TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Big Data Analytics General Support System Security Controls Need Improvement

June 9, 2017

Reference Number: 2017-20-029

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
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

To report fraud, waste, or abuse, call our toll-free hotline at:

1-800-366-4484

By Web:

www.treasury.gov/tigta/

Or Write:

Treasury Inspector General for Tax Administration
P.O. Box 589
Ben Franklin Station
Washington, D.C. 20044-0589

Information you provide is confidential and you may remain anonymous.

THE BIG DATA ANALYTICS GENERAL SUPPORT SYSTEM SECURITY CONTROLS NEED IMPROVEMENT

Highlights

Final Report issued on June 9, 2017

Highlights of Reference Number: 2017-20-029 to the Internal Revenue Service Chief Information Officer.

IMPACT ON TAXPAYERS

The Integrated Production Model (IPM) system is a centralized analytical data store that provides a single point of access to core taxpayer data. Security weaknesses could adversely affect tax administration and the protection of taxpayer data.

WHY TIGTA DID THE AUDIT

The IRS made a variety of significant changes to the IPM system, including moving its data to different software and hardware platforms. When these changes were made, business ownership and security responsibilities of the IPM system also changed and the IPM is no longer classified as a major application. The IPM system is now part of the Big Data Analytics (BDA) General Support System. The overall objective of this review was to determine whether the IPM system security has been effectively incorporated into the BDA General Support System.

WHAT TIGTA FOUND

The IRS did not follow its change management procedures when absorbing the IPM system into the BDA General Support System. IRS executives agreed to the IPM and BDA changes prior to going through the security change management process and notifying the Information Technology organization's Cybersecurity office. As a result, approximately 10 percent of security controls which previously protected the IPM system data were not captured by the BDA General Support System.

The IRS maintained Security Control Assessment and Authorization documents for the BDA General Support System but those documents were not updated after the IPM system was absorbed into its security boundary. For example, the BDA System Security Plan did not include information regarding the Information Handling and Retention security control, and the Information Flow Enforcement security control was not updated to include Interface Control Document requirements.

Further, TIGTA found 21 (40 percent) of 52 database administrator and service accounts on the BDA system had not been properly authorized through the Online 5081 application. Finally, the IRS did not properly complete and approve Interface Control Documentation for the IPM system's internal connections.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer: 1) ensure that the security change management process is followed; 2) establish a new Memorandum of Understanding to reflect all changes in responsibilities as a result of the IPM system's transition to the BDA security boundary; 3) evaluate the IPM system non-inherited security controls and ensure that these controls are included in the BDA General Support System's System Security Plan; 4) ensure that all BDA database administrator accounts and service accounts are compliant with the Online 5081 application requirements and that access is still required; and 5) ensure that all the IPM system's interfacing entities have properly completed and approved Interface Control Documents.

The IRS agreed with TIGTA's recommendations. Some of the planned corrective actions include evaluating the BDA System Security Plan to ensure that IPM information is included in the appropriate security controls; ensuring that existing BDA accounts are compliant with the Online 5081 application requirements and ensuring that the established Online 5081 process is followed before accounts are created; and establishing a procedure and a validation checklist that will require review of the Interface Control Documents to ensure that they are up-to-date, reviewed, and approved.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

June 9, 2017

MEMORANDUM FOR CHIEF INFORMATION OFFICER

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Big Data Analytics General Support System Security Controls Need Improvement (Audit # 201620022)

This report presents the results of our review of whether the Integrated Production Model system security has been effectively incorporated into the Big Data Analytics General Support System. This audit is included in our Fiscal Year 2017 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of Internal Revenue Service Resources.

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

Copies of this report are also being sent to the Internal Revenue Service managers affected by the report recommendations. If you have any questions, please contact me or Danny R. Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services).

Table of Contents

Appendices

Abbreviations

BDA	Big Data Analytics
GSS	General Support System
IPM	Integrated Production Model
IRS	Internal Revenue Service
IT	Information Technology

Background

The Integrated Production Model (IPM) system is a centralized analytical data store that provides a single point of access to core taxpayer data (such as taxpayer accounts and tax returns). It also provides other specific data used by a wide range of Internal Revenue Service (IRS) business applications to support case identification, selection, prioritization, delivery, and reporting. When the IRS Information Technology (IT) organization's Big Data Analytics (BDA) office (hereafter referred to as the BDA office) assumed responsibility for the IPM system, it was with the understanding that it would be absorbed by the BDA General Support System (GSS).[1]

All information systems must be covered by a System Security Plan and labeled as a major application or GSS. Specific System Security Plans for minor applications are not required because the security controls for those applications are typically provided by the GSS or major application in which they operate. The BDA GSS is made up of Greenplum data computing appliances that provide the IRS the ability to conduct advanced analytics, low latency data processing, as well as in-depth analysis of data. According to the BDA GSS System Security Plan, it is an infrastructure-only environment.[2]

This review was performed at the New Carrollton Federal Building in Lanham, Maryland, and the Enterprise Computing Center in Martinsburg, West Virginia, in the Applications Development, Cybersecurity, Enterprise Operations, and Enterprise Services IT offices, during the period March 2016 through January 2017. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[1] See Appendix IV for a glossary of terms.
[2] *IRS BDA System Security Plan*, Version 2.0, February 23, 2016.

Results of Review

The Internal Revenue Service Did Not Properly Follow Its Security Change Management Process

A change request for the migration of the IPM system's databases was submitted in 2014 to move the IPM system from a Solaris infrastructure to the BDA GSS Greenplum appliances owned by the BDA office. In April 2015, the ownership of this data was transferred from the Small Business/Self-Employed Division—the previous owners of the IPM system—to the BDA office. According to the Memorandum of Understanding between the Small Business/ Self-Employed Division, the IT organization's Applications Development organization, and the BDA office, 90 percent or more of IPM system security controls were inherited from the BDA GSS once the IPM system's data were migrated to the BDA GSS.

According to the National Institute of Standards and Technology, as part of the configuration change control,[3] an organization:

- Determines the types of changes to the information system that are configuration-controlled.
- Reviews proposed configuration-controlled changes to the information system and approves or disapproves such changes with explicit consideration for security impact analyses.
- Documents configuration change decisions associated with the information system.
- Implements approved configuration-controlled changes to the information system.
- Retains records of configuration-controlled changes to the information system.
- Audits and reviews activities associated with configuration-controlled changes to the information system.
- Coordinates and provides oversight for configuration change control activities.

[3] National Institute of Standards and Technology Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (January 2015); *security* control CM-3 (Configuration Change Control).

Additionally, the Internal Revenue Manual[4] requires the IRS to ensure that all business and functional unit owners utilize the IRS Federal Information Systems Modernization Act[5] guidance and the Security Configuration Management Standard Operating Procedures[6] for security change management. Further, the IRS IT organization Cybersecurity office policy states that the first step for a proposed security change is submitting a security change request for new information systems being introduced to the IRS infrastructure and for changes to existing information systems.

The IRS did not follow established procedures requiring the submission of a security change request for new information systems being introduced to the IRS infrastructure and for changes to existing information systems. The change request to move the IPM system to the BDA GSS security boundary was submitted on July 9, 2015; however, the IRS approved the move April 2015. The first documented instance of a change to the IPM system security boundary is located in a memorandum dated April 30, 2015, approving the transfer of the IPM system to the BDA GSS and the appointment of an authorizing official.[7] This occurred because IRS executives agreed to the IPM system change prior to going through the security change management process and notifying the IRS IT organization Cybersecurity office. The memorandum signed April 30, 2015, by authorizing officials of the Small Business/ Self-Employed Division and the BDA office executives signaled to stakeholders that the change had happened. The change request dated July 9, 2015, states that the IPM system's transition was approved six months prior to the change request. As a result of not following the established security change management process, approximately 10 percent of security controls which previously protected the IPM system data were not captured by the BDA GSS, as discussed further in the following section.

Without following the security change management process there is an increased risk that changes could expose the BDA GSS and its taxpayer data to additional security vulnerabilities. Changes to operating environments or applications introduce new or increase existing security vulnerabilities, heightening risk to the overall information technology infrastructure. The process of tracking and monitoring security-related changes to the IRS infrastructure is critical to effectively managing the individual information system and its supporting infrastructure as well as the information resources that support the daily activities of the IRS employees.

[4] Internal Revenue Manual 10.8.1 *Information Technology Security - Policy and Guidance* (July 8, 2015).
[5] Pub. L. No. 113-283. This bill amends chapter 35 of title 44 of the United States Code to provide for reform to Federal information security.
[6] *IRS Security Change Management Standard Operating Procedures*, Version 6.7, August 20, 2012.
[7] We reviewed prior change requests from January and December 2014, and there was no mention of a change in the IPM system's status as a major application.

Recommendation

Recommendation 1: The Chief Information Officer should ensure that the security change management process is followed prior to new information systems being introduced to the IRS infrastructure and for changes to existing information systems.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS Cybersecurity office completed a full review and update to the Security Change Management Standard Operating Procedures in March 2017 and ensured that it clearly stipulates that the security change management process must be followed prior to new information systems being introduced to the IRS infrastructure and for changes to existing information systems.

The Big Data Analytics General Support System Security Documentation Is Outdated

According to the Internal Revenue Manual,[8] the IRS is required to review and update its current security planning policy and procedures every three years or when there is a significant change. Examples of significant changes to an IRS information system include, but are not limited to:

- Installation of a new or upgraded operating system, middleware component, or application.
- Modification to system ports, protocols, or services.
- Installation of a new or upgraded hardware platform or firmware component.
- Modification to cryptographic modules or services.

Further, the Internal Revenue Manual requires the IRS to review the System Security Plan at a minimum annually (or as a result of a significant change). The IRS is also required to update the plan to address changes to the information system or when problems are identified during plan implementation or Security Control Assessments.

Although the IRS maintained Security Control Assessment and Authorization documents for the BDA GSS, those documents, specifically its System Security Plan, were not updated following the IPM system being absorbed into its security boundary. According to a Security Control Assessment performed in February 2016, as part of the BDA's annual Security Control Assessment, the IRS determined the BDA GSS System Security Plan was not fully updated to address all of the components for the BDA GSS, specifically the IPM system. We determined the security controls for the BDA GSS were not updated to include the non-inherited IPM security controls.

[8] Internal Revenue Manual 10.8.1 *Information Technology Security - Policy and Guidance* (July 8, 2015).

When the IPM system was owned by the Small Business/Self-Employed Division, the IPM System Security Plan accounted for the necessary security controls that were specific to protect the IPM system's data, but not all controls were inherited by the BDA GSS, as previously discussed. IRS personnel stated that this group of non-inherited security controls that were used to protect the IPM system's data prior to its transition to the BDA GSS infrastructure were no longer necessary. However, based on our assessment those controls are needed because the BDA GSS was designed as an infrastructure-only environment, according to the BDA GSS System Security Plan. In this context, "infrastructure-only" refers to hardware and software deployed for use enterprise-wide, without directly addressing project-specific requirements.

For example, we reviewed the IPM system security controls that were not inherited by the BDA GSS and identified:

- In the most recent IPM System Security Plan, the Information Handling and Retention security control (SI-12) from the National Institute of Standards and Technology guidance deals with how an organization handles and retains information within the information system and information output from the system in accordance with applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements. However, the most recent BDA GSS System Security Plan states this control is not applicable, even though the IPM system does handle and retain information.

Additionally, the respective IPM system and the BDA GSS System Security Plans both address the same security controls, but the means in which they address these controls differ.

- The implementation of the Information Flow Enforcement security control (AC-4) in the IPM System Security Plan requires internal connections to be documented in Interface Control Documents. The BDA GSS System Security Plan has not been updated to reflect those requirements.

The IRS did not follow its security change management process; did not update the BDA GSS System Security Plan to fully address all of the components for the BDA GSS, specifically the IPM system; and did not update its Memorandum of Understanding between the BDA office and the Applications Development organization that included the Applications Development organization's responsibilities when the IPM system moved under the BDA's GSS security boundary. As a result, the Applications Development organization was unclear of its responsibilities with regard to the controls and assumed the BDA GSS was responsible for implementing the IPM system's non-inherited controls.

Because the Memorandum of Understanding, which included the Applications Development organization's responsibilities, was not updated after the memorandum transferring ownership from the Small Business\Self-Employed Division to the BDA office, the Applications Development organization cannot be held accountable for performing responsibilities included in the agreement. Further, the BDA GSS has no assurance that the Applications Development

organization continues to maintain effective security controls for the development, management, operation, and security posture between the IPM system and the BDA GSS infrastructure.

Recommendations

The Chief Information Officer should:

Recommendation 2: Ensure that a new Memorandum of Understanding between the BDA office and the Applications Development organization is established to reflect all changes in responsibilities as a result of the IPM system's transition to the BDA GSS security boundary.

> ***Management's Response:*** The IRS agreed with this recommendation. Enterprise Services currently has a Memorandum of Understanding between Enterprise Services and Applications Development organization's Data and Delivery Services. The Enterprise Services and Applications Development organization agreed to update the Memorandum of Understanding by July 15, 2017, to reflect all changes in roles and responsibilities as a result of the IPM system's transition to the BDA GSS security boundary.

Recommendation 3: Evaluate the IPM system non-inherited security controls and ensure that these controls are included in the BDA GSS System Security Plan.

> ***Management's Response:*** The IRS agreed with the recommendation. The IT organization's Cybersecurity office will evaluate the BDA GSS System Security Plan to ensure that IPM information is included in the appropriate security controls.

Unauthorized Accounts Are Operating Within the Big Data Analytics General Support System

The National Institute of Standards and Technology[9] requires approval for requests to create information system accounts, including service accounts, and further defines information system account types to include individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service accounts. The Internal Revenue Manual[10] also requires the application owner to ensure that an IRS-approved access control (*e.g.*, Online 5081 application) request is submitted for traceability of all service accounts.

Per the BDA GSS System Security Plan dated April 13, 2016, the Online 5081 application is used to document access requests, modifications, and terminations for all types of users, including system administrators, system accounts requiring File Transfer Protocol access, and test accounts. When a new user needs access to the IRS systems, the user's manager or

[9] National Institute of Standards and Technology, Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (January 2015); *security* control AC-2 (Account Management).
[10] Internal Revenue Manual 10.8.1 *Information Technology Security, Policy and Guidance* (July 8, 2015).

designated official accesses the Online 5081 application to request access for the new user. The Online 5081 application is an online form which requires information such as the name of the system or application, type of access, and the manager's signature approving authorization of access. According to the IRS, the BDA GSS currently has four categories of accounts: built-in superuser, role, service, and database administrator. Of these four categories, only service accounts and database administrator accounts must go through the Online 5081 application for approval.

The IRS did not follow existing policy regarding system access and approval. For the BDA GSS, we found 21 (40 percent) of 52 accounts were not authorized through the Online 5081 application. We divided these accounts into the two categories required to follow the Online 5081 process and determined three (23 percent) of 13 database administrator accounts and 18 (46 percent) of 39 service accounts were not approved.

In some cases, database administrator account requests were denied because the administrator did not properly register through the Employee User Portal. After these database administrator users were initially denied, they then registered with the Employee User Portal. According to IRS personnel, when they resubmitted approval requests through the Online 5081 application they were again denied, this time because their accounts already existed on the BDA GSS. The BDA office is taking steps to remediate the issue as it pertains to database administrators by realigning the sequence of approvals so that registration with the Employee User Portal has already been verified before database administrators approve and create new accounts.

The overarching cause for both service and database administrator accounts existing without Online 5081 application approval is due to accounts being created on the system prior to being fully approved through the existing process. Improper account management increases the risk of an unauthorized user gaining access to sensitive and privileged data such as a taxpayer's Personally Identifiable Information including date of birth and Social Security Number.

Recommendation

Recommendation 4: The Chief Information Officer should enforce current request and approval policy for all the BDA GSS database administrator accounts and service accounts to ensure that these accounts are compliant with the Online 5081 application requirements and that access is still required.

> ***Management's Response:*** The IRS agreed with this recommendation. Enterprise Services will ensure that all existing BDA database administrator accounts and service accounts are compliant with the Online 5081 application requirements and that access is still required. Additionally, Enterprise Services will collaborate with the Enterprise Operations Online 5081 organization to modify the approval path for BDA database administrator account requests to ensure that the established Online 5081 process is followed before accounts are created.

Interface Control Documents Are Not Complete

The purpose of the Interface Control Document is to establish an agreement of responsibilities among the organizations owning the interfacing entities. The IPM System Security Plan states that all IPM connections to internal IRS systems will be documented in Interface Control Documents that provide details regarding the configuration of each connection along with the authorization.

We used the IPM Design Specification Report to determine what IPM system inputs would need Interface Control Documents. In a previously issued report,[11] we determined there were 27 interconnecting IPM system interfaces. We found that three (11 percent) of 27 connecting interfaces did not have Interface Control Documents. We reviewed the existing 24 documents and none were properly approved.

The IRS did not follow its guidance for completing Interface Control Documents. Required signatures and dates for all Interface Control Documents were missing. We determined that roles and responsibilities were not clearly known and understood by the IRS employees following the transition of the IPM system to the BDA GSS. Without completed Interface Control Documents, the IRS cannot hold connecting interface owners accountable for maintaining security requirements for the interfacing entities in order to maintain an effective security posture.

Recommendation

Recommendation 5: The Chief Information Officer should ensure that all IPM system interfacing entities have properly completed and approved Interface Control Documents and all future Interface Control Documents follow existing guidance.

> ***Management's Response:*** The IRS agreed with the recommendation. The Applications Development organization's Data Delivery Services will establish a procedure in the Project Management Plan and a validation checklist will require review of the Enterprise Life Cycle Interface Control Documents. The procedure will apply to any existing or new IPM interfaces to ensure that the Interface Control Documents are up-to-date, reviewed, and approved.

[11] Treasury Inspector General Tax Administration, Ref. No. 2016-20-058, *The Integrated Production Model Increases Data Access Efficiency; However, Access Controls and Data Validation Could Be Improved* p. 4 (July 2016).

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether IPM system security has been effectively incorporated into the BDA GSS. To accomplish our objective, we:

I. Determined whether the IRS has policies and procedures for system changes.

- A. Identified Federal and Internal Revenue Manual policies and procedures in place to govern system changes.
- B. Identified IRS definitions for significant system changes.
- C. Interviewed personnel to determine what processes and procedures were followed to transfer the IPM system to the BDA GSS Greenplum appliances.

II. Determined whether proper security documentation was maintained for the IPM system preceding and while transitioning the IPM system into the BDA GSS.

- A. Reviewed IRS policies and procedures, internal directives, and correspondence to determine what IPM system documentation needed to be maintained or updated during the transition of the IPM system into the BDA GSS boundary.
- B. Obtained and reviewed the IPM system security documentation to determine whether documents were correctly updated in accordance with IRS policies.

III. Determined whether the IRS IT organization took the required steps to ensure that the BDA GSS Security Control Assessment and Authorization package was updated and is compliant with IRS and other Federal policies after the system change.

- A. Determined whether Federal and Internal Revenue Manual policies and procedures required updates to the Security Control Assessment and Authorization package as a result of a major application transfer.
- B. Interviewed IRS officials to determine whether a risk assessment was performed to determine the security impact on the BDA GSS as a result of absorbing the IPM system.
- C. Determined whether the appropriate Security Control Assessment and Authorization documentation for the BDA GSS was updated based on the risk assessment results.

IV. Determined whether security controls are in place to prevent unauthorized access to the IPM BDA GSS data.

A. Obtained and reviewed security policy and procedure documentation to gain an understanding of the processes in place for managing and monitoring access to the IPM BDA GSS data.

B. Determined the various levels of access an end user can obtain and the roles associated with the level of access (*i.e.*, end users, privileged user).

C. Determined how user access is granted for the IPM BDA GSS.

D. Determined whether connecting interfaces are properly authorized by reviewing Interface Control Documents.

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 that the following internal controls were relevant to our audit objective: National Institute of Standards and Technology Special Publication requirements for system development life cycle and security controls over Federal information systems, Internal Revenue Manual policies related to access control management and system changes, and IRS IT organization Cybersecurity office Security Change Management Standard Operating Procedures. Through interviews with the IRS, we gained an understanding of policies and procedures related to IRS system change management program. Significant deficiencies we identified with the transition of the IPM system to the BDA GSS security boundary and security weaknesses are presented in the audit results section of this report.

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Acting Assistant Inspector General for Audit (Security and Information Technology Services)
John L. Ledford, Director
Jena Whitley, Audit Manager
Jason McKnight, Lead Auditor
Khafil-Deen Shonekan, Senior Auditor

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, Enterprise Services
Director, Office of Audit Coordination

Appendix IV

Glossary of Terms

Term	Definition
Authorizing Official	The official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.
Cryptographic	Pertaining to, or concerned with, cryptography.
Employee User Portal	A web hosting infrastructure that supports an intranet portal which allows IRS employees to access business applications and data.
Enterprise Computing Center	Supports tax processing and information management through a data processing and telecommunications infrastructure.
Enterprise Life Cycle	A framework used by IRS projects to ensure consistency and compliance with government and industry best practices.
Firmware	The programs and data components of a cryptographic module that are stored in hardware within the cryptographic boundary and cannot be dynamically written or modified during execution.
General Support System	An interconnected set of information resources under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, and people.
Greenplum	Appliances purchased from the Dell EMC Corporation and commodity servers used for data staging. The appliances are considered commercial off-the-shelf products with modifications to conform to IRS Internal Revenue Manual requirements.
Information Technology Organization	The IRS organization responsible for delivering information technology services and solutions that drive effective tax administration to ensure public confidence.

Term	Definition
Interface Control Document	Technical document describing interface controls and identifying the authorities and responsibilities for ensuring the operation of such controls. This document is baselined during the preliminary design review and is maintained throughout the information system life cycle.
Memorandum of Understanding	A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. A Memorandum of Understanding defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.
National Institute of Standards and Technology	A part of the Department of Commerce that is responsible for developing standards and guidelines for providing adequate information security for all Federal agency operations and assets.
Oracle Database	A collection of data treated as a unit. The purpose of a database is to store and retrieve related information.
Role Account	It is frequently convenient to group users together to ease management of object privileges: that way, privileges can be granted to, or revoked from, a group as a whole. In the Greenplum Database this is done by creating a role that represents the group, and then granting membership in the group role to individual user roles.
Service Account	Represents a process or a set of processes to manage authentication service operations with the operating system and/or network resources.
Solaris	Solaris is the UNIX based operating system of Sun Microsystem.
Superuser Account	A user who has been given permission to logon to a specific Linux/UNIX computer system and use an authorized subset of "root" special privileges.
System Security Plan	A formal document that provides an overview of the security requirements for the information system and describes the security controls in place or planned for meeting those requirements.

Appendix V

Management's Response to the Draft Report

CHIEF INFORMATION OFFICER

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

MAY 11 2017

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: S. Gina Garza
Chief Information Officer

SUBJECT: Draft Audit Report–The Big Data Analytics General Support System Security Controls Need Improvement (Audit # 201620022) (etrak # 2017-91699)

Thank you for the opportunity to review the draft audit report and meet with the audit team to discuss early report observations. As the report indicates, the IRS moved its Integrated Production Model (IPM) system to the Big Data Analytics (BDA) General Support System (GSS), and in doing so, made changes to its hardware and software environments. This move provided the IRS the ability to conduct advanced analytics, low latency processing, and in-depth analysis of data.

The IRS has well defined processes and controls to ensure the security of our IT systems. We continue to refine and mature our approaches to align with technology changes. Improvements to our security change management processes have already been made to manage our environment and we are refining our security documentation and subsequent approval processes. However; while the security change management process was not fully followed, the technical security controls were fully addressed and assessed within the BDA security boundary, the IPM security controls that were not captured were primarily documentation related management controls. At no time was the IPM data put at risk because of unassessed security controls.

The attached is our detailed planned corrective actions to implement the audit team's recommendations. The IRS values your continued support and the assistance your organization provides. If you have any questions, please contact Sharon James, ACIO Cybersecurity, at (202) 317-7061.

Attachment

Attachment

Draft Audit Report – The Big Data Analytics General Support System Security Controls Need Improvement (Audit # 201620022) (etrak- 2017-91699)

RECOMMENDATION #1: The Chief Information Officer should ensure that the security change management process is followed prior to new information systems being introduced to the IRS infrastructure, and for changes to existing information systems.

CORRECTIVE ACTION #1: IRS agrees with this recommendation. IRS Cybersecurity completed a full review and update to the Security Change Management Standard Operating Procedures in March 2017 and ensured that it clearly stipulates that the security change management process must be followed prior to new information systems being introduced to the IRS infrastructure and for changes to existing information systems.

IMPLEMENTATION DATE: Completed – March 31, 2017

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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

RECOMMENDATION #2: Ensure that a new Memorandum of Understanding between the BDA office and the Applications Development organization is established to reflect all changes in responsibilities as a result of the IPM system's transition to the BDA GSS security boundary.

CORRECTIVE ACTION #2: IRS agrees with this recommendation. Enterprise Services (ES) currently has a Memorandum of Understanding (MOU) between ES and Applications Development's Data and Delivery Services (AD DDS). ES and AD agree to update MOU to reflect all changes in roles and responsibilities as a result the IPM system's transition to BDA GSS security boundary by July 15, 2017.

IMPLEMENTATION DATE: July 15, 2017

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Services

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

RECOMMENDATION #3: Evaluate the IPM system non-inherited security controls and ensure these controls are included in the BDA GSS System Security Plan.

CORRECTIVE ACTION #3: IRS agrees with this recommendation. IT Cybersecurity will evaluate the BDA GSS System Security Plan to ensure IPM information is included in appropriate security controls.

Attachment

Draft Audit Report – The Big Data Analytics General Support System Security Controls Need Improvement (Audit # 201620022) (etrak- 2017-91699)

IMPLEMENTATION DATE: July 15, 2017

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Cybersecurity

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

RECOMMENDATION #4: The Chief Information Officer should enforce current request and approval policy for all the BDA GSS database administrator accounts and service accounts to ensure that these accounts are compliant with the Online 5081 application requirements and that access is still required.

CORRECTIVE ACTION #4: IRS agrees with this recommendation. Enterprise Services (ES) will ensure all existing BDA database administrator accounts and service accounts are compliant with the Online 5081 application requirements and that access is still required. Additionally, ES will collaborate with EOps Online 5081 organization to modify the approval path for BDA DBA account requests to ensure that they follow the established online 5081 process before accounts are created.

IMPLEMENTATION DATE: July 15, 2017

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Enterprise Services

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

RECOMMENDATION #5: The Chief Information Officer should ensure that all IPM system interfacing entities have properly completed and approved Interface Control Documents and all future Interface Control Documents follow existing guidance.

CORRECTIVE ACTION #5: The IRS agrees with the recommendation. Applications Development, Data Delivery Services will establish a procedure in the Project Management Plan and a validation checklist that will require review of the ELC Interface Control Documents. The procedure will apply to any existing or new IPM interfaces to ensure the ICDs are up-to-date, reviewed, and approved.

IMPLEMENTATION DATE: September 15, 2017

RESPONSIBLE OFFICIAL: Associate Chief Information Officer, Applications Development (Data Delivery Services Domain)

Attachment

Draft Audit Report – The Big Data Analytics General Support System Security Controls Need Improvement (Audit # 201620022) (etrak- 2017-91699)

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