



*Standard Database Security Configurations
Are Adequate, Although Much Work Is
Needed to Ensure Proper Implementation*

August 22, 2007

Reference Number: 2007-20-129

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

Phone Number | 202-927-7037

Email Address | Bonnie.Heald@tigta.treas.gov

Web Site | <http://www.tigta.gov>



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

August 22, 2007

MEMORANDUM FOR CHIEF INFORMATION OFFICER

FROM: 
Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Standard Database Security Configurations Are Adequate, Although Much Work Is Needed to Ensure Proper Implementation (Audit # 200620033)

This report presents the results of our review of the adequacy of the Internal Revenue Service's (IRS) standard database security configurations and effectiveness of their implementation. This audit is part of the statutory audit coverage under the Information Systems Programs and is included in the Treasury Inspector General for Tax Administration Fiscal Year 2007 Annual Audit Plan.

Impact on the Taxpayer

Database security controls are an organization's last line of defense in protecting sensitive data. While the IRS' standard database security configurations are adequate, they are not effectively implemented on critical databases. Failure to adequately secure these databases places nearly all individual and business taxpayer accounts at risk of unauthorized access, which can lead to identity theft or fraud.

Synopsis

IRS databases contain some of the most sensitive information in the Federal Government—taxpayer personal and financial information. While security of any computer system is dependent on the number and strength of the layers of security protecting it, the last and possibly best line of defense in protecting data are database security controls.



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

The IRS has developed adequate standard database security configurations that are aligned with Federal Government guidelines and best practices. However, these standard configurations have not been effectively implemented. We tested basic database security controls on 17 databases from 8 tax administration applications. Collectively, these databases failed 30 percent of our tests. Using the IRS' rating methodology for standards compliance, all databases we reviewed earned the lowest possible rating. Exploitation of the vulnerabilities found could result in unauthorized accesses to taxpayer information and ultimately result in identity theft or fraud.

The control weaknesses occurred because standard database security configurations were poorly communicated, security roles and responsibilities were not assigned or carried out, and tests to detect noncompliance with standard configurations were inadequate.

Many of the employees supporting the applications we reviewed were unaware of the IRS' standard database security configurations. In fact, some employees first became aware the configurations existed during interviews conducted during this audit. Several factors contributed to the poor communication of the standard configurations, including problems with the announcements of the issuance of the configurations and posting of an outdated version of the configurations on an internal IRS web site.

Also, the roles and responsibilities for securing databases have not been fulfilled. Key security responsibilities, such as ensuring standard database security configurations are implemented, have not been assigned. Managers and employees with responsibility for securing the applications have not taken their security responsibilities seriously and managers are not holding employees accountable for failing to implement database security controls. Their approach to security appears to be reactive, waiting for others to point out security actions that need to be taken. However, security requires a proactive approach. If such an approach had been taken, managers and employees would have sought out the configurations instead of waiting for them to be delivered to their desktops.

We also found inadequate processes for detecting noncompliance with standard database security configurations, although progress is being made. The Mission Assurance and Security Services organization is responsible for assessing the security of computer systems and tracking compliance with IRS standard configurations. Security testing in 2006 for two of the applications we reviewed did not include tests of database controls. The Mission Assurance and Security Services organization did revise its security testing and evaluation methodology for the 2007 testing cycle, which now includes more testing of database controls. In addition, the IRS currently does not have tools to test compliance with standard database security configurations. Efforts are underway to conduct more testing, but the IRS has not developed a project plan or procedures to aid in managing this effort. In July 2007, the information technology security program within the Mission Assurance and Security Services organization was realigned to a new Cybersecurity organization, reporting to the IRS Chief Information Officer.



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

Recommendations

We recommended the Chief Information Officer ensure the database security control weaknesses we identified are corrected, re-publicize standard database security configurations, and ensure the Modernization and Information Technology Services organization's internal web sites refer to the appropriate web site for current security configurations. In addition, we recommended the Chief Information Officer ensure security and administration responsibilities are properly assigned for all IRS databases and investigate alternatives for ensuring employees are aware of their database security responsibilities, with managers holding their employees accountable for meeting those responsibilities. We also recommended the Chief Information Officer ensure security testing evaluates compliance with standard database security configurations and develop an implementation plan and standard operating procedures for the IRS' database compliance assessment tool.

Response

The Chief Information Officer agreed with all of our recommendations. Planned corrective actions include adding specific weaknesses identified in this review to corrective plans of actions and milestones. The IRS' standard database security configurations will also be re-communicated throughout the agency. A memorandum will be distributed within the Modernization and Information Technology Services organization reiterating that internal web sites refer to the appropriate web site for current security configuration guidance. The Chief Information Officer will assign a project officer and develop a project plan to coordinate activities required to resolve all IRS-wide issues associated with the implementation of database security controls in IRS systems, including activities to ensure all IRS databases have individuals assigned to specifically perform security and administration responsibilities. Quarterly reviews will be performed to ensure compliance with IRS policy for these responsibilities, with noncompliance reported to IRS executives for appropriate action. The Chief Information Officer also agreed to include standard database security configurations in the list of controls tested annually. Also, an implementation plan and procedures will be developed for the IRS' database compliance assessment tool. Management's complete response to the draft report is included as Appendix VI.

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 Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at 202-622-8510.



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

Table of Contents

Background	Page 1
Results of Review	Page 3
Standard Database Security Configurations Are Adequate	Page 3
Standard Database Security Configurations Have Not Been Effectively Implemented.....	Page 4
<u>Recommendation 1</u> :.....	Page 7
<u>Recommendations 2 through 4</u> :.....	Page 8
<u>Recommendations 5 through 7</u> :.....	Page 9
Appendices	
Appendix I – Detailed Objective, Scope, and Methodology	Page 11
Appendix II – Major Contributors to This Report	Page 12
Appendix III – Report Distribution List	Page 13
Appendix IV – Scope of Database Assessment	Page 14
Appendix V – Details of Database Assessment.....	Page 16
Appendix VI – Management’s Response to the Draft Report	Page 21



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

Abbreviations

IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
SQL	Structured Query Language



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

Background

All Federal Government systems contain data that require protection under Office of Management and Budget and Congressional mandates. This protection is typically applied in layers around a computer system. The first layer is the perimeter of the system, where network controls identify and prevent attacks originating from outside an organization. Successive layers of controls in the operating systems, applications, and databases are usually needed to protect an organization's data. Consequently, a computer system's security is dependent on the number and strength of the layers of protection. However, because database software stores and manages an organization's data, database security controls are the last and possibly the best line of defense in protecting this critical asset.

Database security controls are the last and possibly the best line of defense in protecting an organization's data.

For the Internal Revenue Service (IRS), taxpayer personal and financial information are the most critical assets it is charged with safeguarding. Due to the sensitivity of this data, the IRS could be a target for malicious users intent on committing identity theft. Attacks on this data could also result in financial losses to the Federal Government, privacy violations, and breaches of national security. Consequently, the IRS' database controls need to be strong.

The Mission Assurance and Security Services organization¹ is responsible for establishing IRS computer security policies, assessing the security of computer systems, and tracking compliance with IRS policies and standards. Responsibility for implementing database security policies and standards generally falls to the Modernization and Information Technology Services organization. IRS business units also share responsibility for implementing computer security controls.

While the IRS uses more than 30 different database software products and has more than 2,100 database installations, 3 databases (Microsoft's Structured Query Language [SQL] Server, IBM's DB2, and Oracle database systems) are by far the most widely used. Our review focused on answering the questions of whether the IRS' standard database security configurations are adequate and effectively implemented on these three databases.

¹ In July 2007, the information technology security program within the Mission Assurance and Security Services organization was realigned to a new Cybersecurity organization within the Modernization and Information Technology Services organization. The new organization reports to the IRS Chief Information Officer.



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

This review was performed at the Chief Information Officer and Mission Assurance and Security Services organization offices in New Carrollton, Maryland, the Enterprise Computing Center² in Memphis, Tennessee, and the IRS campuses³ in Chamblee, Georgia, and Austin, Texas, during the period January through April 2007. The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

² IRS Computing Centers support tax processing and information management through a data processing and telecommunications infrastructure.

³ The data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts.



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

Results of Review

Standard Database Security Configurations Are Adequate

Minimum Security Requirements for Federal Information and Information Systems (Federal Information Processing Standard 200) identifies minimum security requirements in 17 security-related areas addressing the management, operational, and technical aspects of protecting Federal Government information and information systems. The National Institute of Standards and Technology's (NIST)⁴ *Recommended Security Controls for Federal Information Systems* (Special Publication 800-53) aids Federal Government agencies in implementing these requirements by providing guidelines for selecting computer security controls. Additionally, Federal Government agencies publish requirements for specific controls for use within their organizations.

To further aid Federal Government agencies in implementing security controls, the NIST maintains a repository of security configuration checklists it and other organizations, such as the Defense Information Systems Agency, have developed.⁵ These checklists provide a series of instructions for securing a particular computer product, such as an operating system or database software.

In March 2006, the IRS issued standard security configurations for all IRS databases. We reviewed these configurations and determined they are aligned to management, operational, and technical control areas specified in NIST Special Publication 800-53 and adequately address database-specific security controls in these areas. We also compared the configurations for specific database software with database security checklists from the NIST repository, published by the Defense Information Systems Agency, and determined the IRS configurations adequately include the controls from these checklists. Therefore, we conclude the IRS has adequate database security configurations for its most widely used database software.

Although security configurations are adequate for its most widely used databases, nearly one-third of the IRS' moderate-risk applications use database software without a database-specific standard security configuration. We plan to perform future audits of these applications to determine whether their databases are secured according to IRS standards.

⁴ The NIST, under the Department of Commerce, is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal Government agency operations and assets.

⁵ Checklists are developed in accordance with *Security Configuration Checklists Program for Information Technology Products* (NIST Special Publication 800-70).



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

Standard Database Security Configurations Have Not Been Effectively Implemented

While IRS standard database security configurations are adequate, they have not been effectively implemented. We reviewed 17 databases from 8 applications supporting critical tax administration business processes, such as processing of tax returns, receipt of tax payments, and correspondence with taxpayers. These databases were tested for compliance with controls required by IRS standard database security configurations. The tests included basic database security controls in the areas of identifying and authenticating users, granting access based on job necessity, recording user activity, and updating database software. Appendix IV provides additional details on the scope of our assessment.

Collectively, the databases we reviewed failed 30 percent of the more than 800 controls tested. Included in these results are failed tests for controls aimed at preventing high and moderate risk vulnerabilities. Most databases failed tests in all four basic security control areas tested. The IRS has established a method for rating operating system compliance with IRS requirements and assigning a color rating. Using this same methodology, we determined that each database received the lowest rating possible, RED. Appendix V provides additional details on the results of our tests.

Exploitation of the vulnerabilities found could result in the unauthorized access to taxpayer information and could ultimately result in identity theft or fraud. The systems we reviewed process transactions for nearly all individual and business taxpayer accounts, including paper returns, electronic returns, and electronic payment of taxes. Between October 2006 and April 2007, 2 of the databases we reviewed processed nearly 153 million electronic transactions. If these systems were to be corrupted or disabled, the IRS tax processing system could be crippled, preventing millions of taxpayers from filing their tax returns or paying their taxes.

The control weaknesses we found occurred because standard database security configurations were poorly communicated, security roles and responsibilities were not assigned or carried out, and enforcement of standard configurations is inadequate. The following sections further discuss these issues.

Standard database security configurations were poorly communicated

The standard database security configurations are posted on the Mission Assurance and Security Services organization web site and accessible to all IRS employees. During interviews, however, we found many employees with key security responsibilities for the applications we reviewed were unaware of the IRS standard database security configurations. For many, their first notice of the existence of the configurations was through these interviews. For example, we found:

- Employees in two application project offices did not receive notice of the issuance of the configurations. For the applications we reviewed, application project offices are



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

responsible for configuring SQL and DB2 databases or managing contractors that manage database configurations.

- One business unit owner was unaware of the IRS standard database security configurations. Business owners are responsible for overall security of their applications.

Employees were unaware of the standard configurations due, in part, to poor communications by the Mission Assurance and Security Services organization with other business units. These employees were not notified that the configurations had been posted to the Mission Assurance and Security Services organization's web site. We also reviewed the web site of the organization responsible for maintaining Oracle database standard configurations, which is part of the Modernization and Information Technology Services organization. We found the web site did not contain current configurations or a link to the Mission Assurance and Security Services organization's web site. After we raised this issue with IRS management during this review, a link to the correct version of the configurations was posted to the web site.

Database security responsibilities were not carried out

The IRS has defined roles and responsibilities for administering and securing its databases. In particular:

- System owners have ultimate responsibility for those systems that support their missions.
- Database administrators are responsible for maintaining a secure database environment.
- Security specialists are responsible for ensuring IRS database security requirements, as documented in standard database security configurations, are met. Security specialists coordinate with database administrators and other operational personnel to ensure requirements are met.

However, some key database security responsibilities were not assigned. Specifically, database administrators were not assigned for SQL Server and DB2 databases. Currently, application developers manage the configuration of these databases and send implementation instructions to server administrators. In addition, security specialist roles were not assigned for most of the applications we reviewed. None of the specialists identified were assigned to the Mission Assurance and Security Services organization, where security specialists are typically located.

Security responsibilities were not taken seriously by the managers and employees responsible for some of the applications we tested. For example:

- The project office for a contractor-managed application was aware of the standard database security configurations issued in March 2006. However, project office personnel informed us that in 2006 they did not require the contractor to implement the configurations due to higher priorities, such as system upgrades. In 2007, a limited budget prevented implementation of the requirements.



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

- For another contractor-managed application, we were informed that database software updates could not be installed at any point during the IRS' tax filing season⁶ to ensure the application's services would not be disrupted. However, another tax filing application we reviewed, managed by IRS personnel, was adequately updated. In our compliance ratings, contractor-managed applications scored among the lowest of all applications reviewed.
- In response to our testing, project office personnel for two applications cited perimeter controls as mitigating factors to the risk that database control vulnerabilities pose. However, it is well established that insiders pose as great or greater risk to computer security than external attackers.
- Employees in the division responsible for managing Oracle databases were unaware of the issuance of standard database security configurations, despite their involvement in the development of the configurations.

Some developers also made design choices for their applications that make it difficult to maintain security. For example, the project office for an application that did not have database software updates installed informed us the database software could not be kept current because the version needed to be compatible with other commercial software used by the application. Consequently, the database software cannot be consistently kept at the most current version.

To ensure database security requirements are implemented, the IRS needs to ensure security roles and responsibilities are appropriately assigned. In addition, the examples we cite indicate that personnel responsible for securing databases are not being held accountable for failing to implement database security controls. Their approach to security appears to be reactive, waiting for others to point out security actions that need to be taken. However, security requires a proactive approach. If such an approach had been taken, managers and employees would have sought out the configurations instead of waiting for them to be delivered to their desktops.

Testing to detect noncompliance with standard database security configurations was inadequate

The Mission Assurance and Security Services organization is responsible for assessing the security of computer systems and tracking compliance with IRS policies and standards. There are two primary means by which the Mission Assurance and Security Services organization accomplishes these responsibilities:

⁶ The period from January through mid-April when most individual income tax returns are filed.



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

- Security testing and evaluation (security controls tested as part of an application's certification⁷ and accreditation).
- Routine compliance assessment (software tools used quarterly to assess compliance of systems with security standard configurations).

Our assessment of these efforts determined that the Mission Assurance and Security Services organization has not adequately enforced standard database security configurations, but it is making progress. Security testing and evaluation results for two of the applications we reviewed, both tested in 2006, determined that, while application controls were tested, database controls were not. The Mission Assurance and Security Services organization did revise its security testing and evaluation methodology for the 2007 testing cycle, which now includes more testing of database controls.

While the Mission Assurance and Security Services organization has compliance assessment tools in place for computer operating systems, it currently does not have tools to test database controls. Currently, the IRS scans databases for commonly known user accounts and passwords, which are included in default installations of database software. We did not identify any of these accounts for the databases we reviewed. However, the Mission Assurance and Security Services organization currently does not have tools to test compliance with standard database security configurations. Mission Assurance and Security Services organization management informed us that efforts are underway to implement a testing tool by mid-summer of 2007. There are, however, no project plans or procedures to aid in managing this effort.

Recommendations

To ensure the applications we reviewed comply with IRS database security requirements:

Recommendation 1: The Chief Information Officer should ensure the database security control weaknesses we identified are corrected.

Management's Response: The Chief Information Officer agreed with this recommendation. Each of the database security control weaknesses that were identified in the specific applications will be included in corrective plans of action and milestones, as required by the Federal Information Security Management Act.⁸ Priority will be placed on correcting or mitigating any identified high risk weaknesses. As medium or low risk weaknesses are reviewed, the plans will reflect whether the weaknesses are to be corrected or mitigated, or whether the applicable approving official has made a risk acceptance determination. In addition, a project officer will be assigned to coordinate all

⁷ An independent technical evaluation for the purpose of accreditation that uses security requirements as the criteria for the evaluation.

⁸ Pub. L. No. 107-347, Title III, 116 Stat. 2946 (2002).



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

activities required to resolve all IRS-wide issues associated with the implementation of database security controls in IRS systems. Several of the database security control weaknesses, such as auditing, will be addressed as part of the IRS computer security material weakness corrective action plans.

To improve communication of standard database security configurations:

Recommendation 2: The Chief Information Officer should re-publicize the standard database security configurations and coordinate with IRS organizations to ensure the configurations are effectively distributed to necessary personnel or employees are advised to access the Mission Assurance and Security Services organization web site where the configurations are posted.

Management's Response: The Chief Information Officer agreed with this recommendation. In July 2007, the information technology security program within the Mission Assurance and Security Services organization was realigned to a new Cybersecurity organization within the Modernization and Information Technology Services organization. This new organization is headed by an Associate Chief Information Officer for Cybersecurity, who will notify other IRS organizations of the database security configuration guidance posted on the Cybersecurity organization web site. This information will also be formally re-publicized using available communications capabilities supporting computer systems governance and oversight.

Recommendation 3: The Chief Information Officer should ensure the Modernization and Information Technology Services organization's internal web sites refer to the Mission Assurance and Security Services organization web site for current security configurations.

Management's Response: The Chief Information Officer agreed with this recommendation. The IRS will remind the Associate Chief Information Officers in the Modernization and Information Technology Services organization to ensure their internal web sites refer to the Cybersecurity organization web site for current security configuration guidance. In addition, to improve uniformity in current security configuration guidance, the IRS will distribute a memorandum to the Associate Chief Information Officers reiterating the policy to post only documentation on their internal web sites that is owned and maintained by their organizations.

To ensure security roles and responsibilities are enforced for IRS databases:

Recommendation 4: The Chief Information Officer should ensure security and administration responsibilities are properly assigned for all IRS databases.

Management's Response: The Chief Information Officer agreed with this recommendation. The Associate Chief Information Officer for Cybersecurity will assign a project officer to coordinate activities required to resolve all IRS-wide issues associated with the implementation of database security controls in IRS systems. The associated project plan will include the coordination activities required to ensure a full accounting



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

and inventory exists for all IRS databases, and that each of the databases has individuals assigned to specifically perform security and administration responsibilities.

In conjunction with the IRS' material weakness for information technology security roles and responsibilities, database security roles and responsibilities have been developed and documented in IRS manuals. At a minimum, periodic checks as part of the annual Federal Information Security Management Act review will be conducted to ensure assignment of security and administrative responsibilities are in compliance with IRS policy.

Recommendation 5: The Chief Information Officer should investigate alternatives for ensuring employees are aware of their database security responsibilities, such as establishing an element in employee performance plans specifically for carrying out their database security responsibilities. For whichever alternative is used, managers should ensure employees are held accountable for meeting those responsibilities.

Management's Response: The Chief Information Officer agreed with this recommendation. The Associate Chief Information Officer for Cybersecurity will ensure that quarterly compliance reviews by its field staff will specifically review the compliance with database security roles and responsibilities. Formal noncompliance reports will be forwarded to IRS executives so managers can take appropriate actions to address and resolve any employee violations. Individual managers can decide whether additional training or disciplinary actions are the appropriate remedy for those employees who fail to meet assessment standards.

An assessment of compliance with assigned security roles and responsibilities, including those for databases, will be included in the IRS' annual Federal Information Security Management Act assessment.

To improve the IRS' ability to detect noncompliance with database security requirements and emphasize the importance of database security controls:

Recommendation 6: The Chief Information Officer should ensure security testing evaluates compliance with standard database security configurations.

Management's Response: The Chief Information Officer agreed with this recommendation. The Associate Chief Information Officer for Cybersecurity will include appropriate NIST 800-53 controls relating to standard database security configurations in the list of "volatile" controls to be tested annually.

Recommendation 7: The Chief Information Officer should 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. To ensure security controls are adequately considered by application project offices, application development databases should be included in the scope of database testing.



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

A standard operating procedure should be developed to accompany the tool's implementation. These procedures should describe the process and responsible organizations for addressing the outcome and remediation of the results of the compliance assessment tool.

Management's Response: The Chief Information Officer agreed with this recommendation. The IRS will implement a process for detecting noncompliance with database security requirements. This will include 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. In addition, standard operating procedures will be developed to accompany the tool's implementation. These procedures will describe the process and responsible organizations for addressing the outcome and remediation of the results of the compliance assessment tool.



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

Appendix I

Detailed Objective, Scope, and Methodology

The objective of our review was to determine whether the IRS' standard database security configurations were adequate and effectively implemented. To accomplish this objective, we:

- I. Determined whether the IRS standard database security configurations were adequate.
 - A. Determined whether current standard database security configurations existed for all database management systems.
 - B. Assessed the adequacy of IRS standard database security configurations. For this analysis, we used the security configurations specified in the Defense Information Systems Agency Database Security checklist as criteria. To identify databases in use by the IRS, we used network scanning software to scan the IRS network, which identified services listening on specified network ports. We scanned 45 networking ports that are commonly used by database systems. Most IRS network segments were scanned, although those from the Office of Chief Counsel and the Criminal Investigation organization were omitted. These organizations manage their own databases and were not included in the scope of this review.
 - C. Assessed the effect of inadequate standard configurations.
- II. Determined whether the IRS standard database security configurations were effectively implemented.
 - A. Determined whether technical database controls specified in IRS standard database security configurations and the NIST *Recommended Security Controls for Federal Information Systems* (Special Publication 800-53) were implemented on IRS systems. We assessed controls using a database scanning tool that collected information from IRS databases and analyzed it to identify weaknesses. We selected applications for review using several factors, including being a part of the IRS tax administration process, database technology used (i.e., Oracle, SQL Server, or DB2), importance of the system, and business system owner. Mainframe computers were not included in this analysis because IRS standard database security configurations pertain primarily to computers running UNIX and Microsoft Windows operating systems. We did not assess the implementation of database controls on mainframe computers.
 - B. Assessed the effect of database vulnerabilities on the IRS.
 - C. Determined why the vulnerabilities occurred.



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

Appendix II

Major Contributors to This Report

Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs)
Stephen R. Mullins, Director
Joan Raniolo, Acting Audit Manager
Marybeth Schumann, Audit Manager
Michael Howard, Lead Auditor
Dan Ardeleano, Senior Auditor
Allen Gray, Senior Auditor
Abraham Millado, Senior Auditor
Jacqueline Nguyen, Senior Auditor
Midori Ohno, Senior Auditor
Larry Reimer, Senior Auditor



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

Appendix III

Report Distribution List

Acting Commissioner C
Office of the Commissioner – Attn: Acting Chief of Staff C
Deputy Commissioner for Operations Support OS
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 Liaisons:
 Chief Information Officer OS:CIO
 Director, Program Oversight OS:CIO:SM:PO



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

Appendix IV

Scope of Database Assessment

This appendix provides additional details on the scope of the applications and database controls tested in this review. During this review, we assessed eight applications for adequacy of the implementation of database security requirements. Table 1 identifies these applications and the number and location of databases tested.

Table 1: List of Applications Tested

Application	Database Software Used	Enterprise Computing Center – Memphis	Austin Campus	Atlanta Campus
Automated Lien System	Oracle	1	0	0
Correspondence Imaging System	DB2	4	1	1
Electronic Federal Tax Payment System	Oracle	1	0	0
Electronic Management System	Oracle	1	0	0
Individual Taxpayer Identification Number	Oracle	1	0	0
Integrated Submission and Remittance Processing	SQL Server	0	2	2
On Line Notice Review	SQL Server	0	1	1
Tax Exempt/Government Entities Reporting and Electronic Examination System	SQL Server	1	0	0

Source: Treasury Inspector General for Tax Administration assessment of selected IRS databases, using data collected from these systems.



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

We tested controls against the IRS standard database security configurations. We tested basic controls in four areas, which match the NIST *Recommended Security Controls for Federal Information Systems* (Special Publication 800-53) controls described in Table 2.

Table 2: Database Controls Tested

Category	NIST Special Publication 800-53 Control	Control Number
Access Controls	Least Privilege: The information system enforces the most restrictive set of rights and privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks.	Access Control – 6
Auditable Events	Auditable Events: The information system generates audit records for the organization-defined auditable events.	Audit and Accountability – 2
User Identification and Authentication	User Identification and Authentication: The information system uniquely identifies and authenticates users (or processes acting on behalf of users).	Identification and Authentication – 2
Database Software Updates	Flaw Remediation: The organization identifies, reports, and corrects information system flaws.	System and Information Integrity – 2

Source: NIST Special Publication 800-53.



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

Appendix V

Details of Database Assessment

This appendix provides additional details of the database security controls tested during this review. As stated in the report, the databases we reviewed failed 30 percent of the more than 800 controls tested. Table 1 summarizes the test results:

Table 1: Summary of Control Test Results

Database	Percentage of Tests Failed
Oracle	33 percent
SQL Server	35 percent
DB2	24 percent
All databases	30 percent

Source: Treasury Inspector General for Tax Administration assessment of selected IRS databases, using data collected from these systems.

The IRS has established a method for rating operating system compliance with IRS requirements and assigning a color rating. Using this methodology, we determined that each database received the lowest rating possible, RED. Table 2 summarizes our compliance rating results:

Table 2: Summary of Compliance Ratings

Database	Compliance Score ¹	Average High-Risk Vulnerabilities per Database ²	Compliance Rating
Oracle	71%	8.5	RED
SQL Server	74%	10.6	RED
DB2	80%	3.0	RED
Overall	75%	7.4	RED

Source: Treasury Inspector General for Tax Administration assessment of selected IRS databases, using data collected from these systems, and IRS compliance assessment guides for Windows and UNIX operating systems.

¹ The compliance score represents how well the standard database security configurations tested were met. Test scores were weighted based on the level of risk associated with the configuration being tested.

² This average represents how many high-risk vulnerabilities were found, on average, for each of the three types of database software tested.



**Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation**

Most databases we reviewed failed tests in all four basic security control areas tested, although a few databases passed tests for updating database software. Table 3 identifies the specific controls that failed, their risk rating, and the number of applications that failed the test.

Table 3: Database Controls Failing Audit Tests

Database Controls Tested	Risk	Description	Applications Failing Test
2(f)			



***Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation***

Database Controls Tested	Risk	Description	Applications Failing Test
2(f)			



***Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation***

Database Controls Tested	Risk	Description	Applications Failing Test
2(f)			



**Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation**

Database Controls Tested	Risk	Description	Applications Failing Test
2(f)			

Source: Treasury Inspector General for Tax Administration assessment of selected IRS databases, using data collected from these systems.



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

Appendix VI

Management's Response to the Draft Report



CHIEF INFORMATION OFFICER

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

RECEIVED
JUL 30 2007

July 30, 2007

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Richard A. Spires
Chief Information Officer

SUBJECT: Draft Audit Report – Standard Database Security Configurations Are Adequate, Although Much Work Is Needed to Ensure Proper Implementation (Audit #200620033) (i-trak #2007-26303)

Thank you for the opportunity to review and respond to the subject draft audit report. As noted in the report, the Internal Revenue Service (IRS) issued a standard security database configuration that maps to the management, operational, and technical control areas specified in the National Institute of Standards and Technology Special Publication 800-53 and adequately addressed database-specific security controls in these areas. The IRS' Modernization and Information Technology Services (MITS) organization continually strives to improve the security of our information technology (IT) resources by implementing current policies and TIGTA recommendations.

We agree with, and will implement, all of your recommendations. The attachment to this memo describes our planned actions to implement your recommendations. Please note that on July 8, 2007, the IT Security Program, formerly under Mission Assurance & Security Services, was realigned to MITS, under the new name of Cybersecurity. The corrective actions reference that new organizational realignment.

Thank you for your continued support and guidance. We look forward to working with your staff throughout the year to develop appropriate measures. If you have any questions, please contact me at (202) 622-6800. Members of your staff may also contact Perry Robinett, Director of Program Oversight Coordination, at (202) 283-6283.

Attachment



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

Attachment

Draft Audit Report – Standard Database Security Configurations Are Adequate, Although Much Work Is Needed to Ensure Proper Implementation (Audit #200620033) (i-trak #2007-26303)

RECOMMENDATION #1: To ensure the applications we reviewed comply with IRS database security requirements: The Chief Information Officer should ensure the database security control weaknesses we identified are corrected.

CORRECTIVE ACTION #1: We agree with this recommendation. Each of the database security control weaknesses that were identified in the specific applications reviewed by TIGTA will be included in corrective plans of actions and milestones (POAMs), as required by the Federal Information Security Management Act (FISMA) of 2002. Priority will be placed on correcting or mitigating any identified high-risk weaknesses. As medium or low risk weaknesses are reviewed, the POAMs will reflect if the weaknesses are to be corrected or mitigated, or whether the applicable Designated Approving Authority (DAA) has made a risk acceptance determination. In addition, a project officer will be assigned to coordinate activities required to resolve all IRS-wide issues associated with the implementation of database security controls in IRS systems. This will include applications and servers maintained by contractors and those maintained separately by the business units.

A number of the database security control weaknesses, such as auditing, will be addressed as part of the IRS computer security material weakness corrective action plans. The IRS will ensure that all actions required to resolve individual application-level database security weaknesses, and any associated IRS-wide supporting infrastructure security weaknesses, are accounted for in FISMA POAMs and in IRS-wide computer security material weakness plans.

IMPLEMENTATION DATE: July 1, 2008

RESPONSIBLE OFFICIAL #1: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion. Progress on the corrective actions contained in the FISMA POAMs for IRS applications and systems that contain database security control weaknesses will be reviewed quarterly.

RECOMMENDATION #2: To improve communication of standard database security configurations: The Chief, Mission Assurance and Security Services, should re-publicize the standard database security configurations and coordinate with IRS organizations to ensure the configurations are effectively distributed to necessary personnel or employees are advised to access the Mission Assurance and Security Services organization web site where the configurations are posted.

CORRECTIVE ACTION #2: We agree with this recommendation. On July 8, 2007, the IT Security Program, formerly under Mission Assurance & Security Services (MA&SS), was realigned to the Modernization and Information Technology Services (MITS) organization. The MITS Associate Chief Information Officer (ACIO) for Cybersecurity will notify MITS ACIOs along with other IRS business units of the database security configuration guidance posted on the Cybersecurity website. This information will also be formally re-publicized using the communications capabilities that are in place to support IT systems governance and oversight,



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

АҞАСШЕНІ

Draft Audit Report – Standard Database Security Configurations Are Adequate, Although Much Work Is Needed to Ensure Proper Implementation (Audit #200620033) (i-trak #2007-26303)

effectively distributing the standard database security configuration guidance to the appropriate project personnel and employees.

IMPLEMENTATION DATE: October 1, 2007

RESPONSIBLE OFFICIAL #2: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: Monthly progress reports on these corrective actions are reviewed with the ACIO, Cybersecurity.

RECOMMENDATION #3: To improve communication of standard database security configurations: The Chief Information Officer should ensure the Modernization and Information Technology Services internal web sites refer to the Mission Assurance and Security Services organization web site for current security configurations.

CORRECTIVE ACTION #3: We agree with this recommendation. The IRS will remind the MITS ACIOs to ensure their internal websites refer to the Cybersecurity website for current security configuration guidance. In addition, to ensure uniformity in current security configuration guidance, the IRS will distribute a memorandum to all MITS ACIOs reiterating the policy to only post documentation on their internal websites that is owned and maintained by their organizations.

IMPLEMENTATION DATE: October 1, 2007

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Operations

CORRECTIVE ACTION MONITORING PLAN: We enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION #4: To ensure security roles and responsibilities are enforced for IRS databases: The Chief, Mission Assurance and Security Services, and Chief Information Officer should ensure security and administration responsibilities are properly assigned for all IRS databases.

CORRECTIVE ACTION #4: We agree with this recommendation. The ACIO, Cybersecurity will assign a project officer to coordinate activities required to resolve all IRS-wide issues associated with the implementation of database security controls in IRS systems. This will include applications and servers maintained by contractors and those maintained separately by the business units. The associated project plan will include coordination activities required to ensure that a full accounting and inventory exists for all IRS databases, and that each has an individual assigned to perform security and administration responsibilities.

In conjunction with MW 1-4 IT Security Roles and Responsibilities, database security roles and responsibilities have been developed. The following Internal Revenue Manuals (IRMs) were developed or updated based on the policies and guidelines listed in IRM 10.8.4 and 10.8.2: IRM



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

Attachment

Draft Audit Report – Standard Database Security Configurations Are Adequate, Although Much Work Is Needed to Ensure Proper Implementation (Audit #200620033) (i-trak #2007-26303)

2.7.1, 2.7.2, 2.7.4, 2.7.5, 2.7.6, 2.13.10, 2.13.11, and 2.20.15. The IRMs listed were issued as Interim Guidance on February 17, 2006. Subsequent reviews and updates have been completed in accordance with IRM publishing standards. At a minimum, periodic checks as part of the annual FISMA review will be conducted to ensure assignment of security and administrative responsibilities comply with IRS policy.

IMPLEMENTATION DATE: July 1, 2008

RESPONSIBLE OFFICIAL #4: Associate Chief Information Officer, Cybersecurity.

CORRECTIVE ACTION MONITORING PLAN: IT security staff in the field will conduct quarterly reviews. An annual assessment will be completed as part of the required annual FISMA review.

RECOMMENDATION #5: To ensure security roles and responsibilities are enforced for IRS databases: The Chief Information Officer should investigate alternatives for ensuring employees are aware of their database security responsibilities, such as establishing an element in employee performance plans specifically for carrying out their database security responsibilities. For whichever alternative is used, managers should ensure employees are held accountable for meeting those responsibilities.

CORRECTIVE ACTION #5: We agree with this recommendation. The ACIO, Cybersecurity will ensure that the quarterly compliance reviews conducted by field IT security staff will specifically review compliance with database security roles and responsibilities. Formal non-compliance reports will be forwarded to executives in MITS and the business units, so that managers can take appropriate actions to address and resolve any employee violations. Individual managers can decide if additional training or disciplinary actions are the appropriate remedy for those employees who fail to meet assessment standards.

In conjunction with MW 1-4 IT Security Roles and Responsibilities, including database security roles and responsibilities, the Cybersecurity organization will complete the annual FISMA assessment of compliance with assigned security roles and responsibilities.

IMPLEMENTATION DATE: April 1, 2008

RESPONSIBLE OFFICIAL #5: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: The ACIO, Cybersecurity will review the results of the quarterly compliance reviews. An annual assessment will be completed as part of the FISMA review. Managers will document actions taken for individual employees.

RECOMMENDATION #6: To improve the IRS' ability to detect noncompliance with database security requirements and emphasize the importance of database security controls: The Chief, Mission Assurance and Security Services, should ensure security testing evaluates compliance with standard database security configurations.



*Standard Database Security Configurations Are Adequate,
Although Much Work Is Needed to Ensure Proper Implementation*

Attachment

Draft Audit Report – Standard Database Security Configurations Are Adequate, Although Much Work Is Needed to Ensure Proper Implementation (Audit #200620033) (i-trak #2007-26303)

CORRECTIVE ACTION #6: We agree with this recommendation. On July 8, 2007, the IT Security Program, formerly under MA&SS, was realigned to the MITS organization. The ACIO, Cybersecurity will include appropriate National Institute of Standards and Technology (NIST) Special Publication 800-53 controls relating to standard database security configurations in the list of “volatile” controls to be tested annually.

IMPLEMENTATION DATE: December 1, 2007

RESPONSIBLE OFFICIAL #6: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: Monthly progress reports on all corrective actions are reviewed with the ACIO, Cybersecurity.

RECOMMENDATION #7: To improve the IRS’ ability to detect noncompliance with database security requirements and emphasize the importance of database security controls: The Chief, Mission Assurance and Security Services, should 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. To ensure security controls are adequately considered by application project offices, application development databases should be included in the scope of database testing. A standard operating procedure should be developed to accompany the tool’s implementation. These procedures should describe the process and responsible organizations for addressing the outcome and remediation of the results of the compliance assessment tool.

CORRECTIVE ACTION #7: We agree with this recommendation. The IRS will implement a process for detecting non-compliance with database security requirements. This will include 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 implementation schedule. In addition, a standard operating procedure will be developed to accompany the tool’s implementation. These procedures will describe the process and organizations responsible for addressing the outcome and remediation of the compliance assessment tool results.

IMPLEMENTATION DATE: July 1, 2008

RESPONSIBLE OFFICIAL #7: Associate Chief Information Officer, Cybersecurity

CORRECTIVE ACTION MONITORING PLAN: Monthly reports on progress on all corrective actions are reviewed with the ACIO, Cybersecurity.