Audit Report

OIG-15-042

INFORMATION TECHNOLOGY: Fiscal Service's Management of Virtual Servers Needs Improvement

August 19, 2015

Office of Inspector General

Department of the Treasury

Contents

Audit Report

Appendices

Abbreviations and Acronyms

APL	Approved IT Products List
ARM	Application Reference Model
EICAM	Enterprise Identity Credentialing and Access Management
EITI	Enterprise Information Technology Infrastructure
ERT	Enterprise Recertification Tool
IT	Information Technology
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
SP	Special Publication
SSP	System Security Plan
TD P	Treasury Directive Publication
TRM	Technical Reference Model

This Page Intentionally Left Blank

August 19, 2015

Sheryl Morrow
Commissioner, Bureau of the Fiscal Service

This report represents the results of our audit of the security controls over virtual servers used by the Bureau of the Fiscal Service (Fiscal Service). The overall objective of this audit was to determine whether controls were in place for securing data stored on virtual servers[1] and virtual hosts[2] that were located in Fiscal Service's consolidated data centers. Fiscal Service was selected for audit because there were more virtual hosts located at its consolidated data centers than at other Department of the Treasury (Treasury) bureaus and offices.

To accomplish our audit objective, we surveyed Treasury bureaus and offices to assess how virtual server technology has been implemented; interviewed key officials and personnel at Fiscal Service; reviewed and analyzed security-related documentation; and observed security control configurations demonstrated by technical personnel. Appendix 1 provides more detail on our objective, scope, and methodology.

[1] The term "virtual server" as used in this report is a virtualized computer that functions as a server, as contrasted with one that functions as a workstation or other system.
[2] A virtual host is a computer that runs one or more virtualized computers and controls the flow of instructions between the virtualized computers and physical hardware, such as the central processing unit (CPU), disk storage, memory, and network interface cards.

Results in Brief

We determined that Fiscal Service had security controls in place for securing data on the virtual servers selected for our review. However, we found that improvement is needed in the management of those servers for ensuring compliance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3,[3] as well as Treasury's and Fiscal Service's policies and procedures. Specifically, we found that Fiscal Service lacked an enterprise-wide inventory to account for all of its virtual servers. We also noted that a complete and accurate centralized inventory of approved software was not maintained. Lastly, we identified five active administrative accounts on Unix virtual servers that were not disabled upon separation of employees and contractors.

Overall, we are making five recommendations to management to address the deficiencies identified. First, we recommend that management create and maintain a complete enterprise-wide inventory of virtual servers in its environment. With regard to the software on those servers, we recommend that management ensure an approved centralized software inventory across Fiscal Service's lines of business is created, maintained, and regularly updated to ensure that only approved software is included. Accordingly, we also recommend that software is timely removed from virtual servers when retired. We recommend that management ensure that staff responsible for the account management function is aware of Fiscal Service's exit procedures so that inactive user accounts are disabled and administrative privileges are immediately removed when no longer needed. In this regard, we also recommend that periodic reviews of administrative accounts be performed in accordance

[3] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* (Aug. 2009)

with NIST SP 800-53 and Fiscal Service's policies and procedures.

As a separate matter, we provided some of our observations regarding communication among Fiscal Service's Information Technology (IT) management functions responsible for Fiscal Service's virtual servers. In particular, we noted that critical information was not being shared among staff managing the virtual servers. We were concerned that the current channels of communication may risk Fiscal Service's ability to respond timely to IT emergencies such as a critical patch installation or cyber security incident. Although we did not identify any weaknesses in the security controls over the virtual servers, we believe it would be prudent that management assess its current IT processes and functions in order to identify opportunities to improve information sharing and collaboration among IT teams. More detail regarding our observations is provided later in this report.

In a written response, management agreed with our findings and recommendations and stated that remediation plans to address the deficiencies identified in this report have been developed along with targeted implementation dates. Overall, we found that management's response meets the intent of our recommendations. We have summarized and evaluated management's response in the recommendation sections of this report. Management's response is provided in appendix 2.

Background

Server virtualization is a term used to describe the environment where one or more servers' operating systems and the applications on them are run on one host machine. The goal of virtualization is to centralize administrative tasks, improve scalability, and improve overall hardware resource utilization. Virtualization can also reduce overhead costs which makes it an attractive option to users, including Federal agencies. However, security for virtualization can be problematic. For example, combining many virtualized computers onto a single physical computer can result in a larger operational impact if security is

compromised. Additionally, due to the dynamic environment of virtualization, creating and maintaining security boundaries becomes more complex.

Fiscal Service's mission is to promote the financial integrity and operational efficiency of the Federal government through exceptional accounting, financing, collections, payments, and shared services. Fiscal Service uses virtualization to support infrastructure operations and business functions within Treasury components and other governmental agencies, as well as general computing services within the Bureau. Fiscal Service's virtual servers reside primarily at data centers located in Parkersburg, West Virginia, and Kansas City, Missouri.

Results of Audit

Finding 1 Fiscal Service Lacked an Enterprise-Wide Inventory of Virtual Servers

Fiscal Service did not maintain an enterprise-wide inventory of its virtual servers, and as a result, could not provide complete information for all of them. Instead, there were several lists of virtual servers which were assembled from various sources including system management software, print-outs, spreadsheets, and in some instances, the partial recollection of system administrators across the different branches within Fiscal Service. These lists lacked sufficient detail regarding the purpose and function of the virtual servers, the applications and operating systems running on them, their system owners, and the physical server(s) on which they reside. Additionally, the lists contained inaccurate and out of date information.

According to the NIST SP 800-53, Revision 3, federal organizations must develop, document, and maintain an inventory of information system components that accurately reflects the current information system, is at the level of granularity deemed necessary for tracking and reporting, and is available for review and audit by designated organizational officials. Additionally, Fiscal Service requires that the organization develop, document, and maintain an inventory of

information system components as part of its *Enterprise Information Technology Infrastructure (EITI) System Security Plan (SSP).*[4] The inventory must include information on hardware specifications (e.g., manufacturer, type, model, serial number, physical location), software licensing, information system/component owner(s), and for a networked component or device, the machine name and network address. Since all of Fiscal Service's virtual servers are part of the EITI, they must be protected by security controls required by the EITI SSP.

When we inquired as to why a single enterprise-wide inventory was not maintained, the Information Security Services Deputy Assistant Commissioner explained that Fiscal Service employed software to scan and inventory its virtualized environment which did not fully meet the bureau's needs. He also stated that Fiscal Service recognized problems with the software in early 2014 and engaged its vendor to troubleshoot the issues. The Director of the Division of Service Management informed us that the bureau has also been pursuing a new product that should improve the current scanning shortcomings, and staff were still learning the capabilities of this new product.

As a result of lacking a reliable enterprise-wide inventory, we were unable to determine whether the universe of virtual servers was complete. Furthermore, we believe there are potential impacts that could negatively affect Fiscal Service's operations. That is, without a complete and reliable enterprise-wide inventory, Fiscal Service staff may experience delays in responding to security incidents, unexpected maintenance requirements, and regulatory requests. Regular maintenance such as patching and antivirus management may also be affected. Finally, Fiscal Service management may not be able to determine whether all virtual servers are compliant with federal

[4] An SSP provides an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements, responsibilities and expected behavior of all individuals who access the system.

information system security laws and regulations, as well as Treasury's directives and policies.

Recommendation

1. We recommend that the Commissioner of the Bureau of the Fiscal Service ensure that a complete enterprise-wide inventory of virtual servers in Fiscal Service's environment is created and maintained.

   Management Response

   Management agreed with our recommendation and noted that a remediation plan was developed to ensure full implementation of their Configuration Management Program, revise policies and procedures, and increase staff awareness. Completion is scheduled for March 31, 2016.

   OIG Comment

   Management's response meets the intent of our recommendation.

Finding 2 Software Assets Were Not Effectively Managed

Fiscal Service did not maintain a complete and accurate centralized inventory of approved software as required by NIST SP 800-53, Revision 3, Treasury Directive Publication (TD P) 85-01 *Treasury Information Technology Security Program*, and Fiscal Service's own policy. In our review of Fiscal Service's virtual servers, we found that a retired software application was installed on one of the servers in our sample.

In order to determine whether software applications installed on the virtual servers in our sample were approved, we requested an approved software list. Fiscal Service's audit liaison initially provided us with a list of approved software included in the

"Technical Reference Model" (TRM).[5] However, of the sampled servers we tested, we found that six installed software applications were missing from this list. When we requested clarification of the discrepancy, the Information Security Services Deputy Assistant Commissioner referred us to another approved software list, the "Approved IT Products Listing" (APL), but noted that neither the TRM nor the APL were consistently maintained or relied upon. Still, we found that the APL only included 5 of the 6 software applications missing from the TRM, which left 1 application[6] not approved on either list. Upon further inquiry, the Director of the Division of Service Management stated that this software application was retired and its presence on the virtual server was an oversight.

We also raised the question as to why there were multiple lists of approved software and were informed that there was yet a third list, the "Application Reference Model" (ARM).[7] According to the Chief Security Officer the ARM replaced the TRM. Additionally, he stated that the bureau has been aggressively working toward the design and implementation of a Fiscal Service-wide Software Asset Management Program. This program generated a fourth list that is a consolidated Fiscal IT APL.

According to NIST SP 800-53, Revision 3, organizations must maintain a "blacklist" of software not permitted for a moderate impact system[8] such as EITI. Fiscal Service's SSP for EITI requires that the bureau substitute a more stringent requirement and maintain a "whitelist" of software that is permitted, thereby

[5] A TRM is a framework used to categorize the standards, specifications, and technologies that support and enable the delivery of IT services.
[6] Hercules Remediation Client for Windows is an automated vulnerability remediation tool by McAfee that reached its end of life in September 2009.
[7] An ARM is a framework used to categorize the software standards and technologies that support and enable the delivery of IT and business services.
[8] *Federal Information Processing Standard 199* defines Low, Moderate, and High categories. Organizations categorize their systems based on risk and apply one of the three baselines as appropriate.

excluding all other software from running. As we noted above, Fiscal Service maintained multiple whitelists. Furthermore, TD P 85-01 requires the heads of bureaus and offices to establish and maintain an accurate software inventory.

The lack of a complete and accurate centralized inventory of approved software can impact Fiscal Service's ability to manage approved software efficiently in several ways. For example, de-authorized software may inadvertently run in Fiscal Service's environment when it is not removed from one of the approved inventory lists, such as the one missing from the whitelists, TRM and APL, noted above. Similarly, software approved on one inventory list but not on another list may not be consistently be deployed. Furthermore, de-authorized software may be unpatched or contain vulnerabilities that could provide unauthorized access to systems and data. The lack of a centralized inventory of approved software also poses a risk that Fiscal Service may potentially run more software copies than legally permitted, and therefore, be subject to fines and other legal actions.

Recommendations

We recommend that the Commissioner of the Bureau of the Fiscal Service:

1. Ensure an approved centralized software inventory across Fiscal Service's lines of business is created, maintained, and regularly updated to ensure that only approved software is included.

   Management Response

   Management agreed with our recommendation and responded that a remediation plan was developed to create a single approved software inventory and implement revised policies and procedures for ensuring the list is regularly updated. Completion is scheduled for March 31, 2016.

OIG Comment

Management's response meets the intent of our recommendation.

2. Ensure that software is timely removed from virtual servers when retired.

Management Response

Management agreed with our recommendation and responded that a remediation plan was developed to review service provider compliance beginning March 31, 2016.

OIG Comment

Management's response meets the intent of our recommendation.

Finding 3 Some Unix Administrative Accounts Were Not Disabled

Fiscal Service did not disable user accounts upon separation of employees and contractors as required by NIST SP 800-53, Revision 3, and Fiscal Service's own exit clearance policies and procedures. That is, we found five user accounts with administrative privileges on Unix virtual servers were not disabled as of August 2014. Three of these accounts belonged to contractors who separated from Fiscal Service as far back as May and June of 2012. The remaining two accounts belonged to employees who had transferred to different units within Fiscal Service in November 2013 and May 2014.

NIST SP 800-53, Revision 3, requires organizations to manage information system accounts, including deactivating accounts of terminated or transferred users, and reviewing accounts at a frequency defined by the organization. Fiscal Service's EITI SSP

and the *Unix Account Management Version 0.5* define the frequency of recertification[9] for privileged accounts as at least twice annually. Fiscal Service specifies in its *Exit Clearance Program Standard Operating Procedure* that user accounts be suspended within 2 business days of employee separation from the bureau. In the case of an internal transfer, Fiscal Service's *Enterprise Identity Credentialing and Access Management* (EICAM) *Exit Clearance and Validation Process* requires that accounts be disabled within 1 day of transfer or notification of transfer, whichever comes first.

The Director of EICAM informed us that System Owners and Information System Security Officers are responsible for account recertification. His organization supports recertification processes through its reporting mechanisms and the Enterprise Recertification Tool (ERT). However, ERT can only facilitate recertification for systems on which it is installed and the last automated recertification for some of the user accounts was completed in 2011. Furthermore, the manager of the Unix Administration Branch/Division of Platform Services stated that he has no recollection of a manual recertification being done, and that he relied solely on automated recertification. However, he was aware that after operating system upgrades on servers were performed, ERT had issues. Consequently, Fiscal Service could not provide evidence that they had reviewed or recertified Unix privileged accounts on a semi-annual basis in accordance with its exit policies.

Privileged accounts that are not timely removed when no longer needed provide opportunities for unauthorized use of a system, including modification, deletion, or access of information and system files. Even if there are compensating controls preventing the original account holder from logging in, unused accounts are attractive targets for hackers. Unauthorized activities from these

[9] Recertification is the process of reviewing existing accounts to ensure they are still needed and have the appropriate permissions.

privileged accounts could possibly go undetected, as the actions are originating from what appears to be an authorized source.

In response to our discovery of the five user accounts in question, the Director of EICAM reported that the separated users were removed and the transferred users had their access privileges modified in August 2014.

Recommendations

We recommend that the Commissioner of the Bureau of the Fiscal Service:

1. Ensure that staff responsible for account management is aware of Fiscal Service's exit procedures so that inactive user accounts are disabled and administrative privileges are immediately removed when no longer needed.

   Management Response

   Management agreed with our recommendation and responded that it developed a remediation plan to train appropriate staff on exit clearance processes and standard operating procedures by May 31, 2016.

   OIG Comment

   Management's response meets the intent of our recommendation.

2. Ensure that periodic reviews of administrative accounts are performed in accordance with NIST SP 800-53 and Fiscal Service policies and procedures.

   Management Response

   Management agreed with our recommendation and responded that a remediation plan was developed to design and configure semi-annual UNIX automated administrative account recertifications. The targeted completion date is May 31, 2016.

OIG Comment

Management's response meets the intent of our recommendation.

Matter of Concern

Over the course of the audit, we noted communication issues among the IT management functions responsible for Fiscal Service's virtual servers that we believe needs the attention of management. That is, we observed that the organization operated in narrow organizational "stovepipes" wherein some critical information regarding the virtual servers being managed collectively was not being shared. To obtain complete information regarding each virtual server in our sample required input from at least six separate branches.

IT management and staff had difficulty providing complete documentation and other requested information. For example, those managing operating systems on virtual servers did not have all required information about the system owner(s) and applications running on the virtual servers. Furthermore, there were instances when IT management and/or staff were unable to direct us to the correct source for the requested information. Also, there were several occasions when we were provided conflicting information from multiple branches sharing responsibility for the servers in question.

We have serious concerns that the current channels of communication may cause delays or inhibit Fiscal Service's ability to respond to IT emergencies such as a critical patch installation or cyber security incident. As such, it would be prudent for management to assess the current IT processes and functions to identify opportunities to improve information sharing and collaboration among IT teams.

In its *Standards for Internal Control in the Federal Government*, the Government Accountability Office provides that as part of an entity's organizational structure, "management considers how units interact in order to fulfill their overall responsibilities.

Management establishes reporting lines within an organizational structure so that units can communicate the quality information necessary for each unit to fulfill its overall responsibilities. Based on the nature of the assigned responsibility, management chooses the type and number of discrete units, such as divisions, offices, and related subunits. Reporting lines are defined at all levels of the organization and provide methods of communication that can flow down, across, up, and around the structure. Management also considers the entity's overall responsibilities to external stakeholders and establishes reporting lines that allow the entity to both communicate and receive information from external stakeholders."[10]

* * * * * *

I would like to extend my appreciation to the Fiscal Service staff for the cooperation and courtesies extended to my staff during the audit. If you have any questions, please contact me at (202) 927-5171 or Larissa Klimpel, Audit Manager, at (202) 927-0361. Major contributors to this report are listed in appendix 3.

/s/

Tram Jacquelyn Dang
Director, IT Audit

[10] *Standards for Internal Control in the Federal Government* (GAO-14-704G; issued Sept. 2014)

In October 2012, we initiated an audit of the security controls over the Department of the Treasury's (Treasury) information on servers employing virtualization technology. The overall objective of this audit was to determine whether controls were in place for securing data stored on virtual servers and virtual hosts that were located in the Bureau of the Fiscal Service's (Fiscal Service) consolidated data centers.

As part of the audit, we met with senior Treasury officials in the Office of the Chief Information Officer to determine how virtualization was being used. We performed a Treasury-wide data call for information on data center consolidation and virtualization efforts. Based on the result of our survey, we selected Fiscal Service for this audit because its consolidated data centers had the highest total of virtual hosts compared to the Treasury's other bureaus and offices. In January 2013, we issued a separate engagement memo to Fiscal Service management.

We selected a sample of 16 virtual servers to test using a risk-based sampling methodology that was based on virtual servers with critical applications on them, unsupported versions of operating systems, and/or unsecure network services. In performing our work, we interviewed key officials and personnel at Fiscal Service; reviewed applicable National Institute of Standards and Technology Special Publications, as well as Treasury's and Fiscal Service's policies and procedures; reviewed and analyzed key documents related to virtual servers; and observed demonstrations of security control configurations performed by Fiscal Service technical personnel. We performed our fieldwork primarily at Fiscal Service's facility in Hyattsville, Maryland, between February 2013 and August 2014.

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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

DEPARTMENT OF THE TREASURY
BUREAU OF THE FISCAL SERVICE
WASHINGTON, DC 20227

COMMISSIONER

July 31, 2015

Ms. Tram Dang
Director, IT Audit
U.S. Department of the Treasury
Office of the Inspector General
JBAB Building 410/Door 123
250 Murray Lane, SW
Washington, DC 20222

Dear Ms. Dang:

Thank you for the opportunity to respond to the draft report "Fiscal Service's Management of Virtual Servers Needs Improvement", dated June 4, 2015. Fiscal Service agrees with the three (3) findings and five (5) associated recommendations. Our responses are as follows:

Management Response to *Fiscal Service's Management of Virtual Servers Needs Improvement*

Finding 1: Fiscal Service lacked an Enterprise-Wide Inventory of Virtual Servers

Recommendation 1: We recommend that the Commissioner of the Bureau of the Fiscal Service ensure that a complete enterprise-wide inventory of virtual servers in Fiscal Service's environment is created and maintained.

Management Response

Fiscal Service agrees with the finding and recommendation, and has developed a remediation plan to ensure full implementation of the Configuration Management Program, revise policies and procedures, and increase staff awareness so that the inventory is properly maintained. Completion is planned by March 31, 2016.

Finding 2: Software Assets Were Not Effectively Managed

Recommendation 1: Ensure an approved centralized software inventory across Fiscal Service's lines of business is created, maintained, and regularly updated to ensure that only approved software is included.

Management Response

Fiscal Service agrees with the finding and recommendation, and has developed a remediation plan to create a single approved software inventory and implement revised policies and procedures to ensure the list is regularly updated. Completion is planned by March 31, 2016.

Recommendation 2: Ensure that software is timely removed from virtual servers when retired.

Management Response

Fiscal Service agrees with the finding and recommendation, and has developed a remediation plan to perform service provider compliance reviews to begin by March 31, 2016.

Finding 3: Some UNIX Administrative Accounts Were Not Disabled

Recommendation 1: Ensure that staff responsible for account management is aware of Fiscal Service's exit procedures so that inactive user accounts are disabled and administrative privileges are immediately removed when no longer needed.

Management Response

Fiscal Service agrees with the finding and recommendation, and has developed a remediation plan to train appropriate staff on exit clearance processes and standard operating procedures by May 31, 2016.

Recommendation 2: Ensure that periodic reviews of administrative accounts are performed in accordance with NIS TSP 800-53 and Fiscal Service policies and procedures.

Management Response

Fiscal Service agrees with the finding and recommendation, and has developed a remediation plan to design and configure semi-annual UNIX automated administrative account recertifications. Completion is planned by May 31, 2016.

Sincerely,

Sheryl R. Morrow
Commissioner

2

Information Technology (IT) Audit

Tram J. Dang, Director
Larissa Klimpel, Audit Manager
Dan Jensen, Auditor-in-Charge
Jason Beckwith, Auditor-in-Charge
Mitul "Mike" Patel, IT Specialist
James Shepard, Referencer

The Department of the Treasury

Deputy Assistant Secretary for Information Systems and Chief Information Officer

Office of Strategic Planning and Performance Management

Risk and Control Group, Office of Deputy Chief Financial Officer

Bureau of the Fiscal Service

Commissioner

Chief Internal Control Officer

Office of Management and Budget

OIG Budget Examiner