Software Version Control Management Needs Improvement

June 13, 2019

Reference Number: 2019-20-031

<u>Redaction Legend</u>:
2 = Law Enforcement Techniques/ Procedures and Guidelines for Law Enforcement Investigations or Prosecutions

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.

SOFTWARE VERSION CONTROL MANAGEMENT NEEDS IMPROVEMENT

Highlights

Final Report issued on June 13, 2019

Highlights of Reference Number: 2019-20-031 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

The management and control of the IRS's software versions is crucial to ensure that information technology services continue to support the IRS's business operations and to ensure the security of taxpayer data and Personally Identifiable Information. Older versions of software can lead to operational or security vulnerabilities.

WHY TIGTA DID THE AUDIT

The overall objective of this review was to evaluate the strategy and processes to manage and control commercial-off-the-shelf software versions running on the IRS infrastructure and ensure that software versions are up to date.

WHAT TIGTA FOUND

The IRS has made progress in automating its review of software versions through the use of tools. For example, by using the Flexera Technopedia catalog and Big Fix 9.2, the IRS can determine the vendor's most recent released version. However, the IRS is not effectively managing or controlling software versions on systems and applications to ensure that software is approved and up to date. TIGTA identified instances in which software versions running on IRS systems were not listed in the IRS's official software Product Catalog or were shown as outdated and unapproved.

For example, TIGTA found that 55 (50 percent) of the software versions installed on the IRS's mainframe environment were not listed in the software Product Catalog. In addition, TIGTA determined that 32 (21 percent) of the server software versions reviewed were not approved in the software Product Catalog, and 50 (32 percent) were shown as archived/retired.

Finally, the IRS had unauthorized software installed on workstations and neglected to remove older versions of software when newer versions were installed. Although TIGTA did not review all older software versions to determine if known vulnerabilities existed, TIGTA found three software versions that included high vulnerabilities.

Running outdated or unapproved software versions significantly increases the risk of poor system performance and the exploitation of known software vulnerabilities by cyber criminals.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer create an enterprise-wide, integrated structure to centralize commercial-off-the-shelf software version tracking, currency, and management to include roles and responsibilities; update policies and/or procedures to manage mainframe, server, and workstation software assets using industry best practices; create and execute a plan to periodically monitor and compare software running on the enterprise against the Enterprise Architecture Enterprise Standards Profile Product Catalog for accuracy; remove unauthorized software or update the Enterprise Standards Profile Product Catalog to reflect the correct information, if warranted; and document and approve risk acceptance for using older versions of software.

The IRS agreed with all of the recommendations and plans to integrate software version tracking into a centralized enterprise-wide program office with documented roles and responsibilities, including ensuring that policies and procedures are updated and enforced. The IRS also agreed to develop a plan to identify all versions of its software products on at least a semi-annual basis, implement processes to address unauthorized software, and define a process to assess and document the continued use of older versions of software with a risk-based decision.

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

June 13, 2019

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

Michael E. McKenney

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – Software Version Control Management Needs Improvement (Audit # 201720007)

This report presents the results of our review to evaluate the strategy and processes to manage and control commercial-off-the-shelf software versions running on the Internal Revenue Service (IRS) infrastructure and ensure that software versions are up to date. This audit is included in our Fiscal Year 2019 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of IRS Resources.

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

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

Table of Contents

Appendices

Abbreviations

CVE	Common Vulnerabilities and Exposures
ESP	Enterprise Standards Profile
IBM	International Business Machines
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
TIGTA	Treasury Inspector General for Tax Administration
UNS	User and Network Services

Background

To administer the Federal tax system, the Internal Revenue Service (IRS) procures and uses various software packages on its systems and for its applications, including commercial-off-the-shelf solutions. Efficient and effective management of the IRS's software assets is crucial to ensure that information technology services continue to support the IRS's business operations in an efficient and secure manner. Because these software packages often process taxpayer account data, such as Internal Revenue Code Section 6103[1] tax return information and Personally Identifiable Information, using the most current software packages ensures that these data are protected and secured.

Efficient and effective management of the IRS's software assets is crucial to ensure that information technology services continue to support business operations and to provide services to taxpayers efficiently and securely.

One primary purpose for always using the latest software version is to stay protected from potential security threats. Software vendors frequently release new versions to add functionality and address known security vulnerabilities. Cybercriminals pay close attention to new software releases so they can construct attacks on those vulnerabilities in order to compromise the software and extract data for personal gain before organizations update to newer versions. Allowing outdated software versions to run on the computing infrastructure increases the risk to and vulnerability posture of an organization. For example, in September 2017, the credit reporting agency Equifax announced a data breach where confidential information was stolen for more than 143 million users because the agency did not update to the most current software version that was available more than two months prior to the attack.

The IRS uses an Enterprise Architecture process to manage major system software versions authorized and available for use enterprise-wide. Specifically, the Enterprise Architecture Enterprise Standards Profile (ESP) is a system used to document and update software versions that have been reviewed and approved for use. The ESP is the IRS approved products list for IRS approved products and standards, and includes the Federal Enterprise Architecture application and infrastructure mapping models. The products listed in the ESP have been evaluated to functionally fit within the IRS environment. They are tested in accordance with IRS standard processes. Once the product is listed on the ESP, it is considered approved for use in the IRS enterprise. However, ESP listings in and of themselves are not authorization for use or installation since some products may not be ready for deployment or use. Requests for use, purchase, download, or installation require direct coordination with either Enterprise Operations or User and Network Services (UNS) offices as applicable via Information Technology Work

[1] I.R.C. § 6103 - Confidentiality and disclosure of returns and return information.

Request or help desk tickets. The ESP also allows project owners and other stakeholders to select pre-approved technology products and standards. Listings in the ESP include guidance for usage that should be reviewed for useful relevant information. The ESP is updated frequently based on approved change requests. Products are added to the ESP only when the Configuration Control Board approves a proposed Change Request for a product or standard.

The IRS evaluates products used and strives to ensure that versions are the most current or no more than one version behind the current version approved by the Enterprise Architecture organization and listed in the ESP, contingent on budget and risk. Under the "N/N-1" model, "N" represents the most current version of a software product released by the vendor; and "N-1" represents the previous major release of a vendor product. The N-1 release is still within the product support period, but is not the most current released version of the product. The "N/N-1" construct is an industry standard to reference a major release. Minor releases are mapped to their corresponding major release for purposes of calculating "N/N-1" currency metrics within the IRS.

In order to simplify the process to maintain each information technology component, the IRS designated three "Tiers" to group similar components, which also applies to managing software versions. Each Tier is defined in Figure 1.

Figure 1: Definition of Tier Levels

Tier	Components
Tier 1	Supercomputers and mainframe hardware and software, including peripheral subsystems used in a mainframe system environment, *e.g.,* Integrated Data Retrieval System, Security and Communications System, terminal controllers, other resources. This includes International Business Machines (IBM) and Unisys mainframes.
Tier 2	Minicomputers including hardware, software, and peripheral subsystems used in that environment. These systems typically include any hardware operating under a multi-user operating system, such as Windows, Unix, and Linux. These are typically referred to as mid-range servers.
Tier 3	Windows workstations only, *e.g.,* desktops, laptops, and local area network resources.

Source: Treasury Inspector General for Tax Administration (TIGTA), Ref. No. 2017-20-062, The Internal Revenue Service Is Not in Compliance With Federal Requirements for Software Asset Management, pp. 22-23 (Sept. 2017).

The IRS also considers the Common Vulnerabilities and Exposures (CVE) naming standard and the Common Vulnerability Scoring System standard to determine the severity and risk of any vulnerabilities in the software versions. The IRS also relies on the National Vulnerability Database, which is the U.S. Government repository of standards based vulnerability management data enabling automation of vulnerability management, security measurement, and compliance.

This review was performed at the IRS Information Technology organization's Strategy and Planning, Enterprise Services, Enterprise Operations, and UNS offices at the New Carrollton Federal Building in Lanham, Maryland, during the period December 2017 through October 2018. 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.

Results of Review

The Use of Outdated Software on Systems Presents Increased Risks

Internal Revenue Manual (IRM) 10.8.21, *Information Technology Security, Database Security Policy*, issued on June 27, 2018, and IRM 10.8.20, *Information Technology Security, Windows Security Policy*, issued on June 27, 2018, states that the IRS shall ensure that the operating system version running on IRS systems is a version for which the vendor still offers standardized technical support. The IRS shall also ensure that the operating system product and version selected is in accordance with the Enterprise Architecture ESP that dictates the official products and versions of software within the IRS. IRM 2.17.1, *Infrastructure Currency Policy for Software*, issued on October 9, 2018, states that the IRS information technology infrastructure shall run the software version approved in the ESP, either "Major Version Approved" or the immediately preceding major version. In addition, within six months of software products being identified as noncompliant, product owners shall either provide a plan to bring the product into compliance via upgrade, remove the product from the IRS environment, or request to remain on the current version via a Risk Acceptance Form and Tool. These requests are approved by the Infrastructure Executive Steering Committee.

IRM 10.8.1.1.3 (3)[2] states that the IRS shall ensure that the application or system version is a version for which the vendor still offers standardized technical support. Any exception requires the authorizing official of the system to make a risk-based decision. If the risk is accepted, then a Risk Based Decision is created which documents the potential vulnerabilities and the reasons for acceptance.

From a best practice perspective, the Information Systems Audit and Control Association's (better known as ISACA) Control Objectives for Information and Related Technologies (also known as COBIT) 5[3] states that an organization is to maintain an up-to-date and accurate record of all information technology assets required to deliver services and ensure alignment with configuration management and financial management. Further, the National Institute of Standards and Technology (NIST) Special Publication 800-53A[4] recommends an organization define software components to be removed after updated versions have been installed and remove organization-defined software components after updated versions have been installed.

---

[2] IRM 10.8.1, *Information Technology Security, Policy and Guidance* (July 8, 2015).
[3] ISACA COBIT 5, BAI09 *Process Practices, Inputs/Outputs and Activities*; paragraph BAI09.01 "Identify and record current assets."
[4] NIST, NIST Special Publication 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations* (Dec. 2014).

Our review identified that the IRS is not effectively managing or controlling software versions on systems and applications to ensure that the software versions are approved and up to date. Currently, the IRS is using a total of 3,937 software packages across the entire enterprise for all three Tiers which are managed by several different organizations.

Although the ESP is the authoritative approved product list for authorized software, we found instances in each Tier in which software was installed on systems that were not found in the ESP. Each organization managing the software used different methods to identify unauthorized or outdated software on its systems; however, no Tier was 100 percent compliant with the policies stating that software is to be maintained at the N or N-1 version.

Overall, these conditions occurred because there is no enterprise-wide oversight of the software deployed on any of the three Tiers; current reviews of existing software among the Tiers are not consistent across the environments; and the process to update and manage installed software versions is manual, time-intensive, and performed vendor by vendor and Tier by Tier.

Running outdated or unapproved software versions may significantly increase the risk of poor system performance and the exploitation of known software vulnerabilities by cyber criminals. These risks are more often present in older software that is no longer maintained or supported by the vendor. The IRS indicated that it takes actions to mitigate risk through implementing firewall rules to increase protection.

Some software running on Tier 1 mainframes were not listed in the approved ESP Product Catalog or were listed as archived or retired

The Enterprise Operations organization's Enterprise Server Division is responsible for Tier 1 mainframe computer software. The division plans, builds, tests, and deploys mainframe technologies, including IBM, Linux, and Unisys mainframe systems. IBM's Tivoli® Asset Discovery for zOS tool is used to scan mainframes to determine what software is implemented on the IBM mainframes. Linux software is tracked through the Enterprise Architecture ESP. No tool is used to scan the software implemented on the Unisys mainframes. Unisys software is tracked through the Computerized Onsite Maintenance for User Systems[5] database instead of the ESP.

A product is documented as archived when it has reached its End of Life (support) date or a new version is specified as the enterprise solution via a change request. If a product is no longer supported by the vendor or the community for open source, the IRS shall replace the product or document the purpose and justification for continued use of unsupported software required to satisfy mission/business needs. Continued use of an archived product is allowed only if vendor maintenance or community support is provided and is documented through a Risk Based

[5] An OS 2200 software product used to generate and install other software.

Decision memo issued by an authorizing official. New deployments of archived products are not allowed.

A sunset date in the ESP indicates the intentional phasing out of a product or version due to a predetermined lifecycle date or vendor published End of Life (support) date. Specifically, the sunset date represents the last two years before a known End of Life date or the last two years when the five-year rule[6] is applied (*e.g.*, no vendor published End of Life). No new deployments of a product are approved in this phase if End of Life is published. If no End of Life is published, then the product support status must be verified with the vendor before the ESP record is updated or new deployments can occur.

We reviewed 110 software versions installed on the 12 Tier 1 mainframe environments as of February 2017 and discovered 55 software versions that were installed and running on the mainframe that were not listed in the ESP Product Catalog. This situation could be potentially dangerous to the IRS environment because these software versions were running on systems and may not have been reviewed, approved, and authorized prior to installation. Figure 2 presents the results of our analysis of the 110 software versions.

Figure 2: Installed Tier 1 Software Versions

Installed Software Versions	Number	Percentage
Not Located on ESP	55	50%
On ESP – Sunset date 2017 or earlier	13	12%
On ESP – Archived/Retired	28	25%
On ESP – No Exception	14	13%
Total	110	100%

Source: TIGTA analysis of the Tivoli Asset Discovery for z/OS Tool Data and Computerized Onsite Maintenance for User Systems Unisys Software Data.

Of the 110 versions reviewed, we also identified 13 software versions installed on the mainframe environment that were showing a sunset date of 2017 or earlier in the ESP Product Catalog. In addition, the IRS had 28 software versions installed and running that were listed as archived/retired on the ESP site. Users are permitted to use archived products if vendor maintenance or community support is provided and permission is obtained from the authorizing official and documented with a Risk Based Decision document.

Currently, no mechanism is in place to reconcile the software versions installed on Tier 1 environments to the ESP. The IRS stated that it performs an annual review with the vendors for

[6] The five-year rule is three years current from the date of release and two years in sunset status.

Tier 1 software to determine the approximate time to implement newer versions of software based on the cost, resource constraints, and risks; however, we did not see evidence of the review that resulted in updating older software versions.

The IRS stated that the responsibility for maintaining some of the mainframe software was transferred from one team to another and the update requirements of the ESP were overlooked. In addition, the IRS stated that in some situations current software running on systems and applications were installed many years ago and therefore have not been listed in the ESP. The IRS implemented the five-year rule to project lifecycle costs and allow projection of fiscal year funding requirements for upgrades when there is a published End of Life date. When the Enterprise Architecture organization began applying the five-year rule to sunset products, the staff was unaware of the new requirement to revalidate products on the ESP, which caused the products listed in the ESP to show as being sunset. Because the responsibilities for validating software products shifted and the new team was unaware of the requirements, no Risk Based Decision documents were prepared for older software versions.

Software versions not listed in the approved ESP Product Catalog are running on servers

The Enterprise Operations organization's Server and Support Services Division is responsible for installing, maintaining, and upgrading Tier 2 server software, which includes provisioning servers for all platforms including the installation and configuration of commercial-off-the-shelf products. The IBM BigFix 9.2 tool is used to scan the servers and determine what software is implemented.

The IRS provided an ad hoc list of the software installed on approximately 3,000 servers. We reviewed the software installed on the 3,000 servers to determine whether the software versions were in the ESP Product Catalog as approved software. Our analysis determined that there were 156 unique software versions in the Tier 2 environment, of which 32 (21 percent) were not approved in the ESP Product Catalog. Similar to this issue on the mainframe environment, these software versions were installed on servers and may not have gone through the proper review and approval process. The IRS policy states that software versions are to be reviewed, approved, and authorized prior to installation. Figure 3 shows our analysis of the 156 software versions.

Figure 3: Installed Tier 2 Software Versions

Installed Software Versions	Number	Percentage
Not Located on ESP	32	21%
On ESP – Sunset date 2017 or earlier	0	0%
On ESP – Archived/Retired	50	32%
On ESP – No Exception	74	47%
Total	156	100%

Source: TIGTA analysis of the BigFix 9.2 Tool Data.

The IRS uses the Big Fix 9.2 tool to obtain a list of software installed on servers and compares the list against the Flexera Technopedia BDNA Normalize Catalog[7] of software to determine the vendor's most recent released version. The ESP is then assessed to identify product versions approved to run on systems and applications. The decision to update software versions is directly related to how or if it will affect the upcoming tax filing season. The IRS uses a scoring methodology to determine the risk and impact that a specific outdated software has on the agency, in addition to identifying critical security vulnerabilities. The scoring methodology assigns a numerical value to a product, making it easier to determine whether it should be included in an upgrade. Typically, the higher the score value, the more critical the update. The IRS has the ability to waive any product that it deems not necessary to update through a governance model based on severity, cost, level of effort, and material weaknesses identified.

This approach to managing software versions led to installed software in the Tier 2 environment that was overlooked for many years and contained known critical vulnerabilities. For example, our review of the IRS's list of software versions indicated that ActiveState Active Perl 5.8, which is only N-1 version behind the most current market version, was selected for upgrade. However, the upgrade was not processed due to limited resources and competing priorities, *e.g.*, filing season and tax reform. Although this software is only one version behind the most current market version and falls within the IRS standards for currency, it should have been upgraded because of the known security risks. The software has a Maximum Common Vulnerability Scoring System Severity of eight on a scale of 10, and an End of Life and End of Support date of December 16, 2008, and is no longer supported by the vendor. We found two known vulnerabilities listed in the National Vulnerability Database for this software. These vulnerabilities allow attackers to cause a denial of service (crash) and possibly execute arbitrary code via a system command, which leads to a stack-based buffer overflow.

[7] The Flexera Technopedia BDNA Normalize Catalog is the most trusted and comprehensive asset information repository of enterprise software and hardware.

We reviewed the list of software candidates selected for upgrading prior to Filing Season 2019 and identified one instance of **************2**************, that was installed on two servers. *****************************2***********************************. The IRS did not know what was installed in the Tier 2 environment prior to installing an automated solution in 2017. The Flexera Technopedia catalog and the BigFix 9.2 tool now provides the IRS with an automated view of Tier 2 commercial-off-the-shelf products and their disposition. The IRS stated that the software was not critical to the filing season and therefore was not updated.

The current practice of reviewing and prioritizing software updates based on how critical they are to the filing season, rather than updating all software, appears to be a short-term solution based on time and resource constraints. TIGTA believes that the IRS should review older versions of software to determine whether the software should be removed from the environment or if the software is still in use and has been reviewed for known vulnerabilities. Using older software versions can provide many opportunities for cyber criminals to access and exploit data.

During the review process for selecting products to upgrade for the filing season, the IRS solicits input from the offices of Applications Development, Cybersecurity, Enterprise Operations, Enterprise Services, UNS, and Enterprise Program Management Office. The IRS requires each office to sign off on whether or not to upgrade the software. These sign-offs are governed by the Infrastructure Executive Steering Committee. We identified seven software versions installed on 40 servers that were 10 years or older than the vendor's most recent version of software.

In addition, the IRS had multiple versions of ********2******** in use in the Tier 2 environment. The current approved version in the Enterprise Architecture ESP is ****2****; however, that version is not being used in the Tier 2 environment. ****2**** is in the Enterprise Architecture ESP as retired/archived. *************2*********** are installed and in use, ranging from **************2*************. The IRS stated that it is in the process of upgrading the software.

Allowing outdated software to remain on a system when newer software versions are available runs contrary to NIST Special Publication 800-53A, which recommends an organization define software components to be removed after updated versions have been installed. In addition, having multiple versions of the same software installed across the agency only creates additional work for system administrators because maintenance needs to occur on each version installed, including scanning for vulnerabilities or installing patches. The number of instances of a software installation increases the number of possible vulnerabilities.

Some software versions running on Tier 3 workstations were not listed in the approved ESP Product Catalog or were listed as archived or retired

The UNS office is responsible for Tier 3 laptop/desktop workstation software. The UNS office currently uses the Symantec® Information Technology Management Solution for Software Asset Management. This solution is used for software version control and automates software asset management tasks related to software deployment, file inventory, software update, and software removal and reporting. The UNS office is currently using the Thycotic® Application Control Solution. This solution complements the Information Technology Management Solution by allowing the UNS office to identify and block the execution of "blacklisted" unauthorized software. Unauthorized software is defined as software not approved for use or not listed on the Enterprise Architecture ESP (across all Tiers) and UNS Application Registration libraries. The Application Control Solution application analyzes for unauthorized software and identifies and categorizes software as either "blacklisted," which is blocked by the Application Control Solution and slated for removal through Information Technology Management Solution, "orangelisted" for needing further analysis, or "whitelisted" for approved software.

Similar to the other two tiers, software for Tier 3 is required to be authorized and documented in the Enterprise Architecture ESP prior to use. However, for Tier 3, software may be requested and downloaded from an UNS office site. This site lists ESP approved software for use and identifies if there are any remaining licenses available.

We reviewed a list of 6,970 Tier 3 software applications installed on IRS workstations. The list identified 6,533,792 software version instances installed in each operating division of the IRS. Due to the substantial volume of Tier 3 software versions recorded by the IRS, we limited our analysis to 5,697,421 software version instances installed on 10,000 or more workstations. This represented 87 percent of the entire population of software version installs. From this subset, we identified 146 unique major software versions for review. Of these 146 software versions, we found seven (5 percent) that are not listed on the Enterprise Architecture ESP Product Catalog. Figure 4 presents our analysis of the 146 software versions.

Figure 4: Installed Tier 3 Software Versions

Installed Software Versions	Number	Percentage
Not Located on ESP	7	5%
On ESP – Sunset date 2017 or earlier	4	3%
On ESP – Archived/Retired	2	1%
On ESP – No Exception	133	91%
Total	146	100%

Source: TIGTA analysis of Common Operating Environment download of installed software applications.

In addition, the IRS does not efficiently remove old versions of software from the Tier 3 environment when a newer version of software is installed. For example, the IRS currently shows ******************2******************** installed and in use, ranging from

************************2*************************, even though these older versions have been identified to include high vulnerabilities and a Max Common Vulnerability Scoring of 10.

The IRS Computer Security Incident Response Center's ***********2*******,[8] *****2***** ******************2*********************** required all IRS computers to update *************2************, as of September 13, 2017. As of October 1, 2017, we found 166,748 installs of older versions of ********2********, which has a known vulnerability. In addition, there were only 188 versions updated to *****2***** across all divisions. Having that many older versions on workstations across the agency is a significant issue as older software with known vulnerabilities and with active Computer Security Incident Response Center advisories unnecessarily exposes the IRS to security risks.

The following are just a few examples of older software versions that are currently running on the Tier 3 platform with multiple versions.

- Twenty major versions of ******2****** installed and in use, ranging from ****2**** ************2************. One known high vulnerability (9.3) that affects **2** ********************************2*********************************** ********************************2*********************************** ***********2***********.[9] Even if the IRS implements mitigating factors, it should have upgraded or removed older versions of the software to remove the known vulnerability.
- Sixteen major versions of ******2****** installed and in use, ranging *******2****** *************2*************. One known high vulnerability (8.8) that affects ********************************2*********************************** ********************************2*********************************** ********************************2************.[10]
- Six major versions of ***************2*************** installed and in use, ranging from ********************2*********************************** ********2********.
- Five major versions of *********2********** installed and in use, ranging from ********************2***********************.

The IRS has a decentralized software version control process with insufficient oversight of potentially unapproved, outdated, or archived/retired software running on IRS systems that could

[8] TIGTA reviewed the IRS Computer Security Incident Response Center's Critical Advisories for the time frame January 2017 through December 2017 and did not find a correlation between outdated software and reported incidents.

[9] **********************2*********************, with a vulnerability of 9.3 HIGH.

[10] *********************2***********************, with a vulnerability of 8.8 HIGH.

result in unacceptable risks to overall operations and taxpayer data. Effective centralized accountability in monitoring software versions running across the entire IRS network can allow for more effective decisions on cost, risk, and compatibility.

Recommendations

To improve the management of mainframe, server, and workstation software versions based on Federal requirements and recommended industry best practices, the Chief Information Officer should:

Recommendation 1***:*** Create an enterprise-wide, integrated structure to centralize commercial-off-the-shelf software version tracking, currency, and management to include documenting roles and responsibilities.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS has already created an enterprise-wide, integrated structure to centralize commercial-off-the-shelf software version tracking. It will continue to strengthen and mature this approach, and these efforts will integrate commercial-off-the-shelf software version tracking into a centralized enterprise-wide program office with documented roles and responsibilities.

Recommendation 2: Update policies and procedures to manage mainframe, server, and workstation software assets using industry best practices, including identifying, prioritizing, and removing outdated software when newer versions are installed.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS currently has policies and procedures in place to manage mainframe, server, and workstation software assets. The current policies and procedures, such as IRMs, will be assessed to determine potential gaps specific to software asset identification, prioritization, and removal of outdated software when new versions are installed. Existing policies will be updated and new policies and procedures will be established. The centralized enterprise-wide program office will ensure that the policies and procedures are updated and enforced.

Recommendation 3: Create and execute a plan to periodically monitor and compare software running on the enterprise against the Enterprise Architecture ESP Product Catalog for accuracy.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will develop a plan to identify all versions of its commercial-off-the-shelf products on at least a semi-annual basis. The results will be compared to the ESP product catalog to identify any discrepancies, which will help ensure compliance with IRM 2.17.1 and support implementation of permitted remedies.

Recommendation 4***:*** Remove unauthorized software or update the ESP Product Catalog to reflect the correct information, if warranted.

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will implement processes to address instances of unauthorized software in accordance with remedies available in IRM 2.17.1 and as recommended by IRM 10.8.1.1.3 and NIST Special Publication 800-53A.

Recommendation 5: Document and approve risk acceptance to continue using older versions of software (*i.e.*, sunset, archived/retired).

> ***Management's Response:*** The IRS agreed with this recommendation. The IRS will define a process to assess and document the risks associated with continued use of older versions of software. Consistent with IRM 2.17.1, risks will be assessed at the "major version" level as identified by a given publisher, and a risk-based decision will be documented as described in IRM 10.8.1.1.3.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to evaluate the strategy and processes to manage and control commercial-off-the-shelf software versions running on the IRS infrastructure and ensure that software versions are up to date. To accomplish our objective, we:

I. Identified the methodologies used by various IRS organizations for managing software version control for systems (Tiers 1 and 2) and applications (Tier 3), including how software versions are kept current.

   A. Obtained and reviewed NIST (and other regulatory) requirements regarding software version control management.

   B. Obtained and reviewed guidance issued by the Department of the Treasury regarding software versions.

   C. Obtained and reviewed applicable IRM citations on software version control.

   D. Identified and reviewed internal controls implemented by the Information Technology organization to manage software versions.

   E. Determined if the Information Technology organization maintains performance data and metrics on software versions for systems (Tiers 1 and 2) by reviewing and evaluating procedures for management of software version control.

   F. Determined if the Information Technology organization maintains data on software versions for applications (Tier 3) by reviewing and evaluating procedures for the management of software version control.

   G. Identified and reviewed Computer Security Incident Response Center incidents for January 2017 through December 2017 to determine whether the use of outdated software versions was a contributing factor for the incidents.

II. Determined if the processes for managing software version controls for systems (Tiers 1 and 2) and applications (Tier 3) are in compliance with internal policies and external regulatory guidance.

   A. Interviewed responsible Strategy and Planning and UNS office personnel regarding processes for tracking and managing software version controls for systems and applications (Tiers 1, 2, and 3).

   B. Evaluated procedures for documenting system software versions and application software versions implemented enterprise-wide.

C. Evaluated procedures for identifying the correct version to be implemented on each system or application (current version or one behind the current version).

D. Evaluated the process for determining whether to install the most up-to-date version or to keep using an older version and evaluated the reasonableness of this risk-based approach.

E. Determined whether the IRS is monitoring version control on systems and applications on a regular interval (monthly, yearly, as needed).

III. Determined whether version control management for systems software (Tiers 1 and 2) is effective to ensure that software versions are current.

A. Obtained a list of all authorized system software (including versions and date updated) the IRS is using, by tier level.

B. Determined whether the list of system software is adequate to properly document the software versions and whether the IRS is regularly updating the list.

C. Obtained a separate list of software currently installed on systems.

D. Selected software versions from the list of current system software versions to compare to industry published most recent versions obtained from Big Fix 9.2.

E. Selected and reviewed 100 percent of Tier 1 mainframe software versions (110 total software versions) and 100 percent of Tier 2 provided server software versions (156 total software versions) as identified by the IRS. Because the IRS could not readily provide the full list of Tier 2 software, we limited our review to software versions they were able to provide during our fieldwork.

IV. Determined whether version control management for application software (Tier 3) is effective to ensure that software versions are current.

A. Obtained a list of all authorized application software (including versions and date updated) the IRS is using in Tier 3.

B. Determined whether the list of application software is adequate to properly document the software versions and whether the IRS is regularly updating the list.

C. Obtained a separate list of software actually installed on systems.

D. Selected software versions from the list of application software versions to compare to industry published most recent version.

E. Selected and reviewed unique major software versions installed on more than 10,000 machines (146 software versions were reviewed of the total population remaining) and judgmentally sampled, as we were not going to project our results. By utilizing this approach, we focused our attention on the software with the highest level of utilization by employees.

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: the Information Technology organization's policies, procedures, and processes for managing and tracking software versions. We evaluated these controls by interviewing Information Technology organization management, identifying Federal requirements and industry best practices for managing and tracking software versions, reviewing a sample of software in use, and reviewing relevant documentation.

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Joseph Cooney, Audit Manager
Naomi Koehler, Lead Technical Specialist
George Franklin, Senior Auditor

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Chief Information Officer
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Enterprise Operations
Associate Chief Information Officer, Strategy and Planning
Associate Chief Information Officer, User and Network Services
Director, Office of Audit Coordination

Appendix IV

Glossary of Terms

Term	Definition
Application	A software program hosted by an information system.
Authorizing Official	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.
Commercial-off-the-Shelf	Pre-packaged, vendor-supplied software that will be used with little or no modification to provide all or part of the solution.
Common Vulnerabilities and Exposures	A dictionary that provides definitions for publicly disclosed cybersecurity vulnerabilities and exposures. The goal of the CVE is to make it easier to share data across separate vulnerability capabilities (tools, databases, and services) with these definitions. CVE entries are comprised of an identification number, a description, and at least one public reference. The CVE list feeds the National Vulnerability Database, which builds upon the information.
Common Vulnerability Scoring System	Provides an open framework for communicating the characteristics and impacts of information technology vulnerabilities. It attempts to assign severity scores to vulnerabilities, allowing responders to prioritize responses and resources according to threat.
Computer Security Incident Response Center	The IRS office that receives and disseminates incident information, responds to incidents, and reports on incidents.
Configuration Control Board	A group of technical experts and managers with the assigned authority and responsibility to make decisions on the configuration of a baselined product.
Denial of Service	Actions that strive to make a computer resource unavailable to authorized users, generally consisting of the concerted efforts of an attacker to prevent an information resource from functioning efficiently or at all, temporarily or indefinitely.
Desktop Computer	A computer that is designed to stay in a single location, cannot be powered from an internal battery, and therefore must remain connected to a wall outlet.

Term	Definition
End of Life	Hardware or software that is no longer manufactured or supported. An end of life announcement by a vendor stipulates when the manufacturing will end, or if already ended, how long future support for the product will be provided.
End of Support	The date the vendor stops providing software version technical support and other types of support services.
Enterprise Architecture	A unifying overall design or structure for an enterprise that includes business and organizational aspects of the enterprise as well as technology aspects. Enterprise Architecture divides the enterprise into its component parts and relationships and provides the principles, constraints, and standards to help align business area development efforts in a common direction. An Enterprise Architecture ensures that subordinate architectures and business system components developed within particular business areas and multiple projects fit together into a consistent, integrated whole.
Filing Season	The period from January through mid-April when most individual income tax returns are filed.
Firewall	A gateway that limits access between networks in accordance with local security policy.
Fiscal Year	Any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30.
IBM BigFix	A collaborative endpoint management and security platform that provides continuous policy enforcement and reporting, software patching, distribution and provisioning, and audits for authorized and unauthorized software.
IBM Tivoli Asset Discovery	Defines an inventory of software products installed on a z/Architecture mainframe running z/OS. It provides auditing information about the usage and installation of load modules and z/OS UNIX executables. Reports include software inventory, product use, identification of mainframe storage subsystem hardware, and discovered machine inventory.
Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency.
Inventory	To take stock of assets. A detailed list of assets.
Mainframe	A powerful, multiuser computer capable of supporting many hundreds of thousands of users simultaneously.

Term	Definition
Major Release	A major upgrade to a product containing new features along with product defect fixes.
Microcode	The lowest specified level of processor and machine instruction sets. It is a layer comprised of small instruction sets, which are derived from machine language. Microcode performs short, control-level register operations, including multiple micro instructions, each of which performs one or more micro operations.
Model	A graphical, mathematical, physical, or verbal representation or simplified version of a concept, phenomenon, relationship, structure, system, or an aspect of the real world.
National Institute of Standards and Technology	Part of the Department of Commerce. The NIST develops management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of "other than national security"-related information in Federal information systems.
National Vulnerability Database	The U.S. Government repository for standards based vulnerability management data, including databases of security checklist references, security-related software flaws, product names, and impact metrics. It performs analysis on CVEs that have been published in the CVE dictionary.
Operating System	The software that serves as the user interface and communicates with computer hardware to allocate memory, process tasks, and access disks and peripherals.
Personally Identifiable Information	Information that can be used to distinguish or trace an individual's identity, such as his or her name, Social Security Number, biometric records, *etc.*, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, *etc*.
Risk Based Decision	A decision made when meeting a requirement is technically or operationally not possible or is not cost-effective. It is required for any situation in which the system will be operating outside of IRS information technology security policy or the NIST guidelines, whether related to a technical, operational, or management control.
Server	A system capable of managing and running virtual machines. It is also a process capable of accepting and running instructions from another process.
Software	A general term that describes computer programs and consists of lines of code written by computer programmers that have been compiled into a computer program.

Term	Definition
Stack-based Buffer	A type of buffer or temporary location created within a computer's memory for storing and retrieving data from the stack. It enables the storage of data elements within the stack, which can later be accessed programmatically by the program's stack function or any other function calling that stack.
Sunset Date	Intentional phasing out of a product or product version due to a predetermined retirement date or vendor published End of Life (support) date. The period from identification to retirement date is the sunset period. Products in this phase will no longer be supported and are no longer approved for deployment.
Tier 1 Environment	A computing infrastructure consisting of mainframe computers that handle a high volume of critical operational data.
Tier 2 Environment	A computing infrastructure consisting of non-mainframe servers. These servers run various operating systems. The servers may also operate as database, web, e-mail, and file servers and provide a host of other important functions supporting the IRS network infrastructure.
Tier 3 Environment	Systems that include all workstation devices and any hardware operating under a Windows operating system, including all hardware used in a desktop environment: workstations functioning with a single-user (stand-alone) operating system including UNIX workstations that run single-user versions of UNIX and workstations that run any Windows operating system.
Virtual Machine	A simulated environment created by virtualization, also described as a tightly isolated software container that can run its own operating systems and applications as if it were a physical computer.
Vulnerability	A flaw or weakness in an information system's design, implementation, or operation and management that could potentially be exploited by a threat to gain unauthorized access to information, disrupt critical processing, or otherwise violate the system's security policy.

Appendix V

Management's Response to the Draft Report

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

CHIEF TECHNOLOGY OFFICER

MAY 23 2019

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Nancy A. Sieger *Nancy A. Sieger*
Acting Chief Information Officer

SUBJECT: Draft Audit Report – 201720007 - Software Version Control Management Needs Improvement (e-trak # 2019-11299)

Thank you for the opportunity to review your Draft Audit report titled "Software Version Control Management Needs Improvement" and discuss observations with the audit team. We appreciate TIGTA's acknowledgement of the progress made in improving IRS' processes and capabilities to effectively manage software version control. IRS agrees with TIGTA's recommendations, which will continue to improve the effectiveness of these disciplines. Improvements in these areas were in progress even prior to receiving the TIGTA Draft Audit Report. IRS also appreciates the partnership with TIGTA to achieve clarity and accuracy in the report, to describe the complex processes executed across the enormous and multi-tiered scope that is the IRS infrastructure ecosystem.

The IRS is committed to continuously improving the technology and processes in support of Federal tax administration. The IRS procures and uses a vast array of software to accomplish this, including Commercial Off The Shelf (COTS) software solutions. Efficient and effective management of the IRS' software assets is crucial to ensure that information technology services continue to support the IRS' business operations in an efficient and secure manner. The IRS uses the Risk Acceptance Form Tool (RAFT) and Risk Based Decision (RBD) processes to document and approve accepting the risks associated with continuing to use older versions of software for critical systems, such as filing season and external-facing systems. These processes are critical to maintain the integrity, confidentiality and availability of taxpayer data and IRS will build on this discipline as the scope is expanded for the entire enterprise.

The attachment lists our planned corrective actions to implement the audit report's recommendations.

2

The IRS values your continued support and the assistance your organization provides. If you have any questions, please contact me at (202) 317-5000 or a member of your staff may contact Warren Gove, Manager, Emerging Programs & Initiatives, at (317) 581-5780.

Attachment

Attachment

Draft Audit Report – Software Version Control Management Needs Improvement (Audit # 201720007) (E-trak # 2019-11299)

RECOMMENDATION 1: The Chief Information Officer should create an enterprise-wide, integrated structure to centralize commercial-off-the-shelf software version tracking, currency, and management to include documenting roles and responsibilities.

CORRECTIVE ACTION: The IRS agrees with this recommendation. The IRS has already created an enterprise-wide, integrated structure to centralize commercial-off-the-shelf (COTS) software version tracking. We will continue to strengthen and mature this approach. These efforts will integrate COTS software version tracking into a centralized enterprise-wide program office with documented roles and responsibilities.

IMPLEMENTATION DATE: May 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Enterprise Services

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

RECOMMENDATION 2: The Chief Information Officer should update policies and/or procedures to manage mainframe, server, and workstation software assets using industry best practices, including identifying, prioritizing, and removing outdated software when newer versions are installed.

CORRECTIVE ACTION: The IRS agrees with this recommendation. The IRS currently has policies and procedures in place to manage mainframe, server, and workstations software assets. The current policies and procedures, such as IRMs, will be assessed to determine potential gaps specific to software asset identification, prioritization, and removal of outdated software when new versions are installed. Existing policies will be updated and new policies and/or procedures will be established. The centralized enterprise-wide program office will ensure the policies and procedures are updated and enforced.

IMPLEMENTATION DATE: July 15, 2020

RESPONSIBLE OFFICIAL(S): Associate Chief Information Officer, Enterprise Services

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

Attachment

Draft Audit Report – Software Version Control Management Needs Improvement (Audit # 201720007) (E-trak # 2019-11299)

RECOMMENDATION 3: The Chief Information Officer should create and execute a plan to periodically monitor and compare software running on the enterprise against the Enterprise Architecture ESP Product Catalog for accuracy.

CORRECTIVE ACTION: The IRS agrees with this recommendation and will develop a plan to identify all versions of its COTS products on at least a semi-annual basis. The results will be compared to the ESP product catalog to identify any discrepancies, which will help ensure compliance with IRM 12.7.1 and support implementation of permitted remedies.

IMPLEMENTATION DATE: October 15, 2020

RESPONSIBLE OFFICIAL(S): 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.

RECOMMENDATION 4: The Chief Information Officer should remove unauthorized software or update the ESP Product Catalog to reflect the correct information, if warranted.

CORRECTIVE ACTION: The IRS agrees with this recommendation. The IRS will implement processes to address instances of unauthorized software in accordance with remedies available in IRM 12.7.1 and as recommended by IRM 10.8.1.1.3 and NIST Special Publication 800-53A.

IMPLEMENTATION DATE: October 15, 2020

RESPONSIBLE OFFICIAL(S): 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.

RECOMMENDATION 5: The Chief Information Officer should document and approve risk acceptance to continue using older versions of software (*i.e.*, sunset, archived/retired).

Attachment

Draft Audit Report – Software Version Control Management Needs Improvement (Audit # 201720007) (E-trak # 2019-11299)

CORRECTIVE ACTION: The IRS agrees with this recommendation. The IRS will define a process to assess and document risk(s) associated with continued use of older versions of software. Consistent with IRM 2.17.1, risks will be assessed at the "major version" level as identified by a given publisher, and a risk-based decision will be documented as described in IRM 10.8.1.1.3.

IMPLEMENTATION DATE: October 15, 2020

RESPONSIBLE OFFICIAL(S): 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.