Security Over Databases Could Be Enhanced to Ensure Taxpayer Data Are Protected

May 4, 2011

Reference Number: 2011-20-044

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Redaction Legend

2(f) = Risk Circumvention of Agency Regulation or Statute

SECURITY OVER DATABASES COULD BE ENHANCED TO ENSURE TAXPAYER DATA ARE PROTECTED

Highlights

Final Report issued on May 4, 2011

Highlights of Reference Number: 2011-20-044 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

The Internal Revenue Service (IRS) uses more than 2,200 databases to manage and process its taxpayer data. Databases are increasingly being targeted by attackers. When the right degree of security diligence is not applied to databases, disgruntled insiders or malicious outsiders can exploit security weaknesses over databases and may gain unauthorized access to taxpayer data, resulting in identity theft or fraud.

WHY TIGTA DID THE AUDIT

This review was included in TIGTA's Fiscal Year 2010 Annual Audit Plan and is part of our statutory requirements to annually review the adequacy and security of IRS information technology. This audit also addresses the major management challenge of Security of the IRS. The overall objective of this review was to determine whether the IRS adequately configured databases operating in its non-mainframe production environment to properly secure taxpayer data.

WHAT TIGTA FOUND

TIGTA found that non-mainframe databases containing taxpayer data were not always configured in a secure manner and that databases were running out-of-date software that no longer received security patches and other vendor support.

In addition, the IRS had not fully implemented its plans to complete vulnerability scans of databases within its enterprise. Also, the IRS purchased a database vulnerability scanning and compliance assessment tool without the completion of adequate product evaluation and testing. As a result, the IRS spent more than $1.1 million in software licenses and support costs for a tool that was not fully implemented.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer ensure: 1) the security vulnerabilities identified on databases are remediated; 2) explicit management approvals are included in the database configuration building process; 3) a strategic plan is developed to address outdated database versions; 4) outdated databases are upgraded, planned to be migrated to newer versions, or properly approved to deviate from existing standards; 5) database vulnerability scans are conducted as required by policies; 6) database vulnerability scans test all high- and medium-risk configuration settings; and 7) a thorough technical product evaluation is consistently conducted and documented for the purchase of future software products.

In its response to the report, the IRS agreed with TIGTA's recommendations. The IRS plans to: 1) develop a strategy to ensure vulnerabilities are documented; 2) identify appropriate organizations to develop a management approval process to be used in the database build and configuration change processes; 3) develop a strategic plan for obsolescence of technology, including database version control; 4) develop a migration plan to upgrade database software to supported versions; 5) establish a process for conducting monthly scans of databases; 6) establish a Memorandum of Understanding to ensure database vulnerability scans are conducted with the privileges necessary to test all high- and medium-risk database configuration settings; and 7) create\designate a location to ensure all Product Evaluation and Selection and testing documentation is accessible from a centralized location.

The IRS disagreed with TIGTA's $1.1 million outcome measure related to the licensing of the IRS vulnerability scanning tool. TIGTA maintains the appropriateness of the measure.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

May 4, 2011

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

Michael R. Phillips

FROM: Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Security Over Databases Could Be Enhanced to Ensure Taxpayer Data Are Protected (Audit # 201020014)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) adequately configured databases operating in its non-mainframe production environment to properly secure taxpayer data. This review was included in the Treasury Inspector General for Tax Administration Fiscal Year 2010 Annual Audit Plan and is part of our statutory requirements to annually review the adequacy and security of IRS information technology. This audit also addresses the major management challenge of Security of the IRS.

Management's complete response to the draft report is included as Appendix V.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-5894.

Table of Contents

Abbreviations

ACIO	Assistant Chief Information Officer
DBMS	Database Management System
IBM	International Business Machines
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
MITS	Modernization and Information Technology Services
RDBMS	Relational Database Management System
SQL	Standard Query Language
TIGTA	Treasury Inspector General for Tax Administration

Background

Data are often referred to as the "crown jewels" of an organization because data represent the organization's core business purpose. Data can consist of customer records, trade secrets, business partners, or any other highly sensitive information. For the most part, data in its electronic form are often stored in a database management system (DBMS), which uses standard methods for accepting and managing incoming data, cataloging and storing the data, and providing ways for the data to be modified or extracted by users or other programs. Databases are increasingly being targeted by attackers. A 2009 report[1] on data breaches cited that 30 percent of all known security breaches were against databases. This trend was particularly disturbing because when a database was breached, 75 percent of the records were compromised.

The Internal Revenue Service (IRS) employs almost 100,000 employees and operates more than 200 applications to administer our Nation's tax laws and regulations. The IRS relies on more than 2,200 databases to manage and process data, such as personally identifiable taxpayer information and sensitive financial/tax information, on its computer systems. Two database management software products are primarily used in the IRS's non-mainframe computer processing environment: Oracle and Microsoft Standard Query Language (SQL) Server.

The Treasury Inspector General for Tax Administration (TIGTA) previously issued an audit report on database security[2] in which we reported that the prescribed IRS database security policies adequately aligned with Federal Government guidelines and best practices. However, at that time, we found databases did not fully comply with IRS policy because standard database security configurations were poorly communicated, security roles and responsibilities were not assigned or carried out, and tests to detect noncompliance were inadequate.

Our current database security review was performed at the IRS National Headquarters in New Carrollton, Maryland, in the Office of Cybersecurity within the Chief Technology Officer's Modernization and Information Technology Services (MITS) organization during the period January through October 2010. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

---

[1] *2009 Data Breach Investigations Report*, conducted by the Verizon business risk team.
[2] *Standard Database Security Configurations Are Adequate, Although Much Work Is Needed to Ensure Proper Implementation* (Reference Number 2007-20-129, dated August 22, 2007).

Results of Review

Production Environment Databases Containing Taxpayer Data Were Not Configured in a Secure Manner

The Internal Revenue Manual (IRM) 10.8.4, Relational Database Management System (RDBMS) Security Configurations, provides general security standards for databases and requires that all DBMS installations operated by the IRS shall comply with the provisions of this IRM. The IRM states that all requirements detailed in this policy apply to all IRS databases regardless of vendor product or version. IRS requirements specific to Oracle Database Server and Microsoft SQL Server are covered in individual exhibits.

We used database vulnerability assessment software to conduct remote scans of the primary databases for 13 applications supporting critical tax administration business processes. Of these 13 applications, **********2(f)**********. We tailored the scan policies to reflect security configurations set forth by the IRM and found high- and medium-risk vulnerabilities, as classified by the scanning tool, in each of the 13 databases in the following security vulnerability categories:

- The account management control area includes management of individual user account profiles. Vulnerabilities identified in this area included the existence of default or generic accounts and inappropriate password settings.
- The privilege management control area includes the management of user access to sensitive files and utilities on the database. Vulnerabilities identified in this area included management of powerful administrative privileges that should be assigned according to specific job functions.
- The operating system protection control area includes management of access to sensitive system files and program code. Vulnerabilities in this area included inappropriate user access to system source code and source code that is not protected by encryption.

Figure 1 presents the security vulnerabilities identified in each of the 13 database systems on the applications reviewed.

Figure 1: Number of Security Vulnerabilities Identified In Each Security Vulnerability Category by Application

IRS Application	Database Security Vulnerability Category		
	Account Management	Privilege Management	Operating System Protection
2(f)	3	2	2
2(f)	4	7	0
2(f)	7	5	3
2(f)	3	4	2
2(f)	3	3	0
2(f)	3	3	1
2(f)	10	4	1
2(f)	5	3	0
2(f)	5	5	0
2(f)	4	10	3
2(f)	6	4	3
2(f)	3	3	2
2(f)	5	5	2
Totals	61	58	19

Source: TIGTA analysis of automated scan results.

In several cases, the databases contained the default settings from the previous software installation or upgrade. When the results of the scans were presented to IRS personnel responsible for management of the databases, management advised us that some of the databases were built prior to the governing IRM database configuration policy and some of the databases were misconfigured as a result of oversight. In addition, management cited one possible systemic cause being that the database scanning technology has not yet been fully deployed across its database environment, which would have allowed database administrators to regularly scan and detect database parameter misconfigurations.

We also found the IRS has three separate groups within the MITS organization with roles in the non-mainframe database administration environment.

1. The Applications Development office has responsibility for the initial database design and development and issues transmittals authorizing changes to the database software when necessary.
2. Database administrators in the Enterprise Operations office are responsible for implementing the changes described in the transmittals.
3. The Cybersecurity office is responsible for monitoring the configuration of database software and identifying inconsistencies.

We believe the lack of database configuration management in the IRS is a direct result of database configuration management being a loosely shared responsibility across several MITS organization offices. Further, our discussions with IRS officials verified that no single office has the responsibility to ensure IRS databases are configured appropriately, which highlights the need for an approval process for configuring secure settings on databases.

In our prior audit, we recommended that the IRS correct database security control weaknesses identified at that time. The IRS agreed with this recommendation and stated that each of the database security control weaknesses that the TIGTA identified would be included in the corrective plans of actions and milestones document. However, we reviewed the plans of actions and milestones documents from Fiscal Years 2007 and 2008 for those systems tested in the previous audit and could not determine if the weaknesses were entered, addressed, or closed. As a result, we have no assurance that the previous security weaknesses were corrected.

Exploitation of the security vulnerabilities on databases could result in the unauthorized access to taxpayer information and could ultimately result in identity theft or fraud. Also, if these systems were to be corrupted or disabled, the IRS tax processing system could be adversely affected.

Recommendations

Recommendation 1: The Chief Technology Officer should ensure the vulnerabilities identified in the 13 systems scanned during the current audit, as well as any other high-risk security vulnerabilities identified through automated scans and manual reviews, are remediated. Otherwise, a properly approved deviation should be on file to justify departure from stated standards.

> ***Management's Response:*** The IRS agreed with this recommendation. The Assistant Chief Information Officer, Cybersecurity, in partnership with the Enterprise Operations organization, plans to 1) ensure the vulnerabilities identified in the 13 systems scanned during the current audit are remediated or documented in a plan of actions and milestones and 2) develop an Enterprise process and remediation strategy to ensure that

high-risk vulnerabilities identified during periodic database scans are documented in a plan of actions and milestones.

Recommendation 2: The Chief Technology Officer should ensure explicit management approvals are included in the IRS database configuration building process and the IRS database configuration change process to ensure that databases are properly configured according to the standards cited in IRM 10.8.4, RDBMS Security Configurations.

Management's Response: The IRS agreed with this recommendation. The IRS will identify appropriate organizations to develop an explicit management approval process to be used in the database build and configuration change processes to ensure the databases are properly configured.

Production Environment Databases Were Running Out-of-Date Database Software That No Longer Receives Security Patches and Other Vendor Support

IRM 10.8.4, RDBMS Security Configurations, states that each organization responsible for the management of a database shall ensure that unsupported DBMS software is removed or upgraded to a supported version prior to a vendor dropping support and shall ensure a formal migration plan exists for removing or upgrading the DBMS prior to the date the vendor drops security patch support. Not having vendor support means the databases are not patched by vendors to address newly discovered security vulnerabilities and are vulnerable to attack. As a follow-on requirement to protect the DBMS environment, the IRM also states that database administrators shall ensure the DBMS patch level is current.

Our analysis of a scan conducted by the IRS in the first quarter of Fiscal Year 2010 showed that, of 1,879 databases within the IRS's production computing environment, 326 (48 percent) of 676 Oracle databases and 448 (37 percent) of 1,203 SQL databases were running versions of database software that were no longer supported by the vendor. Figure 2 presents the Oracle and SQL databases reviewed and which versions are no longer supported by the vendors.

Figure 2: Database Systems by Version

Software by Version (out of support versions are in bold)	The Number of Database Servers in the IRS Production Environment	Percentage of Unsupported Versions Within Each Database System
Oracle 8i	***173***	***26%***
Oracle 9i	***153***	***23%***
Oracle 10g	*343*	*Supported*
Oracle 11g	*7*	*Supported*
Oracle Total	***676***	
SQL 2000	***448***	***37%***
SQL 2005	*754*	*Supported*
SQL 2008	*1*	*Supported*
SQL Total	***1,203***	
Total Database Servers	***1,879***	

Source: TIGTA analysis of automated scan results.

The overall percentage of unsupported versions for the Oracle database would have been significantly higher because the Oracle 10g version category includes earlier releases that are no longer supported by the vendor. However, due to limitations of the software used by the IRS to collect the data, our analysis was restricted to only the version level (e.g., 10g) and not the more granular version and release level (e.g., 10g, Release 10.2.0.2).

In response to our requests for strategic database plans to address outdated database versions, IRS management did not provide any documentation and informed us that while informal discussions had been held within the Enterprise Operations office regarding the need to migrate to currently supported versions, no enterprise-wide actions have been taken. As mentioned in the previous finding, we believe the lack of strategic database management in the IRS is a direct result of database management being a shared responsibility across several IRS offices, including the MITS organization's Enterprise Operations, Applications Development, and Cybersecurity offices, as well as IRS business program management.

When outdated and unsupported database versions are used, the organization is susceptible to performance and security weaknesses inherent to older versions. As shown in Figure 3, we found that 6 of the 13 database systems we selected for detailed testing did not have the current critical patch updates or service pack installed. The *****2(f)**********are potentially at

risk for having between 20 and 193 security vulnerabilities, depending on when the latest patch had been applied. The ***2(f)********** did not have the current patches applied was at risk for 16 security vulnerabilities.

Figure 3: Potential Vulnerabilities in Database Systems With Out-of-Date Software

	IRS Application	Database Version	Last Patch Applied	Number of Potential Security Vulnerabilities Since Last Patch
1	*****2(f)*****	Oracle 10g	Critical patch update released in July 2009 applied on November 1, 2009.	30
2	*****2(f)*****	Oracle 9i	Critical patch update released in January 2010 applied on February 28, 2010.	20
3	*****2(f)*****	Oracle 10g 10.1.0.4	Critical patch update released in April 2007 applied on June 3, 2007.	193
4	*****2(f)*****	Oracle 10g 10.2.0.2	Critical patch update released in October 2007 applied on October 27, 2007.	146
5	*****2(f)*****	Oracle 10g 10.2.0.2	Critical patch update released in October 2007 applied on December 9, 2007.	146
6	*****2(f)*****	SQL 2000	Service Pack 4 8.00.2055 released in February 2009.	16

Source: TIGTA analysis of automated scan results.

A critical patch update ***2(f)****** and a service pack **********2(f)****** are bundles of software fixes or patches released to provide corrections to weaknesses in operating systems or software products. **********2(f)********** **********2(f)********** ******2(f)**********. Both critical patch updates and service packs address security weaknesses that compromise:

- Data confidentiality – An attacker is able to view information that he or she should be prevented from viewing.
- Data integrity – An attacker is able to modify information that he or she should be prevented from modifying.

- System availability – An attacker is able to disrupt legitimate use of or access to a system.

The IRS acknowledged that these database systems were not running vendor supported software and, therefore, could not be patched to current levels. The IRS did not provide evidence to support its rationale for not updating these sample systems to a current DBMS or that it had planned upgrades to the systems. However, a Cybersecurity office executive shared with us an email from another MITS organization executive on some problems encountered after they upgraded the database version of one of the systems we reviewed. The email indicated that the application became unstable and was intermittently operational and nonoperational. To address the problems, they had engaged the vendor and database experts.

The IRS advised us that costs to upgrade its database software to currently supported versions are difficult to estimate but would primarily consist of the labor costs of full-time equivalents[3] to implement needed modifications to existing production applications to achieve compatibility with the newer versions of database software. We believe the IRS could be wasting funds by not upgrading or patching its database software that is covered by its enterprise software licenses.

Recommendations

Recommendation 3: The Chief Technology Officer should ensure an enterprise-wide strategic plan is developed to address the outdated database version management issues prevalent in the IRS production environment.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS Enterprise Services organization will coordinate with the affected stakeholders to develop a strategic plan for obsolescence of technology to include database version control.

Recommendation 4: The Chief Technology Officer should ensure databases with out-of-support DBMS software are upgraded to currently supported versions within a reasonable time period. For those systems where upgrading the database software or implementing security patches have been determined to be dangerous to the stability of the system, a migration plan should be developed and a properly approved deviation should be on file to justify departure from stated standards.

> ***Management's Response:*** The IRS agreed with this recommendation. The Assistant Chief Information Officer, Enterprise Services, will coordinate with affected stakeholders to develop a migration plan to upgrade the database management software to currently supported versions. An inventory of all servers with databases on them and

[3] A measure of labor hours in which 1 full-time equivalent is equal to 8 hours multiplied by the number of compensable days in a particular fiscal year. For Fiscal Year 2010, 1 full-time equivalent is equal to 2,088 staff hours.

their associated software version will be created. Enterprise Services will then outline steps to take to address the versions older than n-1 and install updates accordingly. Enterprise Services will establish on ongoing monitoring of servers and institutionalize a process to keep software current.

Complete Vulnerability Scans of Databases at the Frequency Required by Agency Standards Were Not Being Conducted

The National Institute of Standards and Technology's Special Publication 800-39, *Integrated Enterprise-Wide Risk Management: Organization, Mission, and Information System View*, emphasizes the practice of continuous monitoring. It states that a well-designed and well-managed continuous monitoring program can effectively transform an otherwise static security control assessment and risk determination process into a dynamic process that provides essential, near real-time security status information to appropriate organizational officials. This information can be used to maintain a current understanding of the security state and risk posture of the organization and facilitate appropriate risk mitigation actions.

As of October 1, 2009, IRM 10.8.1, Information Technology Security – Policy and Guidance, requires the IRS to conduct monthly vulnerability scans of its systems that have a high or moderate rating, based on the Federal Information Processing Standards Publication 199[4] rating of systems. Prior to this date, the IRM required the IRS to scan these systems on a quarterly basis. Also, IRM 10.8.4, RDBMS Security Configurations, requires that all DBMS installations operated by the IRS, or operated by an IRS contractor on behalf of the IRS, shall comply with the provisions of this IRM. The IRM states that all requirements detailed in this policy apply to all IRS databases, regardless of vendor product or version. IRS requirements specific to Oracle Database Server and Microsoft SQL Server are covered in individual exhibits.

In our August 2007 report, we recommended the Chief Information Officer develop an implementation plan for the organization's database compliance assessment tool that adequately defines the scope of the databases tested, the requirements to be tested, the timing of tests, and the schedule for implementation. The IRS agreed with this recommendation and stated that it would implement a process for detecting noncompliance with database security requirements. In June 2007, the IRS purchased the Application Security's DbProtect AppDetective as its database vulnerability scanning and compliance assessment tool.

In our current review, we found that the implementation plan had been developed but had not been fully implemented. IRS management explained that they experienced significant technical

[4] Federal Information Processing Standards Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*, provides standards to be used by all Federal agencies to categorize all information and information systems collected or maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to a range of risk levels.

difficulties in implementing DbProtect AppDetective as a regular recurring scanning tool for the IRS's database environment. Management stated that the difficulties were due to the many different implementations of the database software across the environment. During the period April 2009 to February 2010, we found that the IRS conducted vulnerability scans of only 79 of its 1,879 non-mainframe databases. These scans were ad hoc in nature and not part of a formal database compliance testing program.

Further, when we reviewed the IRS scanning policy against which databases are tested to ensure it included tests for controls provided in the IRM standard database configurations, we found the IRS scanning policy did not include checks for 42 Oracle and 26 SQL high- and medium-risk security settings. We believe the IRS database scanning policy omitted these high- and medium-risk tests because the necessary access privileges had not been established to allow the tool to scan these sensitive security settings. Instead, the IRS relied on the results provided by the limited scans. The IRS Cybersecurity office recently began drafting procedures for conducting vulnerability scans of its computer environment. These procedures include regularly scheduled scans and ad hoc scans that systems stakeholders may request whenever needed.

In its MITS organization Cybersecurity Operations: Technical Roadmap, dated August 2007, the IRS stated:

> *By exploiting un-patched and un-remediated vulnerabilities in our databases, disgruntled insiders or malicious outsiders may gain unauthorized access to our most sensitive information. Database vulnerabilities exist for several reasons including technological weaknesses, poor security-control implementation, lack of training, and absences of effective oversight. Routine quarterly scans to detect and correct database vulnerabilities and misconfigurations are essential to ensuring the right degree of security diligence is being applied to IRS databases.*

By not having regular and complete monthly database scans checking for key required parameter settings, the IRS has not met this goal of ensuring security diligence is applied to IRS databases and is not proactively identifying insecure databases within its computing environment.

As a secondary issue on the database vulnerability scanning tool, we also found that the IRS had purchased the DbProtect AppDetective database vulnerability scanning tool without completing adequate product evaluation and testing. The National Institute of Standards and Technology's Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, lists the following questions that should be posed by an organization prior to the selection of information security products.

- Have policies been developed for the use of products as appropriate?
- Have operational issues such as daily operation, maintenance, contingency planning, awareness and training, and documentation been considered?
- Have security requirements been identified and compared against product specifications?

- Have total life cycle support, ease-of-use, scalability, and interoperability requirements been determined?
- Have test requirements for acceptance and integration testing and configuration management been developed?

Similarly, the Control Objectives for Information and Related Technology[5] sets forth control objectives for the process of acquiring and maintaining application software. This specific guidance recommends mapping business requirements to design specifications for software acquisition and taking into account the organization's technological direction and information architecture. The Control Objectives for Information and Related Technology recommends having management approve the design specifications to ensure that the high-level design responds to the requirements.

When the IRS Cybersecurity organization licensed Application Security's DbProtect AppDetective database vulnerability assessment software tool in June 2007, the IRS had planned to use the tool to conduct regularly scheduled enterprise-wide scans of IRS databases. As mentioned previously, this scanning tool was part of the IRS's corrective actions from our prior review.

In our current review, however, we determined the DbProtect AppDetective scanning tool was never fully implemented. In addition to the technical difficulty in implementing the tool, IRS management stated they would have incurred significant additional licensing costs to license the tool for their International Business Machines (IBM) mainframe database environment. IRS management decided upon an alternative action to license another database scanning tool in May 2010, IBM's Guardium, to replace the DbProtect AppDetective database scanning tool. The IRS justified the alternative procurement stating that Guardium would provide a cost-effective vulnerability assessment for the mainframe database environment and real-time monitoring of database servers to enable the IRS to identify any changes made to database configurations.

When we requested DbProtect AppDetective product evaluation documentation, the IRS could not provide any product evaluation or control testing documentation justifying its licensing of the DbProtect AppDetective. We believe a technical evaluation of the product's ability to satisfy IRS requirements, and control testing thereof, would have informed the IRS of the actual costs of implementing the DbProtect AppDetective scanning tool across all database products, including its mainframe database environment. Without an adequate product evaluation of the DbProtect AppDetective tool, the IRS was not fully aware of the tool's limitations, including its

[5] The Control Objectives for Information and Related Technology is a complete, internationally accepted process framework for information technology that supports business and information technology management in their definition and achievement of business goals and related information technology goals by providing a comprehensive information technology governance, management, control, and assurance model.

applicability to the IBM mainframe environment. Consequently, the IRS spent more than $1.1 million in software licenses and support costs for a tool that was not fully implemented.

Recommendations

Recommendation 5: The Chief Technology Officer should ensure vulnerability scans of IRS databases are conducted in the frequency required by the IRM and any security weakness identified should be corrected or approved for deviation from security policies.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS Cybersecurity organization's Penetration Testing and Code Analysis group will establish a formal process for conducting monthly agency-wide scans of IRS databases. In addition, the Penetration Testing and Code Analysis group will transmit identified weaknesses to the stakeholders, and the System/Program Owner and Information Systems Security Officer will formulate appropriate remediation actions.

Recommendation 6: The Chief Technology Officer should ensure database vulnerability scans are conducted with the access privileges necessary to test all high- and medium-risk database configuration settings.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS Cybersecurity organization's Penetration Testing and Code Analysis group will establish a Memorandum of Understanding with the Enterprise Operations organization and Systems Owners to ensure database vulnerability scans are conducted with the access privileges necessary to test all high- and medium-risk database configuration settings.

Recommendation 7: The Chief Technology Officer should ensure a thorough technical product evaluation and testing of key functional requirements is consistently conducted and documented for the acquisition of software products.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS has established Product Selection Guidance and has controls in place for technical product evaluation and testing of key functional requirements. The Change Control governance process ensures thorough product evaluation and testing has been completed prior to product acquisition following the Product Evaluation and Selection Guidance. In addition, a centralized repository exists documenting all change requests and their disposition. The IRS can create/designate a location to ensure all Product Evaluation and Selection and testing documentation is stored or accessible from a centralized location.
>
> ***Office of Audit Comment:*** IRS did not agree with the Outcome Measure (see Appendix IV) relating to the purchase of the DbProtect AppDetective software tool. In its response, the IRS stated that DbProtect AppDetective was the best available tool at the time of the purchase, met the immediate needs for a database vulnerability scanning capability in response to TIGTA's audit recommendation, and was put into production

use. The IRS also stated that ongoing costs and business requirements were the main reasons for changing to a new database scanning tool. We disagree that the tool was purchased in response to an audit recommendation. The IRS purchased DbProtect AppDetective in June 2007, and the previous audit report was issued in August 2007. In addition, the report contained a recommendation that IRS develop a formal implementation plan for the tool, which IRS agreed to but never completed. We also disagree that DbProtect AppDetective was put into production use. As noted in the finding, the IRS conducted scans of only 79 of its 1,879 non-mainframe databases from April 2009 to February 2010. After preliminary discussions with IRS management, the outcome measure was adjusted to reflect this limited use of the tool. No further adjustment to Appendix IV was made.

Other Issues From the Prior Audit Report Were Adequately Addressed

As part of this review, we followed up on the IRS's corrective actions to the seven recommendations from our prior report and determined that corrective actions for all seven recommendations were taken and each of the corrective actions was reported as closed on the Joint Audit Management Enterprise System.[6] Specifically, our followup work determined that the IRS had:

- Adequately publicized the standard database configurations.
- Ensured internal web sites referred to the Cybersecurity office's web site for current security configurations.
- Ensured security administration responsibilities were properly assigned.
- Ensured employees are aware of their database security responsibilities.
- Ensured that security testing evaluates compliance with standard database security configurations.

However, we identified database weaknesses had not been adequately addressed prior to their closure on the Joint Audit Management Enterprise System for two recommendations.

- The Chief Information Officer should ensure the database security control weaknesses we identified are corrected.
- The Chief Information Officer should develop an implementation plan for the organization's database compliance assessment tool that adequately defines the scope of

[6] The system used by the Department of the Treasury to record and monitor audit findings and corrective actions taken to address findings from audit reports.

the databases tested, the requirements to be tested, the timing of the tests, and the schedule for implementation.

Both of these two remaining corrective actions are mentioned within the context of the current findings identified during the course of this review.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS adequately configured databases operating in its non-mainframe production environment to properly secure taxpayer data. We also assessed the IRS's progress in implementing corrective actions reported during our prior audit.[1]

We selected an initial sample of 20 primary production databases for detailed testing from the total IRS environment of 226 applications.[2] We used a judgmental sample to ensure we conducted detailed testing on applications that are considered high impact in the IRS. These databases were selected according to the following criteria in order of importance: applications classified as major applications according to criteria provided by Federal Information Processing Standards Publication 199, applications that process Sensitive but Unclassified data, and applications that use Oracle or Microsoft SQL as the database management software. To accomplish our objective, we:

I. Assessed the adequacy of IRS database strategic planning and database security policies.

   A. Obtained and reviewed the IRS's strategic database planning documents regarding DBMS program products and versions. We commented on the reasonableness of the plan in terms of the number of supported program products, plans to migrate from out-of-support products, and plans to roll out newer versions of vendor supported program products.

   B. Reviewed assigned roles and responsibilities for database security (e.g., who develops configuration policy, who implements configuration policy, and who monitors compliance with database configuration policy) to ensure roles and responsibilities are adequately defined. We verified that duties to implement configuration policy and monitor compliance with database configuration policy are appropriately segregated.

   C. Determined, as a followup to our prior audit, whether database administrators are assigned for the SQL and Oracle databases that were included in our current sample for detailed testing. We also determined if security specialist roles are assigned for the databases that were included in our sample for detailed testing.

---

[1] *Standard Database Security Configurations Are Adequate, Although Much Work Is Needed to Ensure Proper Implementation* (Reference Number 2007-20-129, dated August 22, 2007).

[2] Seven of the 20 databases were removed from the sample due to technical issues experienced when conducting the scans.

D. Validated, as a followup to our prior audit, processes in place to ensure employees are aware of their database security responsibilities.

E. Conducted an updated review of the Oracle and SQL database policies that changed since our last review.

F. Verified whether approved IRS IRM database policy exists for versions of database management products executing in the IRS non-mainframe production environment.

G. Interviewed database management personnel to determine reasons for any variance from the standards.

II. Assessed the adequacy of IRS configuration management processes over its databases.

A. Reviewed the inventory management, version management, database configuration parameters, database configuration parameter change control, and patch management processes.

B. Interviewed database management personnel to determine reasons for any variance from the standards.

III. Assessed the effectiveness of IRS database identification and authentication controls.

A. Reviewed the authentication method that the IRS chose for installation of its database software to ensure the authentication method adheres to IRS minimum security requirements in IRM 10.8.4, RDBMS Security Configurations.

B. Determined whether the recommended authentication methods were being used.

C. Interviewed database management personnel to determine reasons for any variance from the standards.

IV. Determined whether adequate database access and authorization controls were in place by using the DbProtect AppDetective scanning tool to verify security settings.

A. Compared IRS IRM database security policies to the IRS's customized DbProtect AppDetective policy to verify existence of and agreement for key parameter settings.

B. Conducted DbProtect AppDetective scans in the control areas of account management, privilege management, trusted link management, operating system protection, network access, and remote management for the sample databases to ensure the database parameters and settings were appropriate, according to guidance provided in IRM 10.8.4, RDBMS Security Configurations.

C. Interviewed database management personnel to determine reasons for any variance from the standards.

V. Assessed the adequacy of IRS vulnerability management over its databases.

A. Verified, as a followup to our prior audit, whether the database security control weaknesses that TIGTA identified were corrected.

B. Verified, as a followup to our prior audit, whether annual security testing evaluates compliance with standard database security configurations.

C. Verified, as a followup to our prior audit, whether the IRS had established an appropriate database compliance testing process, including evaluating the database scanning tool used and defining the scope of the databases tested, the requirements to be tested, the timing of the tests, and the schedule for implementation.

D. Determined the actual frequency of database scans for a recent 6-month period.

E. Determined whether high- and medium-priority database vulnerabilities were properly managed and mitigated in a timely manner for a recent 3-month period.

F. Interviewed database management personnel to determine reasons for any variance from the standards. If applicable, we obtained and reviewed any waiver or other documentation justifying the variance from standards.

VI. Assessed the adequacy of database security awareness and training.

A. Reviewed and verified, as a followup to our prior audit, whether security documentation is publicized to Database Administrators and Systems Administrators.

B. Verified, as a followup to our prior audit, whether the IRS Cybersecurity office's intranet site refers to the current security configurations.

C. Reviewed a list of Database Administrators and associated specialized database security training they have received over the last 3 to 5 years.

D. Interviewed database management personnel to determine reasons for any variance from the standards.

Internal controls methodology

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined the following internal controls were relevant to our audit objective: IRS Enterprise Operations policies and procedures for managing the configuration of its database systems, including patch and vulnerability management. We evaluated these controls by conducting vulnerability scans of the database systems, comparing the results of those scans to standards established by the IRS in its IRM, and also interviewing management responsible for those systems.

Appendix II

Major Contributors to This Report

Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Carol Taylor, Audit Manager
Myron Gulley, Lead Auditor
Louis Lee, Senior Auditor
Elton Jewell, Information Technology Specialist
Monique Queen, Information Technology Specialist

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaison: Director, Risk Management OS:CTO:SP:RM

Appendix IV

Outcome Measure

This appendix presents detailed information on the measurable impact that our recommended corrective action will have on tax administration. This benefit will be incorporated into our Semiannual Report to Congress.

Type and Value of Outcome Measure:

Inefficient Use of Resources – Actual; $1,113,850 ($1,160,260 * 96 percent) (see page 9).

Methodology Used to Measure the Reported Benefit:

In June 2007, the IRS purchased the license for the DbProtect AppDetective vulnerability scanning tool for $1,160,260 to address the need for formally scheduled scans of IRS databases to ensure appropriate security configurations are maintained. However, we determined the tool was never fully implemented. In addition to significant technical difficulty in implementing the tool, IRS management stated that it would have incurred significant additional costs to license the tool for its IBM mainframe database environment. The IRS then decided to pursue the purchase of another tool that could be implemented across its entire computing environment. We noted that IRS used the tool to complete scans for only 79 (4 percent) of the 1,879 databases within its enterprise that it had expected to complete. To calculate the cost of the tool, we multiplied the total cost ($1,160,260) by the percentage of databases that were not scanned by the tool (96 percent), with the result of $1,113,850.

Appendix V

Management's Response to the Draft Report

CHIEF TECHNOLOGY OFFICER

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, D.C. 20224

APR 06 2011

RECEIVED
APR 6 2011

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Terence V. Milholland
Chief Technology Officer

SUBJECT: Draft Audit Report – Security Over Databases Could Be Enhanced to Ensure Taxpayer Data Are Protected (Audit # 201020014) (E-trak #2010-10487)

Thank you for the opportunity to review your draft audit report and to meet with the audit team to discuss earlier draft report observations. The IRS is committed to continuously improving the security of our information technology systems and adequately configured databases operating in its non-mainframe production environment.

The attachment to this memo details our planned corrective actions to implement the recommendations. We do not concur with TIGTA's assertion that the purchase of DbProtect was an inefficient use of resources. At the time of the purchase, DbProtect was the best available tool on the market and met the IRS' immediate needs for a database scanning capability in response to TIGTA's audit recommendations, and was put into production use. However, on-going costs and business requirements were the main reasons for changing to a new database scanning tool. The IRS conducted a thorough technical, cost, and business requirements analysis prior to making the change, and in the process confirmed that the new tool would save the taxpayers over $5.5M in total cost of ownership (compared to the TCO (Total Cost of Ownership) for DbProtect over the next five years while meeting all of the IRS' database scanning requirements.

If you have any questions, please contact me at (202) 622-6800 or Andrea Greene-Horace, Senior Manager, Program Oversight at (202) 283-3427.

Attachment

Attachment

Draft Audit Report – Security Over Databases Could Be Enhanced to Ensure Taxpayer Data Are Protected (Audit # 2001020014) (i-trak #2011-19061)

RECOMMENDATION #1: The Chief Technology Officer should ensure the vulnerabilities identified in the 13 systems scanned during the current audit, as well as any other high-risk security vulnerabilities identified through automated scans and manual reviews, are remediated. Otherwise, a properly approved deviation should be on file to justify departure from stated standards.

CORRECTIVE ACTION #1: We agree with the recommendation. The ACIO Cybersecurity will lead the effort in partnership with Enterprise Operations, to (1) ensure the vulnerabilities identified in the 13 systems scanned during the current audit are remediated or documented in a POAM that will include a remediation strategy and/or risk based decision and (2) develop an Enterprise process and remediation strategy to ensure that high-risk vulnerabilities identified during periodic database vulnerability scans are documented in a POAM that will include a remediation strategy and/or risk based decision

IMPLEMENTATION DATE: December 1, 2011

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #2: The Chief Technology Officer should ensure explicit management approvals are included in the IRS database configuration building process and the IRS database configuration change process to ensure that databases are properly configured according to the standards cited in IRM 10.8.4, RDBMS Security Configurations.

CORRECTIVE ACTION #2: We agree with the recommendation. The IRS will identify appropriate organizations to develop an explicit management approval process to be used in the database build process and the configuration change process that ensures databases are properly configured according to IRM standards.

IMPLEMENTATION DATE: December 1, 2011

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

Attachment

Draft Audit Report – Security Over Databases Could Be Enhanced to Ensure Taxpayer Data Are Protected (Audit # 2001020014) (i-trak #2011-19061)

RECOMMENDATION #3: The Chief Technology Officer should ensure an enterprise-wide strategic plan is developed to address the outdated database version management issues prevalent in the IRS production environment.

CORRECTIVE ACTION #3: We agree with the recommendation. The recommendation is a cross MITS ACIO and cross IRS business unit issue within the purview of Enterprise Services, Infrastructure, Architecture & Engineering (ES, IA&E) as the owner of the IRS architecture program. ES will coordinate with affected stakeholders to develop a strategic plan for obsolescence of technology to include database version control.

IMPLEMENTATION DATE: September 30, 2011

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #4: The Chief Technology Officer should ensure databases with out-of-support DBMS software are upgraded to currently supported versions within a reasonable time period. For those systems where upgrading the database software or implementing security patches have been determined to be dangerous to the stability of the system, a migration plan should be developed and a properly approved deviation should be on file to justify departure from stated standards.

CORRECTIVE ACTION #4: We agree with the recommendation. The ACIO, Enterprise Services (ES) will coordinate with affected stakeholders to develop a migration plan to upgrade the DBMS software to currently supported versions. An inventory of all servers with databases on them and their associated software version will be created. ES will then outline steps to take to address versions older than n-1 and updates will be installed accordingly. ES will establish an ongoing monitoring of servers and institutionalize a process to keep software current.

IMPLEMENTATION DATE: February 1, 2012

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

Attachment

Draft Audit Report – Security Over Databases Could Be Enhanced to Ensure Taxpayer Data Are Protected (Audit # 2001020014) (i-trak #2011-19061)

RECOMMENDATION #5: The Chief Technology Officer should ensure vulnerability scans of IRS databases are conducted in the frequency required by the IRM and any security weakness identified should be corrected or approved for deviation from security policies.

CORRECTIVE ACTION #5: We agree with the recommendation. The Penetration Testing and Code Analysis (PTCA) group within Cybersecurity will establish a formal process for conducting monthly agency-wide scans of IRS databases, as required by the Internal Revenue Manual (IRM) 10.8.1.

In order to ensure identified weaknesses are corrected or approved for deviation from security policies, PTCA will transmit the identified weaknesses and findings report to the stakeholders (i.e., Security Program Management Officer (SPMO), Information System Security Officer (ISSO), IRS Patch Vulnerability Management Group (PVG), Enterprise Operations (EOps), and System Owners). As stated in IRM 10.8.2, the Security Program Management Officer (SPMO) and Information System Security Officer (ISSO) will formulate an appropriate POA&M for correcting the identified weaknesses or recommend approval of deviation from security policies to the System Owner.

IMPLEMENTATION DATE: September 30, 2011

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #6: The Chief Technology Officer should ensure database vulnerability scans are conducted with the access privileges necessary to test all high- and medium-risk database configuration settings.

CORRECTIVE ACTION #6: We agree with the recommendation. For the database systems requiring monthly vulnerability scans in accordance with IRM 1.8.1, the Penetration Testing and Code Analysis (PTCA) group will establish a Memorandum of Understanding (MOU) with Enterprise Operations and System Owners to ensure database vulnerability scans are conducted with the access privileges necessary to test all high- and medium-risk database configuration settings.

IMPLEMENTATION DATE: September 30, 2011

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

Attachment

Draft Audit Report – Security Over Databases Could Be Enhanced to Ensure Taxpayer Data Are Protected (Audit # 2001020014) (i-trak #2011-19061)

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.

RECOMMENDATION #7: The Chief Technology Officer should ensure a thorough technical product evaluation and testing of key functional requirements is consistently conducted and documented for the acquisition of software products.

CORRECTIVE ACTION #7: We agree with the recommendation. The IRS has established Product Selection Guidance and has controls in place for technical product evaluation and testing of key functional requirements. The Change Control governance process ensures thorough product evaluation and testing has been completed prior to product acquisition following the Product Evaluation and Selection (PES) Guidance. In addition, a centralized repository exists documenting all change requests and their disposition. The IRS can create/designate a location to ensure all PES and testing documentation is stored or accessible from a centralized location.

IMPLEMENTATION DATE: September 30, 2011

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Services

CORRECTIVE ACTION MONITORING PLAN: We enter accepted Corrective Actions into the Joint Audit Management Enterprise System (JAMES) and monitor them on a monthly basis until completion.