



*The Mainframe Databases Reviewed Met
Security Requirements; However, Automated
Security Scans Were Not Performed*

September 30, 2011

Reference Number: 2011-20-099

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.

Phone Number | 202-622-6500

Email Address | TIGTACommunications@tigta.treas.gov

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



HIGHLIGHTS

THE MAINFRAME DATABASES REVIEWED MET SECURITY REQUIREMENTS; HOWEVER, AUTOMATED SECURITY SCANS WERE NOT PERFORMED

Highlights

Final Report issued on September 30, 2011

Highlights of Reference Number: 2011-20-099 to the Internal Revenue Service Chief Technology Officer.

IMPACT ON TAXPAYERS

Internal Revenue Service (IRS) mainframe computers support applications associated with processing, tracking, and storing tax return information. Two manufacturers of mainframe computers, International Business Machines Corporation (IBM) and Unisys Corporation, provide the foundation for the IRS computer systems. TIGTA tested the security configurations of two applications processed with DB2 databases residing on IBM mainframes and found it to be effective; however, automated security scans of the 32 IBM DB2 database applications were not performed. By not performing monthly automated database scans, sensitive information may not be secure.

WHY TIGTA DID THE AUDIT

In Fiscal Year 2009, the IRS processed about 144 million individual income tax returns and about 2.5 million corporate income tax returns. This audit is included in our Fiscal Year 2011 Annual Audit Plan and addresses the major management challenge of Modernization. Our overall objective was to determine whether adequate security controls were established for the IBM DB2 databases running on the IBM z/OS operating system.

WHAT TIGTA FOUND

Security policies and configuration settings for the two IBM DB2 databases reviewed were in compliance with Government and industry

standards and were effectively implemented. However, required automated security configuration scans of mainframe databases were not conducted. The audit also identified that the IBM Guardium software application purchased in July 2010 for vulnerability scans on databases had not been fully implemented. In June 2011, the IRS received an invoice for approximately \$700,000 to renew the annual software application license. This invoice was paid in order to continue deployment and avoid penalties for a lapse in maintenance; however, the application had not been fully implemented, resulting in an inefficient use of resources.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Technology Officer implement automated security configuration scanning on mainframe databases, ensure the IBM Guardium software application is fully implemented, and ensure system requirements are identified and agreed upon by all affected Modernization and Information Technology Services organizations prior to purchasing an enterprise-wide software application.

The IRS agreed with all of TIGTA's recommendations. The IRS plans to implement automated security configuration scanning on mainframe databases and coordinate with stakeholders to fully implement the IBM Guardium software application. Vendor Contract Management plans to ensure that all appropriate information technology stakeholders involved in the acquisition of enterprise software applications have been effectively engaged in the articulation of requirements for new enterprise-wide software applications.

The IRS stated that they did not concur with the outcome measure of \$700,000, as the invoice was paid in order to continue deployment and avoid penalties for a lapse in maintenance. However, TIGTA maintains that the inefficient use of resources is due to the delayed deployment that resulted from the lack of proper planning and coordination between the Modernization and Information Technology Services business units prior to the purchase of the application.



TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 30, 2011

MEMORANDUM FOR CHIEF TECHNOLOGY OFFICER

Michael R. Phillips

FROM:

Michael R. Phillips
Deputy Inspector General for Audit

SUBJECT:

Final Audit Report – The Mainframe Databases Reviewed Met Security Requirements; However, Automated Security Scans Were Not Performed (Audit # 201120021)

This report presents the results of our review of the security controls established for the databases residing on the Internal Revenue Service (IRS) mainframe computers. The overall objective of this review was to determine whether adequate security controls had been established for the International Business Machines Corporation (IBM) DB2 databases running on the IBM z/OS operating system. This audit is included in our Fiscal Year 2011 Annual Audit Plan¹ and addresses the major management challenge of Modernization.

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 Alan Duncan, Assistant Inspector General for Audit (Security and Information Technology Services), at (202) 622-5894.

¹ This audit was initially included in *Mainframe Computer Security and Processing (Audit #201120015)*.



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

Table of Contents

Background	Page 1
Results of Review	Page 3
Security Policies and Configuration Settings Were in Compliance With Government and Industry Standards and Were Effectively Implemented for the Two Mainframe DB2 Databases Reviewed	Page 3
Automated Security Configuration Scans of the Mainframe Databases Were Not Conducted	Page 4
<u>Recommendation 1:</u>	Page 4
Delayed Implementation of a Software Application to Scan Databases Resulted in the Inefficient Use of Resources	Page 5
<u>Recommendations 2 and 3:</u>	Page 6
Appendices	
Appendix I – Detailed Objective, Scope, and Methodology	Page 7
Appendix II – Major Contributors to This Report	Page 9
Appendix III – Report Distribution List	Page 10
Appendix IV – Outcome Measure	Page 11
Appendix V – Glossary of Terms	Page 12
Appendix VI – Management’s Response to the Draft Report	Page 15



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

Abbreviations

IBM	International Business Machines Corporation
IRS	Internal Revenue Service



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

Background

The Internal Revenue Service (IRS) relies on a complex environment of computer systems to accomplish its mission. Two manufacturers of mainframe computers, International Business Machines Corporation (IBM) and Unisys Corporation, provide the foundation for its computer systems, which processed about 144 million individual income tax returns and about 2.5 million corporate income tax returns filed in Fiscal Year 2009. These mainframes work with other non-mainframe hardware platforms supplied by companies such as Aspect Computer Corporation, Hewlett Packard Company, Dell Inc., and Sun Microsystems (currently named Oracle America, Inc.).

IRS mainframe computers support applications associated with processing, tracking, and storing tax return information such as the Business Return Transaction File, the Customer Account Data Engine – Individual, and the Business Master File On-Line Processing. Other applications include disparate and unrelated services such as the Currency and Banking Retrieval System used for monitoring monetary transactions exceeding \$10,000, the Personal Identity Verification Background Investigation Process used for tracking contractors, and the Statistics of Income Distributed Processing System that provides mandatory reports to Congress on IRS activities.

Our last audit report issued on IBM mainframe security was in 2002¹ and made two recommendations. The report noted that the IRS was not using a system-software monitoring tool to provide periodic reviews of software which would enable systems programming and security personnel to more efficiently identify system software issues and focus their efforts on resolving those issues. The resultant recommendation was that the IRS needed to evaluate automated tools and establish procedures for their use. The second recommendation was made to timely develop and update mainframe computer access control standards, such as law enforcement manuals and access control matrices, to ensure that progress is made and that these standards are tracked by the Modernization and Information Technology Services (formerly named Modernization, Information Technology, and Security) organization.

During the ensuing years, changes were made to the mainframe environment, including the consolidation of computer processing into one Enterprise Computing Center with three physical locations (Detroit, Michigan; Memphis, Tennessee; and Martinsburg, West Virginia); modifications were made to IRS systems to incorporate income tax law changes; and aging hardware was replaced with technologically advanced equipment.

¹ *System-Level Controls for the Internal Revenue Service's Mainframe Computers Are Generally Adequate; However, Additional Actions Are Needed* (Reference Number 2002-20-168, dated September 4, 2002).



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

The IBM DB2 database system is used in 32 different applications of which 28 are on the IBM z/OS mainframe. Because our review relied on manual analysis of the IBM mainframe security and the DB2 database implementation, the scope of the review was limited to two DB2 database applications on the mainframe. Both applications were owned by the Wage and Investment Division.

This review was performed at the Modernization and Information Technology Services Enterprise Operations organization's offices in New Carrollton, Maryland, and at the Enterprise Computing Center in Martinsburg, West Virginia, during the period November 2010 through July 2011. 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 the audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

Results of Review

Security Policies and Configuration Settings Were in Compliance With Government and Industry Standards and Were Effectively Implemented for the Two Mainframe DB2 Databases Reviewed

The Internal Revenue Manual provides the IRS's standards and policies for the IBM mainframe z/OS operating system, the Resource Access Control Facility,² and the DB2 database. Our review determined the IBM mainframe and DB2 database standards and policies are consistent with guidance provided by the IBM Corporation, the Defense Information Systems Agency, the Department of the Treasury, the Center for Internet Security, and the National Institute of Standards and Technology.

The IRS developed 32 applications that use the IBM DB2 database. We reviewed two applications (the Electronic Tax Administration Marketing Database and the Tax Return Database) owned by the Wage and Investment Division that share resources on the IBM mainframe to verify that the implementation of these applications met IRS standards. Our analysis of system files and system-generated reports verified that both applications met the IRS configuration and security standards for the IBM z/OS operating system and the DB2 database. Following are some examples of the settings that were verified:

- Audit logging settings were appropriate.
- Access controls met the IRS standards of least privilege and separation of duties.
- Resource Access Control Facility security controls met security configuration guidelines.
- Mainframe subsystems were properly separated by function (i.e., test, maintenance, and operations).
- Daily mainframe operating system level audit reports were created.

The Internal Revenue Manual also requires that the Chief Information Security Officer manage, maintain, and track agency Plans of Actions and Milestones for information technology security weaknesses. We reviewed the Plans of Actions and Milestones for Fiscal Years 2009, 2010, and 2011 using the Trusted Agent Federal Information Security Management Act repository for the two applications reviewed. The Plans of Actions and Milestones were entered into the system in a timely manner and resolved in a reasonable length of time.

² See Appendix V for a glossary of terms.



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

Automated Security Configuration Scans of the Mainframe Databases Were Not Conducted

As of April 1, 2010, the Internal Revenue Manual requires monthly automated security configuration scans of all operating and database systems. The IRS performs these scans by using a specialized policy checker program for each of the three major platforms in use within the IRS environment: Microsoft Windows, UNIX, and mainframes.

The monthly mainframe policy checker reports, for the period December 2010 through February 2011, indicated the IBM z/OS mainframes in our sample were 100 percent compliant with IRS mainframe operating system policies. However, the mainframe policy checker does not perform database testing during the automated security configuration scans. Although mainframe database testing is not performed, our review of the two applications determined the database controls were compliant with the IRS configuration policies.

In the Modernization and Information Technology Services organization's *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.

Automated security configuration scans of mainframe databases are not being performed because the IRS has not identified and implemented a tool to perform those scans. By not performing regular and complete monthly automated database scans that check key settings on all applications, sensitive information may not be secure and the IRS has not met its goal of ensuring security diligence is applied to all IRS databases as presented above in the technical roadmap. Additionally, these scans would proactively identify insecure database settings among the remaining DB2 applications that were not tested during our review.

Recommendation

Recommendation 1: The Chief Technology Officer should implement automated security configuration scanning on mainframe databases.

Management's Response: The IRS agreed with this recommendation. The IRS will implement automated security configuration scanning on mainframe databases.



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

Delayed Implementation of a Software Application to Scan Databases Resulted in the Inefficient Use of Resources

Because the IRS does not conduct automated security configuration scans of its mainframe databases, we attempted to identify other testing mechanisms performed to mitigate this issue and identified an issue with the implementation of a database scanning software application. In July 2010, the Cybersecurity organization purchased the IBM Guardium software application to perform automated vulnerability scans of its databases. The enterprise-wide software license covering 3,000 processors and the hardware needed to perform automated vulnerability scans cost \$3.3 million.

The IRS originally anticipated implementation by December 2010. However, by July 2011, the IBM Guardium software application still had not been fully implemented. While automated vulnerability scans could not be performed enterprise-wide, the IRS ran the software manually to perform tests on databases one at a time. The first of these scans was performed in August 2010 on the Tax Professional Preparer Tax Identification Number System database. In addition, in July 2011, the IRS performed an automated test scan of the Customer Account Data Engine 2 database.

The IRS is using its Enterprise Life Cycle systems development methodology to implement the IBM Guardium software application. As of July 2011, the implementation was in the system development phase and was waiting for the Enterprise Architecture organization's approval. Once approval is obtained, the IRS will continue toward completion of the Enterprise Life Cycle process. The IRS could not provide an estimated implementation date for the software application.

One key item that also remains to be completed is for the IRS to set up accounts and permissions on its multiple systems so the IBM Guardium software application could perform credentialed scans of the remaining databases. According to IRS management, the IBM Guardium software application has not been implemented enterprise-wide because of other higher priorities and the lack of support needed from several organizations.

The Clinger-Cohen Act of 1996³ requires agencies to use a disciplined capital planning and investment control process to maximize the value of information technology investments and manage the acquisition risk. In June 2011, the IRS received an invoice for approximately \$700,000 to renew the annual IBM Guardium software application licenses. This invoice was paid in order to continue deployment and avoid penalties for a lapse in maintenance; however, the application had not been fully implemented resulting in an inefficient use of resources.



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

Recommendations

Recommendation 2: The Chief Technology Officer should ensure the IBM Guardium software application is fully implemented.

Management's Response: The IRS is coordinating with stakeholders to fully implement the IBM Guardium software application. This includes vulnerability scan testing of the various database management system platforms, account creation process, mitigation strategy for identified vulnerabilities, identifying appropriate database owners and system administrators across the enterprise, and getting database administrators in all business units to create Guardium user accounts on their databases.

Office of Audit Comment: The IRS does not concur with our assertion that the renewal of the IBM Guardium software application licenses was an inefficient use of resources. The IRS stated that the invoice was paid in order to continue deployment and avoid penalties for a lapse in maintenance. In response to our prior recommendations, the IRS stated that they implemented use of DbProtect software to perform some of the required scanning functionality. DbProtect was the best available tool on the market at the time and met the IRS's immediate needs for a database scanning capability. As a result of on-going costs of DbProtect software and expanded business requirements, the IRS looked at other tools that could provide the scanning functionality. The IRS stated that they conducted a thorough analysis of available tools and made the decision to go with IBM Guardium. This analysis, which was shared with us, showed that the change to the new tool would save the taxpayers in the total cost of ownership compared to the total cost of ownership for DbProtect.

We maintain that the inefficient use of resources is not due to the selection of the IBM Guardium software application, but was caused instead by the delayed deployment that resulted from the lack of proper planning and coordination between the Modernization and Information Technology Services business units prior to the purchase of the application. These issues caused the deployment to be delayed until after the licenses needed to be renewed.

Recommendation 3: The Chief Technology Officer should ensure system requirements are identified and agreed upon by all affected Modernization and Information Technology Services organizations prior to purchasing an enterprise-wide software application.

Management's Response: The IRS agreed with this recommendation. Vendor Contract Management will ensure that all appropriate information technology stakeholders involved in the acquisition of enterprise software applications have been effectively engaged in the articulation of requirements for new enterprise-wide software applications.



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether adequate security controls had been established for the IBM DB2 databases running on the IBM z/OS operating system. The scope of this review was limited to the IBM DB2 database and only those operating systems and Resource Access Control Facility¹ functions directly related to the database. To accomplish our objective, we:

- I. Determined if the IRS established adequate security policies for the IBM DB2 databases.
 - A. Compared the IRS mainframe and IBM DB2 database policies and configuration guides to those published by the Department of the Treasury, the National Institute of Standards and Technology, and the Defense Information Systems Agency.
 - B. Compared the IRS mainframe and IBM DB2 database policies and configuration guides to those published by the Center for Internet Security and IBM.
- II. Determined if the IBM DB2 database programs, objects, and files were adequately protected and that adequate user access controls were in place.
 - A. Judgmentally selected two IBM DB2 production databases for review. The IRS has 32 IBM DB2 databases of which 28 were using the IBM z/OS operating system. Because automated scanning software had not been implemented, a manual review was performed. To limit the scope of the manual review, two Sensitive But Unclassified applications were selected that use the same subsystem (or logical partition) and were owned by the Wage and Investment Division. Both applications also shared the same installation of the security software, Resource Access Control Facility. We believe these two applications were typical of IRS processing of taxpayer data. They are the:
 - Electronic Tax Administration Marketing Database.
 - Tax Return Database.
 - B. Identified where the selected IBM DB2 subsystem resides on the mainframe.
 - C. Determined the IBM DB2 database options that were set.
 - D. Evaluated the controls over the connections to the IBM DB2 subsystem.

¹ See Appendix V for a glossary of terms.



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

- E. Verified that the IBM DB2 datasets are adequately protected.
 - F. Evaluated how user identifications are assigned.
 - G. Identified who can access tables for the selected subsystem.
 - H. Identified who can grant access permissions to other users.
 - I. Identified user privileges.
 - J. Checked to ensure that access permissions adequately protected the IBM DB2 database program files and audit logs.
- III. Determined the effectiveness of security testing conducted on the IBM mainframe and the IBM DB2 databases to identify vulnerabilities and the remediation actions taken.
- A. Reviewed policy checker reports for December 2010 through February 2011.
 - B. Reviewed the results of vulnerability or security testing performed December 2010 through February 2011.
 - C. Verified that the mainframe operating system and the IBM DB2 database application had all relevant security patches installed.
 - D. Discussed what remediation or corrective actions were taken to address problems identified by IRS testing.
 - E. Verified that outstanding problems were timely added to the appropriate Plan of Actions and Milestones reports.

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: the Cybersecurity and Enterprise Operations organizations' policies and procedures for establishing and monitoring IBM mainframe DB2 database security. We evaluated the controls by interviewing management, and reviewing policies and procedures and relevant supporting documentation. We tested the adequacy of DB2 database security by examining DB2 configurations for two IBM mainframe applications.



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

Appendix II

Major Contributors to This Report

Alan R. Duncan, Assistant Inspector General for Audit (Security and Information Technology Services)

Danny Verneuille, Director

Larry Reimer, Information Technology Audit Manager

Richard Borst, Senior Auditor

Stasha Smith, Senior Auditor

Elton Jewell, Information Technology Specialist

Monique Queen, Information Technology Specialist



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Deputy Chief Information Officer for Operations OS:CTO
Associate Chief Information Officer, Cybersecurity OS:CTO:C
Associate Chief Information Officer, Enterprise Operations OS:CTO:EO
Director, Enterprise Computing Centers OS:CTO:EO:EC
Director, Security Risk Management OS:CTO:C:SRM
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 Division OS:CTO:SP:RM



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

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; \$702,560 (see page 5).

Methodology Used to Measure the Reported Benefit:

In July 2010, the Cybersecurity organization purchased the IBM Guardium application for \$3.3 million, including hardware and an enterprise-wide software license for a 1-year period beginning July 30, 2010. The enterprise-wide software license covered the database servers within the IRS architecture regardless of the number of servers actually scanned.

The application was purchased to perform automated vulnerability scans on IRS databases. However, as of July 2011, the IBM Guardium application had not been fully implemented. In June 2011, the IRS received an invoice for approximately \$700,000 to renew the Guardium application license. This invoice was paid in order to continue deployment and avoid penalties for a lapse in maintenance. While the IRS used the software application several times to scan databases, it did not utilize the automated scanning functionality that had been purchased.



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

Appendix V

Glossary of Terms

Term	Definition
Application	A software program that performs a specific function directly for a user and can be executed without access to system control, monitoring, or administrative privileges.
Business Master File On-Line Processing	Is used primarily to display tax account information on business taxpayers.
Business Return Transaction File	These programs receive business tax return data, reformat and post returns to the Return Transaction File, and do periodic file maintenance.
Credential	An object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.
Customer Account Data Engine – Individual	An application that is scheduled to be phased in over several years, processing increasingly more complex tax returns in stages, ultimately replacing the tape-based Master File systems the IRS now uses to process tax return data. The Customer Account Data Engine Release 4.2 was successfully deployed on January 19, 2009. Note: This will be replaced by the Customer Account Data Engine 2 in January 2012.
Customer Account Data Engine 2	The technological foundation that will provide the IRS with the capability to manage its tax accounts in a way that is central to the achievement of the IRS modernization vision.
DB2 Database	A relational model database server developed by IBM.
Electronic Tax Administration Marketing Database	Creates and maintains a national database to profile individual and business return filers to support marketing and communications for e-submissions programs.



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

Term	Definition
Enterprise Life Cycle	In enterprise architecture, is the dynamic, iterative process of changing the enterprise over time by incorporating new business processes, new technology, and new capabilities, as well as maintenance, disposition, and disposal of existing elements of the enterprise.
Identification	The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an information technology system.
Least privilege	The security objective of granting users only those accesses they need to perform their official duties.
Mainframe	Powerful computers used primarily by corporate and governmental organizations for critical applications, bulk data processing such as census, industry and consumer statistics, enterprise resource planning, and financial transaction processing.
Objects	A passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object implies access to the information it contains.
Operating system	Software that runs on computers, manages computer hardware resources, and provides common services for execution of application software.
Patch	An update to an operating system, application, or other software issued specifically to correct particular problems with the software.
Platform	The hardware and software on a computer that allows software to run. Typical platforms include a computer's architecture, operating system, programming languages and related user interface (run-time system libraries or graphical user interface).
Privilege	A right granted to an individual, a program, or a process.
Resource Access Control Facility	An IBM security system that provides access control and auditing functionality for the z/OS and z/VM operating systems.



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

Term	Definition
Sensitive But Unclassified	A designation of information in the Federal Government that, though unclassified, often requires strict controls over its distribution.
Separation of duties	As a security principle, its primary objective is the prevention of fraud and errors. This objective is achieved by disseminating the tasks and associated privileges for a specific business process among multiple users.
System-software	The special software within the cryptographic boundary (e.g., operating system, compilers, or utility programs) designed for a specific computer system or family of computer systems to facilitate the operation and maintenance of the computer system, associated programs, and data.
Tax Return Database	Contains tax return source information for all electronically filed tax returns.
Tax Professional Preparer Tax Identification Number System	A web-based application that will be used by approximately 900,000 to 1.2 million tax return preparers. The application's main business goals are to facilitate taxpayer compliance and ensure uniform and high ethical standards of conduct for tax preparers.
Trusted Agent Federal Information Security Management Act	An automated management tool that maintains Federal Information Security Management Act of 2002 (44 U.S.C. Sections §§ 3541 – 3549) reporting data for application systems and their associated corrective actions.
User Permissions	The authorization that enables the user to access specific resources on a computer (e.g., data files and applications) or to network resources (e.g., printers and file servers).



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

Appendix VI

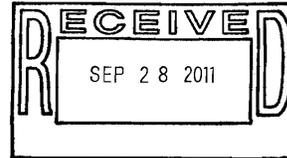
Management's Response to the Draft Report



CHIEF TECHNOLOGY OFFICER

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

SEP 28 2011



MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM:

Terence V. Milholland
Chief Technology Officer

Terence V. Milholland

SUBJECT:

Draft Audit Report – The Mainframe Databases Reviewed Met
Security Requirements; However, Automated Security Scans
Were Not Performed - (Audit # 201120021) (e-trak #2011-25428)

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 maintaining adequately configured databases operating in its IBM mainframe environment.

The attachment to this memo details our planned corrective actions to implement those recommendations with which we concur. We do not concur with TIGTA's assertion that the renewal of the IBM Guardium software application licenses was an inefficient use of resources. This invoice was paid in order to continue deployment and avoid penalties for a lapse in maintenance. In response to prior TIGTA recommendations we implemented use of DbProtect software to perform some of the required scanning functionality. DbProtect was the best available tool on the market at the time and met the IRS' immediate needs for a database scanning capability. As a result of on-going costs of DbProtect software and expanded business requirements we looked at other tools that could provide the scanning functionality. We conducted a thorough analysis of available tools and made the decision to go with IBM Guardium. This analysis, which was shared with TIGTA, showed that the change to the new tool would save the taxpayers in total cost of ownership (TCO) compared to the TCO for DbProtect.

If you have any questions, please or David Stender, Associate Chief Information Officer for Cybersecurity, at (202) 622-8809.

Attachment



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

Attachment

Draft Audit Report – The Mainframe Databases Reviewed Met Security Requirements;
However, Automated Security Scans Were Not Performed (Audit # 201120021) (e-trak #2011-
25428)

RECOMMENDATION #1: The Chief Technology Officer should implement automated security configuration scanning on mainframe databases.

CORRECTIVE ACTION #1: The IRS accepts the recommendation. The IRS will implement automated security configuration scanning on mainframe databases.

IMPLEMENTATION DATE: March 1, 2013

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 the IBM Guardium software application is fully implemented.

CORRECTIVE ACTION #2: The IRS is coordinating with stakeholders to fully implement the IBM Guardium software application. This includes: vulnerability scan testing of the various Database Management System (DBMS) platforms, account creation process, mitigation strategy for identified vulnerabilities, identifying appropriate database owners and system administrators across the enterprise and getting database administrators in all Business Units to create Guardium user accounts on their databases.

IMPLEMENTATION DATE: March 1, 2013

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 #3: The Chief Technology Officer should ensure system requirements are identified and agreed upon by all affected Modernization and Information Technology Services organizations prior to purchasing an enterprise-wide software application.



*The Mainframe Databases Reviewed
Met Security Requirements; However,
Automated Security Scans Were Not Performed*

Attachment

Draft Audit Report – The Mainframe Databases Reviewed Met Security Requirements;
However, Automated Security Scans Were Not Performed (Audit # 201120021) (e-trak #2011-
25428)

CORRECTIVE ACTION #3: We agree with this recommendation. Vendor Contract Management will ensure that all appropriate IT stakeholders involved in the acquisition of enterprise software applications have been effectively engaged in the articulation of requirements for new enterprise-wide software applications."

IMPLEMENTATION DATE: April 2, 2012

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Strategy & Planning

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.