



Evaluation Report



OIG-CA-09-012

INFORMATION TECHNOLOGY: FMS's Database Management Systems Have Weaknesses in Key Controls

September 29, 2009

Office of
Inspector General

Department of the Treasury

Evaluation Report	4
Results in Brief.....	6
Background	6
Findings and Recommendations	7
Database Patches Were Not Applied in a Timely Manner	7
Recommendation	8
Database Users Were Granted Excessive Privileges	8
Recommendation	8
Account and Password Management Was Not Effective	9
Recommendations.....	10
Security Controls Over a Legacy System Were Inadequate.....	10
Recommendations.....	11

Appendices

Appendix 1: Objectives, Scope, and Methodology	13
Appendix 2: Management Comments	15
Appendix 3: Major Contributors.....	17
Appendix 4: Report Distribution.....	18

Abbreviations

FMS	Financial Management Service
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General

This Page Intentionally Left Blank.

*The Department of the Treasury
Office of Inspector General*

September 29, 2009

David A. Lebryk
Commissioner
Financial Management Service

The purpose of this evaluation was to assess the security of Financial Management Service's (FMS) database management systems. Our overall objective was to determine if FMS had security controls over its database servers, which contain sensitive and vital information, that adequately protect that information against unauthorized access, manipulation, or theft.

To accomplish our objective, we planned to perform a vulnerability assessment and penetration test of FMS's database management systems. Specifically, we planned (1) a discovery scan of FMS's primary network to identify databases installed on the FMS network and to reconcile the results of the scan with FMS's database list, (2) an unauthenticated vulnerability scan of selected databases, (3) an authenticated vulnerability scan of selected databases, and (4) an exploitation of database vulnerabilities. Because of the way in which FMS configures its network, we were not able to execute our plan for discovery scanning and reconciliation with FMS's database list. Instead, we relied on a list of databases provided by FMS and compared it with Treasury's system inventory. We selected databases for unauthenticated and authenticated scanning using a risk-based approach which resulted in a crosscut sample of FMS databases. Furthermore, we performed automated scanning and manual testing of preproduction databases and then manually compared the production and preproduction environments. Since we did not identify any vulnerability that could be exploited, we did not perform any penetration testing of FMS's database management systems.

We performed our fieldwork at FMS's facilities in Hyattsville, Maryland, from December 2008 through February 2009, in

accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspections*.¹ Appendix 1 contains a detailed description of our objective, scope, and methodology.

¹ Pursuant to the Inspector General Reform Act of 2008, the President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency were combined to create the Council of Inspectors General on Integrity and Efficiency.

Results in Brief

We determined that FMS's database management systems had weaknesses in key security controls and identified areas where FMS should take steps to improve the security controls over its database management systems. Our overall findings were as follows:

1. Database patches were not applied in a timely manner.
2. Database users were granted excessive privileges.
3. Account and password management was not effective.
4. Security controls over a legacy system were inadequate.

To address these weaknesses, we made nine recommendations to the Commissioner of FMS. In a written response, FMS stated they had taken corrective actions for each of the findings, including patching or scheduling patches for all production databases, modifying privilege settings, correcting account passwords, and implementing the recommended controls for the legacy system.

Background

FMS provides centralized payment, collection, and reporting services for the federal government. It is staffed by approximately 2,100 career civil servants and disburses more than \$1.6 trillion to more than 100 million individuals via social security and veteran's benefits, income tax refunds, and other federal payments. In addition, it collects more than \$3.11 trillion per year in payments on behalf of the federal government. FMS also provides cash management guidance to federal program agencies and collects delinquent debts owed to the federal government.

To protect the confidentiality, integrity, and availability of sensitive financial data, proper security controls must be in place on FMS's database systems. These controls are necessary to prevent unauthorized access, use, disclosure, disruption, modification, or destruction of data. Missing, insufficient, improper, misconfigured, or poorly designed controls can be exploited by attackers to gain unauthorized access to databases and the information they contain.

Database management systems, which control database operations and security, are complex software programs that require continuous maintenance and patching to ensure protection from vulnerabilities that can allow established security controls to be bypassed. Additionally, because database management systems often have control over the operating system they run on, the host and network security can be compromised when vulnerabilities are present in the database's front-end interface or in the database management system itself.

Findings and Recommendations

Finding 1 **Database Patches Were Not Applied in a Timely Manner**

We determined that FMS did not apply patches to its database management systems in a timely manner. Specifically, we found that 1 Oracle system had not been patched since January 2006, 6 DB2 installations had not been patched since November 2006, 1 DB2 installation had not been patched since April 2005, and 1 Sybase installation had not been patched since January 2007. While FMS uses a preproduction environment for testing patch changes, we found that the preproduction databases also significantly lagged behind the latest released patches.

Treasury Department Publication (TD P) 85-01, *Treasury IT Security Program*, contains department-wide IT security requirements and supporting guidance and requires bureaus to ensure that security patches are tested and installed on a timeline in accordance with the criticality of the patches.

The vulnerabilities resulting from the missing patches identified could be exploited by a determined attacker to disrupt service on FMS's mission-critical database systems. Without these patches, the risk of disruption is increased so that attackers could launch denial of service attacks on FMS database systems or compromise system confidentiality or integrity, thus disrupting access to mission-critical resources.

Recommendation

1. We recommend that the Commissioner of FMS, in accordance with TD P 85-01, ensure that patches are tested and installed in a timely manner, commensurate with the criticality of the patches to FMS's database management systems.

Finding 2 Database Users Were Granted Excessive Privileges

We identified several instances where users were assigned excessive privileges within FMS's database management systems. The privileges granted could allow users to (1) create database procedures that allow execution of malicious code; (2) have administrative authority for the database; and (3) read from and write to operating system files.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 2 (Rev. 2), *Recommended Security Controls for Federal Information Systems*, states the following: "[T]he information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks. The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations, organizational assets, and individuals."

Granting excessive privileges to users can allow users or potential attackers to bypass access controls and compromise data confidentiality, integrity, and availability.

Recommendation

2. We recommend that the Commissioner of FMS ensure that unnecessary database privileges are removed and that going forward the principle of least privilege is enforced.

Finding 3

Account and Password Management Was Not Effective

We discovered that FMS did not implement proper account management, which could lead to the compromise of system security. Specifically, we found six accounts on the mainframe with passwords that were the same as the user names associated with the respective accounts. While five of the accounts were established for batch processing and did not have rights to log onto the system, one of the accounts did have full interactive logon privileges. The FMS database and mainframe administrators responsible for the system were not aware of these issues and stated they would take immediate actions to address them. However, our discovery of these vulnerabilities indicates that steps to detect such issues, including frequent reviews of system accounts, are not regularly performed. Additionally, we found that an Oracle system allowed remote access connections using a method that did not lock out accounts after a number of invalid password attempts.

NIST SP 800-53 Rev. 2 states: "The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts [at an agency defined period, at least annually]." In addition, TD P 85-01 defines the control period for account reviews as at least annually for user accounts and requires that accounts be locked after three invalid attempts in 120 minutes.

When accounts and passwords are not administered effectively, the risk of unauthorized users or attackers gaining access to the system with easily guessed passwords is increased. Furthermore, once that access is gained, attackers could create additional accounts to provide themselves a foothold to further access the system by bypassing other security controls. In addition, when accounts on a remote connection are not locked after a set number of invalid password attempts, attackers can continue guessing passwords without being deterred.

Recommendations

We recommend that the Commissioner of FMS:

3. Ensure that periodic reviews of system accounts are performed to disable or remove unnecessary accounts, as required by TD P 85-01.
4. Ensure that service and application accounts do not have the rights to log on to a system interactively.
5. Ensure that all accounts have strong passwords.
6. Enforce account lockout controls as required by TD P 85-01.

Finding 4 Security Controls Over a Legacy System Were Inadequate

We performed manual testing on one of FMS's legacy production database systems to assess its associated security controls. While this database is no longer used to store business information on new contracts, it is maintained for access and updates to legacy contracts. We found multiple areas where the system did not have adequate security controls, including accounts for users who no longer needed access, database administrator accounts for terminated personnel, end user accounts with assigned administrative privileges, and accounts with no password expiration. Based on our review of the system logs, the system is not frequently used. However, since it is connected to FMS's network, it requires proper security controls.

NIST Federal Information Processing Standard 200, "Minimum Security Requirements for Federal Information and Information Systems," states that federal agencies must meet the minimum security requirements it defines through the use of security controls in accordance with NIST SP 800-53 Rev. 2 which states the following: "[T]he organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts at an agency defined period, at least annually." TD P 85-01 defines the period for account reviews as "at least annually" for user accounts within Treasury.

Failure to properly maintain systems that are connected to a network, including infrequently used legacy systems, can provide an unmonitored avenue of attack to an otherwise secure network. Because of the missing security controls and unsupported status of the legacy system, the data it contains could be compromised.

Recommendations

We recommend that the Commissioner of FMS:

7. Review inactive or idle accounts on the legacy systems and remove unnecessary accounts when access is no longer needed.
8. Enforce account password compliance on legacy systems, as required by TD P 85-01.
9. Review and remove excessive privileges on legacy system.

Management Response

As noted in appendix 2, FMS management stated that they have already implemented corrective actions for the identified weaknesses and will ensure compliance with Treasury and FMS policies.

OIG Comment

We agree that the steps FMS stated they have taken are responsive to the intent of our findings and recommendations.

* * * * *

I would like to extend my appreciation to the Commissioner of FMS and to FMS staff for the cooperation and courtesies extended to my staff during the evaluation. If you have any questions, please contact me at (202) 927-5171 or Gerald Steere, IT Specialist, at (202) 927-6351. Major contributors to this report are listed in appendix 3.

/s/

Tram Jacquelyn Dang
Audit Director

The purpose of this evaluation was to assess the security of database management systems at the Department of the Treasury's Financial Management Service (FMS). Our overall objective was to determine if FMS had security controls over its database servers, which contain sensitive and vital information, that adequately protect that information against unauthorized access, manipulation, or theft.

To accomplish the objective, we planned to perform a vulnerability assessment and penetration testing of FMS's database management systems. Specifically, we planned (1) a discovery scan of FMS's primary network to identify databases installed on the FMS network and to reconcile the results of the scan with FMS's database list, (2) an unauthenticated vulnerability scan of selected databases, (3) an authenticated vulnerability scan of selected databases, and (4) an exploitation of database vulnerabilities. Because of the way in which FMS configures its network, we were not able to execute our plan for discovery scanning and reconciliation with FMS's database list. Instead, we relied on a list of databases provided by FMS and compared it with Treasury's system inventory. We selected databases for unauthenticated and authenticated scanning using a risk-based approach which resulted in crosscut sample of FMS databases. We chose our sample based on the following factors (in descending order of importance):

1. availability of a preproduction databases to scan
2. database criticality or NIST Federal Information Processing Standard 199 rating, which reflects the impact level of the system on the Agency mission--systems with a high impact level were a priority
3. vendor of the database management system in use to provide coverage of each system type used by FMS
4. purpose of the system, as described in FMS's inventory

Furthermore, because of the potential disruption to its daily business functions, FMS management asked us not to scan production databases. We agreed, and as an alternative we performed automated scanning and manual testing of preproduction databases and then manually compared the production and preproduction environments. Since we did not

identify any vulnerability that could be exploited, we did not perform any penetration testing of FMS's database management systems.

We performed our fieldwork at FMS's facilities in Hyattsville, Maryland, from December 2008 through February 2009. We conducted our evaluation in accordance with the Council of the Inspectors General on Integrity and Efficiency's *Quality Standards for Inspections*.

Appendix 2
Management Response



DEPARTMENT OF THE TREASURY
FINANCIAL MANAGEMENT SERVICE
WASHINGTON, D.C. 20227

September 25, 2009

Ms. Tram J. Dang
Director, Office of Information Technology Audit
Office of the Inspector General
740 15th Street, NW
Suite 600
Washington, DC 20220

Dear Ms. Dang,

Thank you for the opportunity to comment on the September 2009 draft evaluation report titled "FMS's Database Management Systems Have Weaknesses in Key Controls."

We are pleased to report the following corrective actions:

Finding 1. Database Patches Were Not Applied in a Timely Manner

All FMS production database have either been patched or are scheduled to be patched. We will ensure that patches are completed in accordance with Treasury and FMS policy.

Finding 2. Database Users Were Granted Excessive Privileges

The implicit schema privileges have been corrected. We removed the IBM supplied sample database which encompassed the sited elements. The DB2 catalog table privileges have been modified. [REDACTED - FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)]
[REDACTED - FOIA EXEMPTION 2, 5 U.S.C. §552]

We will enforce the principle of least privilege, and comply with TD P 85-01 and FMS policy.

Finding 3. Account and Password Management Was Not Effective

We corrected the six accounts and associated passwords:
[REDACTED - FOIA EXEMPTION 2, 5 U.S.C. §552(b)(2)]

Appendix 2
Management Response

Page 2 - Ms. Tram J. Dang

We will continue to perform periodic review of system accounts to disable or remove accounts and perform password management as required by TD P 85-01.

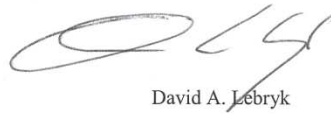
Finding 4. Security Controls Over a Legacy System Were Inadequate

FMS implemented all the recommendations regarding the security controls over a legacy system finding.

We will continue to enforce account password compliance as required by TD P 85-01.

When the final audit report is issued, we will determine and track any outstanding corrective actions via the FMS Plan of Action and Milestone process in the Trusted Agent FISMA repository. The corrective actions will also be tracked in FMS's Audit Monitoring System, and the Department's Joint Audit Management Enterprise System.

Sincerely,



David A. Lebryk

Office of IT Audits

Tram J. Dang, Director
Susan I. Miller, IT Audit Manager
Gerald J. Steere, IT Specialist (Lead)
Abdirahman M. Salah, IT Specialist
Jane E. Lee, IT Specialist
Larissa Klimpel, IT Specialist
Shiela Michel, Referencer

Financial Management Service

Chief Information Officer

Department of the Treasury

Office of Accounting and Internal Control
Office of Strategic Planning and Performance Management
Office of the Chief Information Officer

Office of Management and Budget

Office of Inspector General Budget Examiner