan is December 2005.

We accept the Secret Service's plan of action to establish policies, procedures, and guidelines for configuration management plans as well as to develop a configuration management plan for the SSWeb system.

The Secret Service concurs with recommendation 4. The Secret Service has developed a new contingency plan template, as well as a draft contingency plan for the SSWeb system. The Secret Service plans to complete the new SSWeb contingency plan by October 2005. Also, the Secret Service has begun regular

quarterly testing of system backup and restoration procedures for the SSWeb system. A requirement for regular testing of these procedures will be included in the new SSWeb contingency plan.

We accept the Secret Service's plan of action to conduct regular quarterly testing of system backup and restoration procedures and to develop a SSWeb IT contingency plan. However, the Secret Service did not indicate that an annual test of the contingency plan would be completed. We maintain that the Secret Service should have a process to ensure that an annual test of the contingency plan is conducted.

SSWeb Servers Are Vulnerable

The Secret Service has not established effective database security controls for SSWeb. To assess the security of the SSWeb system, we performed vulnerability assessment scans to identify configuration weaknesses; and, conducted manual checks of the security settings on the SSWeb [REDACTED] database server to identify additional configuration weaknesses as well as to 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]. These control weaknesses could enable an attacker to gain inappropriate access to SSWeb and its data.

Access Privileges Were Not Appropriately Restricted

The Secret Service did not enforce strong identification or authentication measures for SSWeb. The [REDACTED] database server we tested did not appropriately restrict access to the system. For example:

- [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 following software installation. For example, [Redacted]

Table 1 illustrates the number of access rights and password vulnerabilities that we identified on the SSWeb database and application servers, along with the corrective actions that the Secret Service 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]	5	12	17	0	17 (100%)	17 (100%)
[REDACTED]	0	0	0	N/A	N/A	N/A
Total	5	12	17	0	17 (100%)	17 (100%)

(a) Manual security parameter tests were only conducted on the [REDACTED] database server.

Source: OIG table based on the results of technical testing and interviews with Secret Service 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 secure baseline configuration guide for [REDACTED]

[REDACTED] Further, the DHS Handbook and secure baseline configuration guidelines provide specific requirements related to [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 Secret Service networks and systems.

The SSWeb Database Server Is Not Configured Appropriately

The Secret Service did not configure network services and security parameters to protect SSWeb data and files. For example:

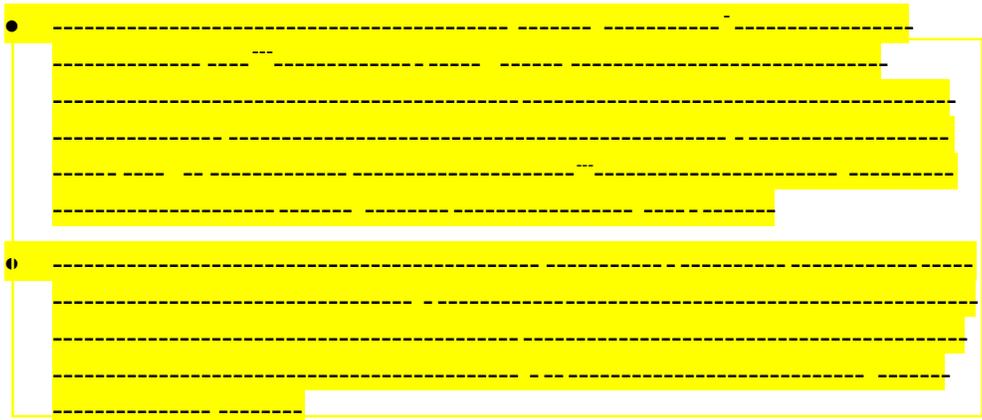


Table 2 illustrates the number of configuration management vulnerabilities that we identified on the SSWeb database and application servers, along with the corrective actions that the Secret Service has planned or already taken to address these weaknesses.

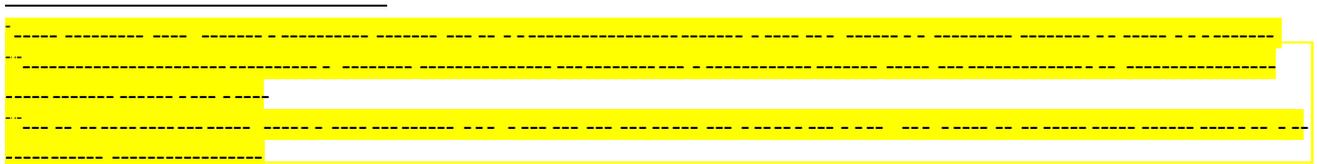
Table 2: Configuration Management Vulnerabilities Identified and Addressed

Server	Number of Vulnerabilities Identified			Number That Have Been Addressed		
	High Risk	Medium Risk	Total	Corrected	Planned	Total
[Redacted]	1	18	19	0	19 (100%)	19 (100%)
[Redacted]	0	0	0	N/A	N/A	N/A
Total	1	18	19	0	19 (100%)	19 (100%)

(a) Manual security parameter tests were only conducted on the [Redacted] database server.

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

The configuration weaknesses noted above are largely the result of default system settings that were not changed at the time the software was installed.



These default settings should be reviewed and properly configured following installation to ensure that the system is adequately protected.

SSWeb Has Not Been [REDACTED]

The Secret Service has not [REDACTED]. We examined the [REDACTED] application and [REDACTED] database servers to determine if all of the appropriate [REDACTED]. The Secret Service had not [REDACTED] database server because the [REDACTED]. Also, we reviewed the [REDACTED] database server to determine if [REDACTED].

Table 3 illustrates the number of [REDACTED] vulnerabilities that we identified on the SSWeb database and application servers, along with the corrective actions that the Secret Service 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		
	High Risk	Medium Risk			Planned	Total
[REDACTED]	2	0	2	1 (50%)	1 (50%)	2 (100%)
[REDACTED]	0	0	0	N/A	N/A	N/A
Total	2	0	2	1 (50%)	1 (50%)	2 (100%)

(a) Manual security parameter tests were only conducted on the [REDACTED] database server.

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

DHS Policy requires that IT security [REDACTED] in accordance with configuration management plans or direction from higher authorities.

[REDACTED]

Table 4 illustrates the number of [REDACTED] that we identified for the SSWeb database and application servers, along with the corrective actions that the Secret Service has planned or already taken to address these weaknesses.

Table 4: [REDACTED] Vulnerabilities Identified and Addressed

Server	Number of Vulnerabilities Identified			Number That Have Been Addressed			Number For Which No Corrective Action Plan Was Provided
	High Risk	Medium Risk	Total	Corrected	Planned	Total	
[REDACTED]	1	2	3	0	2 (67%)	2 (67%)	1 (33%)
[REDACTED]	0	0	0	N/A	N/A	N/A	N/A
Total	1	2	3	0	2 (67%)	2 (67%)	1 (33%)

(a) Manual security parameter tests were only conducted on the [REDACTED] database server.

Source: OIG table based on the results of technical testing and interviews with Secret Service 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. As a result of these encryption weaknesses, an individual could [REDACTED]

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

Recommendations

To protect sensitive SSWeb data, we recommend that the Secret Service Director instruct the CIO to:

5. Develop and implement corrective action plans to address all identified SSWeb vulnerabilities and configuration weaknesses to reduce the risk of system compromise or failure.
6. Examine methods to implement [REDACTED] [REDACTED] to ensure that sensitive data is adequately protected.

Management Comments and OIG Analysis

The Secret Service generally concurs with recommendation 5. The Secret Service started implementing corrective actions to address vulnerabilities shortly after the exit conference, beginning with those items identified as high risk. The Secret Service will complete corrective action plans for 29 of the 41 vulnerabilities by the end of August 2005, and will address an additional eight vulnerabilities by December 2005. The Secret Service does not plan to remedy three of the remaining vulnerabilities due to operational requirements.

We accept the Secret Service's plan to implement corrective action plans for the vulnerabilities identified during our review. For those vulnerabilities deemed necessary due to operational requirements, the Secret Service should document the risks and ensure that the designated approving authority formally accepts these risks for the SSWeb system.

The Secret Service does not concur with recommendation 6. The Secret Service does not plan to implement [REDACTED] due to resource limitations and competing priorities.

We maintain that the Secret Service should continue to explore the implementation of [REDACTED]. Further, the Secret Service should document the risk associated with [REDACTED] [REDACTED] and ensure that the designated approving authority formally accepts this risk.

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 Secret Service'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. Based on our analysis and information obtained from Secret Service officials, we selected the SSWeb system for inclusion in our review.

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

- 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 database and DBMS selected for review.

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

provided the Secret Service with technical reports detailing the specific vulnerabilities detected on the SSWeb system and the actions needed for remediation.

We conducted fieldwork at the Secret Service headquarters in Washington, DC; the Secret Service alternate operating facility in -----; and, the OIG's ATL. We conducted our audit between December 2004 and March 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 SECRET SERVICE

Washington, D.C. 20223

August 16, 2005

MEMORANDUM FOR EDWARD COLEMAN
DIRECTOR
INFORMATION SECURITY AUDIT DIVISION
OFFICE OF INSPECTOR GENERAL
U.S. DEPARTMENT OF HOMELAND SECURITY

Attention: Patrick Nadon

FROM:

Keith W. Young
Assistant Director
Office of Inspection

A handwritten signature in black ink, appearing to read "Keith W. Young", written over the typed name and title.

SUBJECT:

A-IT-05-003 (Database Audit)

Reference is made to the Inspector General (OIG) draft report entitled "Security Weaknesses Increase Risks to Critical United States Secret Service Database."

Attached is a memorandum from the Assistant Director, Office of Protective Research, containing the Secret Service's responses to the findings of the above-mentioned draft report.

Should you have any further questions regarding this matter, please contact GAO/OIG Liaison, DeDee Hayes, Office of Inspection, at 202/406-5766.

Attachment

UNITED STATES GOVERNMENT

memorandum

DATE: August 15, 2005

REPLY TO
ATTN OF: Acting Chief Information Officer *Cgt*

U.S. SECRET SERVICE

SUBJECT: Comments on Draft Audit Report,
"Security Weaknesses Increase
Risks to Critical United States
Secret Service Database", DHS OIG
Report OIG-05-XXX

145.050

THRU: AD – Office of Protective Research *[Signature]*

TO: AD – Office of Inspection

This is in response to the Department of Homeland Security (DHS) Office of Inspector General draft audit report entitled "Security Weaknesses Increase Risks to Critical United States Secret Service Database", received on July 14, 2005. Please forward these comments to the Office of the Inspector General for inclusion in the final report.

General Comments

While in general we concur with the recommendations provided in this report, it is important to note that the security weaknesses identified all occur within the Secret Service IT environment which has strong protection from any external penetration. The fact that all Secret Service employees and contractors having access to production Secret Service systems are required to maintain active Top Secret security clearances significantly mitigates the potential impact of these weaknesses. Regardless, we take these recommendations very seriously and provide specific actions that we either have taken or will take to address each recommendation. For some of the recommendations we also offer clarifying management comments to present a more current interpretation of the issues identified in the report.

Office of the Inspector General Recommendations

The report offered 6 recommendations:

1. Ensure that adequate controls for granting, monitoring, and removing user access to SSWeb are implemented according to DHS requirements and NIST guidelines.
2. Maintain and review [REDACTED]
3. Complete an SSWeb configuration management plan and documented configuration management procedures to ensure that routine and emergency changes to the system are adequately controlled.
4. Develop an IT contingency plan for SSWeb, and ensure that annual tests of the plan and quarterly tests of data restoration procedures are conducted.
5. Develop and implement corrective action plans to address all identified SSWeb vulnerabilities and configuration weaknesses to reduce the risk of system compromise or failure.

Appendix B
Management's Response

6. Examine methods to implement [REDACTED] to ensure that sensitive data is adequately protected.

CIO Response to the Recommendations

Recommendation #1 – "Ensure that adequate controls for granting, monitoring, and removing user access to SSWeb are implemented according to DHS requirements and NIST guidelines."

Management Comments – Authority for granting, monitoring, and removing user access to applications residing on the SSWeb system is given only to the respective application owner, which in most cases is a senior level manager in the respective business area. This is the case for the [REDACTED], which was the primary focus of this audit activity. To maintain the ability to respond quickly to operational needs this authority must be broad in its scope. The audit recommendations point out the need for better controls to ensure removal of access privileges no longer needed and to maintain better records of accesses granted and removed. We concur with these recommendations, and have developed and published a Rules of Behavior policy directive dated 6/9/2005.

Proposed Actions and Completion Date

- Requests for access to individual applications are made through a Secret Service "Profile Request" system. The Secret Service has a project underway to enhance the "Profile Request" system to address the shortcomings identified in the audit report. The target date for completing these enhancements is October 2005.

Recommendation #2 – "Maintain and [REDACTED] to facilitate the detection and investigation of inappropriate access or malicious changes to SSWeb and its applications."

Management Comments – Our ability to fully review audit trail records is constrained by both staffing and financial resources. For this reason we have made a risk based decision [REDACTED]. We recognize the need for more complete and regular review of audit records and have been investigating software-based solutions to facilitate these reviews.

Proposed Actions and Completion Date

- The Secret Service will implement [REDACTED] which will enhance our capability to regularly review audit records. The target date for completion of this action is December 2005.

Recommendation #3 – "Complete an SSWeb configuration management plan and documented configuration management procedures to ensure that routine and emergency changes to the system are adequately controlled."

Management Comments – While we have long recognized the need for a robust configuration management program, resource constraints and operational priorities have presented us with significant challenges in achieving this goal. Alternately, we focused our resources on developing change control policies and procedures to protect the integrity of our IT environment whenever changes are implemented. These change control policies and procedures have proven to be very effective in preventing system failures resulting from inadequately planned or tested changes. While we recognize that these processes are not a substitute for configuration management, they do protect our systems from unauthorized or unplanned changes.

Appendix B
Management's Response

Proposed Actions and Completion Date

- The Secret Service is developing policies, procedures, and guidelines for configuration management plans. The target date for completing these guidelines is October 2005.
- Using these guidelines, we will develop a configuration management plan for the SSWeb system. The target date for completion of this configuration management plan is December 2005.

Recommendation #4 – "Develop an IT contingency plan for SSWeb, and ensure that annual tests of the plan and quarterly tests of data restoration procedures are conducted."

Management Comments – We concur completely with the need to develop and regularly test contingency plans for all our IT systems, and have developed a template which will be used for developing all contingency plans. While completion of these contingency plans is a high priority we are constrained by staffing and financial resources to complete all these plans quickly and must make risk based decisions to determine which systems have the highest priority for developing contingency plans. Completion of a contingency plan for the SSWeb system is considered a high priority and we have completed a draft of this plan. We have begun regular quarterly testing of system backup and restoration procedures for the SSWeb system.

Proposed Actions and Completion Date

- The Secret Service will complete development and approval of the IT contingency plan for the SSWeb system which will include requirements for regular testing of backup and restoration procedures. The target date for completing this plan is October 2005.

Recommendation #5 – "Develop and implement corrective action plans to address all identified SSWeb vulnerabilities and configuration weaknesses to reduce the risk of system compromise or failure."

Management Comments – We started implementing corrective actions to address these specific vulnerabilities and configuration weaknesses shortly after the exit conference for this audit activity, beginning with those items identified as high priority. By the end of August 2005 we will have completed 29 out of 40 of these corrective actions.

Proposed Actions and Completion Date -

- The Secret Service will complete 8 of the remaining corrective actions through implementation of [REDACTED]. The target date for completing this action is December 2005.

- Secret Service managers and technical specialists have researched the remaining three proposed corrective actions and determined that we will not implement these changes. Two of these proposed corrective actions address [REDACTED]. Implementation of this proposed change is not possible due to requirements of the Commercial Off The Shelf (COTS) products used in this environment to provide essential functionality. The other proposed corrective action is to [REDACTED]. Implementing this change will impact legitimate system availability and will require significant staffing to administer. The decision to not implement these proposed changes is based on extensive research by our technical specialists and consideration of risk versus operational needs.

Recommendation #6 – "Examine methods to implement [REDACTED] to ensure that sensitive data is adequately protected."

Appendix B
Management's Response

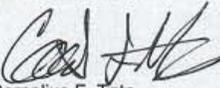
Management Comments – All Secret Service IT systems, including the SSWeb system, operate within our internal environment which is strongly protected from external penetration. All individuals having access to these systems in a production mode must maintain active Top Secret security clearances. All interfaces to systems external to the Secret Service environment are fully encrypted. The cost and operational impact of implementing [REDACTED] is high, and we consider the potential for adverse impact to be very low.

Proposed Actions and Completion Date

- Secret Service management has made a risk based decision, factoring in resource limitations and competing priorities, to not [REDACTED]

I appreciate the opportunity to provide comments on this draft report and to propose these corrective action items. I feel certain these recommendations will serve to improve our already strong security posture on this and other Secret Service systems. The Secret Service Information Resources Management Division is actively working towards completion of the corrective action items I have proposed.

I am available to discuss these comments with you or with the Office of Inspector General, or you may contact Ken Gunderson, Chief of the IT Planning and Policy Staff at 202-406-5649.


Cornelius F. Tate

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	5	12	17	0	17 (100%)	17 (100%)	0
Configuration Management	1	18	19	0	19 (100%)	19 (100%)	0
[REDACTED]	2	0	2	1 (50%)	1 (50%)	2 (100%)	0
[REDACTED]	1	2	3	0	2 (67%)	2 (67%)	1 (33%)
Total	9	32	41	1 (2%)	39 (95%)	40 (98%)	1 (2%)

Source: OIG table based on the results of technical testing and interviews with Secret Service 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 C&A, system impact level determination, NIST SP 800-26 annual assessment, security control costs integrated into the life cycle of the system, assessment of E-authentication risks, specialized security training, and plan of action and milestones (POA&M).¹⁷

Our evaluation of SSWeb shows that the Secret Service has not implemented certain security management practices into its information security program, as required by FISMA.

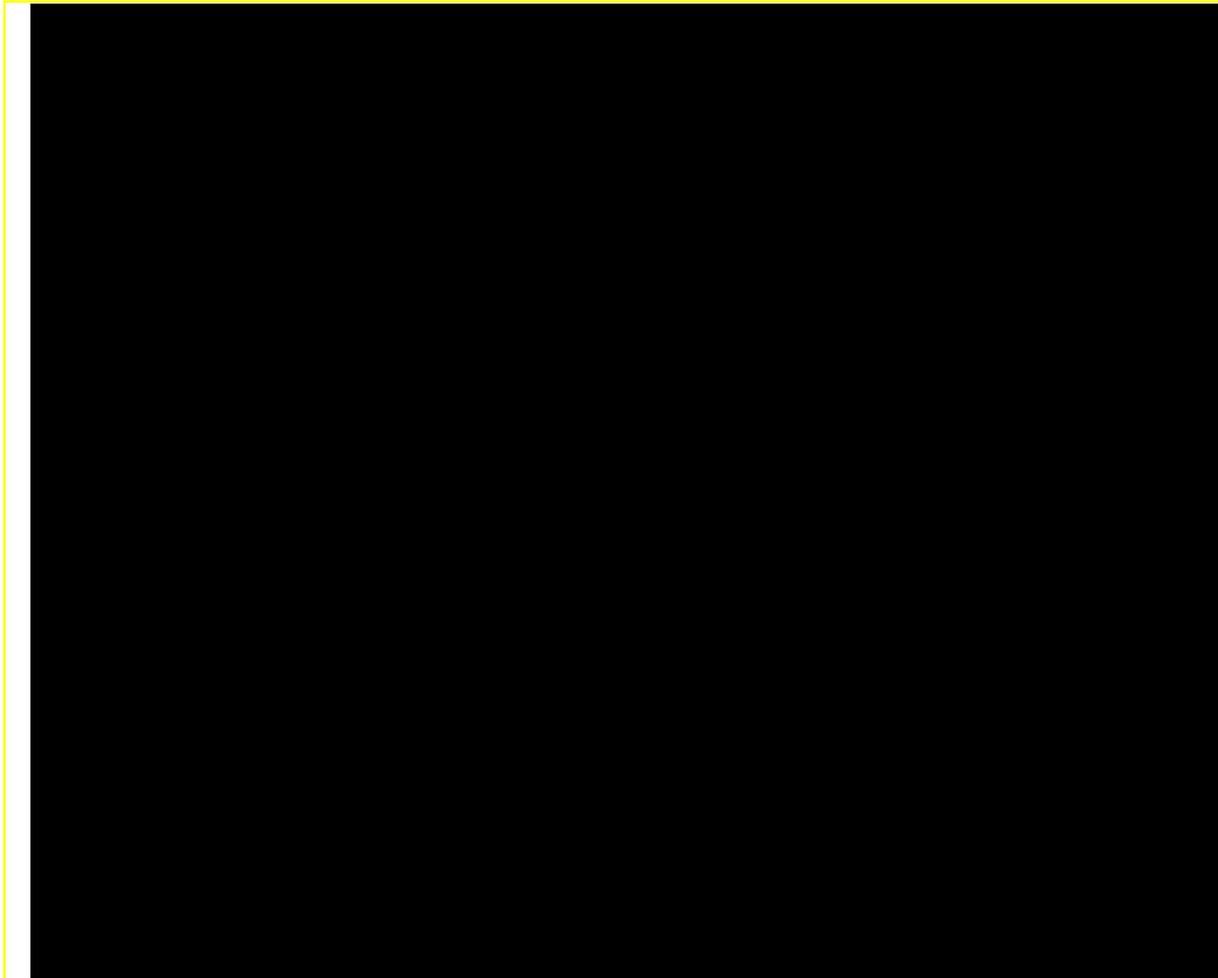
¹⁶ The E-Government Act of 2002 (Public Law 107-347), signed into law on December 17, 2002, recognized the importance of information security to the economic and national security interests of the United States.

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

Table 5: FISMA Compliance Metrics

FISMA Reporting Requirements	Secret Service (SSWeb)	Notes
Does the major application have a complete and current C&A, including a risk assessment and security plan?	Yes	The system underwent an initial C&A in May 2003. While it is undergoing recertification, the system is under an interim authority to operate. The Secret Service decided to recertify SSWeb due to the implementation of a significant system change subsequent to its last C&A.
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 SSWeb would have medium impact on the Secret Service's mission.
Does the major application have a complete and current NIST SP 800-26 annual assessment?	Yes	An SSWeb assessment was completed on October 11, 2004.
Does the assessment indicate that security controls have been tested and evaluated in the last year?	Yes	According to Secret Service officials, SSWeb security controls are reviewed annually and vulnerability scans are conducted every three to six months.
Does the assessment indicate that a contingency plan has been established and tested?	No	The assessment indicates that a system-specific IT contingency plan has not been developed.
Have security control costs been integrated into the life cycle of the system?	No	Although the Secret Service has a separate budget for C&A activities, the component does not track security costs separately. Instead, they are included in the operations and maintenance budget for the system.
Has an assessment of E-Authentication risk been performed for the major application?	Not Applicable	The SSWeb system is only used by Secret Service personnel.
Have the system and database administrators obtained specialized security training?	No	System and database administrators receive the same annual security awareness training that all component personnel receive. Specialized security training is not provided.
Does the major application have any existing POA&Ms?	Yes	As of February 17, 2005, there were POA&Ms entered into the Trusted-Agent FISMA application for two SSWeb weaknesses. However, some of the required system information had not been completed, including the system identifier and the names and contact information for the system manager and system owner.

Source: OIG table based on interviews with Secret Service personnel and analysis of database documentation.



Information Security Audits Division

Edward G. Coleman, Director
Patrick Nadon, Audit Manager
Jason Bakelar, Audit Team Leader
Chris Udoji, Auditor
Chelsea Pickens, Referencer

Advanced Technology Division

Jim Lantzy, Director
Michael Goodman, Security Engineer

Department of Homeland Security

Secretary
Deputy Secretary
Chief of Staff
United States Secret Service, Director
Executive Secretary
General Counsel
Chief Information Officer
Chief Information Security Officer
Public Affairs
United States Secret Service, Chief Information Officer
United States Secret Service, 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.