TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

The Remediation of Configuration Weaknesses and Vulnerabilities in the Registered User Portal Should Be Improved

July 18, 2018

Reference Number: 2018-20-036

This report has cleared the Treasury Inspector General for Tax Administration disclosure review process and information determined to be restricted from public release has been redacted from this document.

Redaction Legend:
2 = Law Enforcement Techniques/ Procedures and Guidelines for Law Enforcement Investigations or Prosecutions.
10 = Trade Secrets or Commercial/Financial Information

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.

HIGHLIGHTS

THE REMEDIATION OF CONFIGURATION WEAKNESSES AND VULNERABILITIES IN THE REGISTERED USER PORTAL SHOULD BE IMPROVED

Highlights

Final Report issued on July 18, 2018

Highlights of Reference Number: 2018-20-036 to the Commissioner of Internal Revenue.

IMPACT ON TAXPAYERS

The Integrated Enterprise Portal (IEP) – Registered User Portal (RUP) is a web-enabled, electronic commerce infrastructure to provide secure, browser-based application services for tax practitioners and taxpayers to access IRS systems. Because sensitive tax information traverses through and resides on the IEP-RUP, the IRS and its web-based infrastructure are an attractive target for hackers. Configuration weaknesses and vulnerabilities in the IEP-RUP environment unnecessarily expose taxpayer data to unauthorized access and disclosure.

WHY TIGTA DID THE AUDIT

This audit was initiated to determine whether the IRS's IEP-RUP offering external web services to the public is timely patched and remediated when vulnerabilities or misconfigurations are identified.

WHAT TIGTA FOUND

The IEP-RUP infrastructure is owned and operated by a contractor for the Enterprise Operations organization's Enterprise Technology Implementation Division. TIGTA determined that the vulnerabilities and misconfigurations on various hardware, virtual machines, and software within the IEP-RUP were generally remediated. Specifically, our analyses of configuration and vulnerability scan reports found **2** (**2** percent) of **2** high-risk configuration weaknesses identified by **2** scans and **2** (**2** percent) of **2** critical and high-risk vulnerabilities identified by **2** scans were remediated.

However, TIGTA remains concerned that the IRS has not timely remediated configuration weaknesses and vulnerabilities. For example, TIGTA found that **2** percent of high-risk configuration weaknesses identified by ****2**** scans were remediated after 30 calendar days. ****************2****************
**********************2*******************************
**********************2******************, although there was reference to the 30-calendar day requirement for configuration weaknesses that were documented and managed to ensure that they were eventually resolved.

TIGTA also found that the contractor had an inventory list of the physical and virtual hardware and operating software in the RUP. However, the inventory list was not always accurate and complete.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the Chief Information Officer establish ****2************************
**********************2*******************************
**********************2*******************************
*******2*******; ensure that the Cybersecurity organization performs follow-up validation on all corrected configuration weaknesses; comply with required processes to document, manage, and eventually resolve vulnerabilities identified by the contractor; update policies to use established processes that are consistent with required time frames; ensure that the contractor performs, at a minimum, an annual reconciliation of the IEP inventory; and ensure that the Cybersecurity organization includes the component inventory as part of its annual security assessment of the IEP-RUP.

The IRS agreed with eight of the nine recommendations, although it did not completely respond to two of the eight recommendations. The IRS plans to validate that the vulnerabilities have been remediated, review monthly status reports, and meet with stakeholders. The IRS also responded that it developed guidance for handling scan results and updated the patch management plan. The IRS partially disagreed with one recommendation. Our comments about the IRS's partial disagreement with our recommendations are discussed in the report.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

July 18, 2018

MEMORANDUM FOR COMMISSIONER OF INTERNAL REVENUE

Michael E McK

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Remediation of Configuration Weaknesses and Vulnerabilities in the Registered User Portal Should Be Improved (Audit # 201620007)

This report presents the results of our review to determine whether the Internal Revenue Service's (IRS) Integrated Enterprise Portal–Registered User Portal offering external web services to the public is timely patched and remediated when vulnerabilities or misconfigurations are identified. This audit is included in our Fiscal Year 2018 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

CMDB	Configuration Management Database
FISMA	Federal Information Security Modernization Act
IEP	Integrated Enterprise Portal
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
NIST	National Institute of Standards and Technology
POA&M	Plan of Action and Milestones
2	**********2**********
RUP	Registered User Portal
SLO	Service Level Objective
TIGTA	Treasury Inspector General for Tax Administration

Background

A vulnerability in the context of cybersecurity refers to a flaw or weakness in a computer system that, if left alone, could be exploited[1] or triggered by a threat source. Generally, a vulnerability can arise in two ways. First, a manufacturer may identify the flaw or weakness within its own product and will release a security patch to fix the vulnerability. Second, a security vulnerability can result from a misconfigured or inadvertent change to a system setting that causes an unintended weakness in the system.

The impact of vulnerable systems has been well documented in the last few years. For example, in October 2016, a National Security Agency official remarked that the high-profile Government hacks to which the National Security Agency has responded, including the cyberattacks on the Office of Personnel and Management and the White House, occurred because the adversary took advantage of poorly secured and poorly patched systems. Once the adversary got inside, he or she elevated his or her privileges and then moved to mission objectives, which ranged from stealing data to destroying it. This risk is heightened for externally facing systems that are accessible to the public via the Internet.

To minimize the exposure of these vulnerabilities, organizations should implement vulnerability management practices designed to proactively mitigate or prevent the exploitation of system vulnerabilities. This process involves the identification, classification, remediation, and mitigation of various vulnerabilities within a system. Vulnerability management is part of the larger cybersecurity risk management framework recommended by the National Institute of Standards and Technology (NIST). The June 5, 2014, updated version of NIST Special Publication 800-37[2] provided guidelines for applying a six-step Risk Management Framework to Federal information systems. The intent of the common framework is to improve information security, strengthen risk management processes, and encourage reciprocity among Federal agencies. The six steps include security control assessments, information system authorization, and security control monitoring.

According to NIST guidelines, information systems are in a constant state of change, with upgrades to hardware, software, or firmware and modifications to the surrounding environments where the systems reside and operate. A disciplined and structured approach to managing, controlling, and documenting changes to an information system or its environment of operation is an effective security control monitoring program. Strict configuration management and control processes are established by the organization to support such monitoring activities.

[1] See Appendix IV for a glossary of terms.

[2] NIST Special Publication 800-37 Rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (Feb. 2010) (includes updates as of June 5, 2014).

The Internal Revenue Service (IRS) continues to demonstrate its commitment to broaden taxpayers' access to secure digital services (in order to provide better assistance to those seeking to comply with the tax laws) by providing one-stop, web-based services for the general public, Federal agencies, and tax professionals from multiple channels. The IRS offers external web services for the public and employees through the Integrated Enterprise Portal (IEP). The IEP was designed to be an innovative and cost-effective system that would provide a fully scalable, managed private cloud capability to the IRS, enabling one-stop, web-based services for internal and external users. The IEP has four portals:

- The Public User Portal, IEP-IRS.gov, allows unrestricted public access to nonsensitive materials and application forms, instructions, news, and tax calculators. No authentication is required for access to any materials on the IEP-IRS.gov.
- The Registered User Portal (RUP) allows registered individuals, third-party users (collectively, "partners" – registration and login authentication required), and other individual taxpayers or their representatives access for interaction with selected tax processing and other sensitive systems, applications, and data.
- The Employee User Portal allows IRS employee users to access IRS data and systems, such as tax administration processing systems, financial information systems, and other data and applications, including mission-critical applications. Registration and authentication are required for access to sensitive and mission-critical applications.
- The Transaction Portal Environment provides the essential security and technology components required for secure structure data exchange between the IRS and the Centers for Medicare and Medicaid Services.

The IEP is a contractor-owned and managed service by *************10*****************
********10********)[3] for the Enterprise Operations organization's Enterprise Technology Implementation Division. The division leads the implementation and operations of enterprise technology programs, including third-party managed services. In addition, the division provides sustaining operations and enhancement support of portal components within the development, test, and production environments.

In its September 2015 Performance Work Statement, the contractor committed to operating the security program in accordance with the six-step Risk Management Framework except for the information systems authorization step, which the contractor stated is an IRS responsibility. The contractor established a Continuous Monitoring Plan that includes a mechanism to update its patch management plan, scan for vulnerabilities, and maintain secure configurations.

This review was performed at one of *****10***** offices and the Enterprise Operations organization's Enterprise Technology Implementation Division in Lanham, Maryland, during the

[3] **********10********** provides solutions to the U.S. Government that include managing change and modernizing information systems for enterprise performance.

period August 2016 through December 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.

Results of Review

Based on our analyses of two different types of vulnerability and configuration scan reports, we determined that critical and high-risk vulnerabilities were generally remediated on hardware,[4] virtual machines, and software[5] in the IEP-RUP environment. Specifically, we found that the contractor had remediated 1,127 (91 percent) of **2** high-risk vulnerabilities identified from ***2*** scans and *2* (*2* percent) of **2** critical and high-risk vulnerabilities identified by **2**,[6] scans. We also found that the contractor had implemented an automated patching process.

However, we identified two areas of improvement needed to ensure that the IRS's IEP-RUP is protected against the exploitation of unpatched vulnerabilities and misconfigurations.

- We had concerns over the length of time for vulnerabilities to be patched and configuration weaknesses to be remediated in the IEP-RUP environment.
- While the contractor maintained an inventory list of the hardware and software in the IEP-RUP environment, we found that the inventory list was not always accurate and complete.

Failure to keep operating systems and application software patched and configured securely is one of the most common issues identified by security and information technology professionals. Security weaknesses within the environment could allow hackers to disrupt communications with users, alter or destroy sensitive data, or gain unauthorized access to other agency resources. Because sensitive tax information traverses through and resides on the IEP-RUP, the IRS and its web-based infrastructure are an attractive target for hackers. Vulnerabilities in the IEP-RUP environment unnecessarily expose taxpayer data to unauthorized access and disclosure. In addition, an inaccurate and incomplete inventory of components means the contractor may not be aware of (and therefore cannot fix) vulnerabilities that exist in the IEP-RUP environment.

[4] Hardware consists of routers, switches, and physical servers.

[5] Software consists of operating systems, web servers, and databases.

[6] ******************2******************.

Network and System Scans Identified Configuration Weaknesses and Vulnerabilities on Network Devices and Servers That Were Not Remediated and Were Not Timely Corrected

*************************************2***************,[7] **********2********** *************************************2************************************* *************************************2*******************.

**********************2********************
*********************2*******************

******2****** ******2******	******2****** ******2****** ******2****** ******2******	***********2*********** ***********2***********	***********2*********** ***********2*********** ***********2***********
******2*****|	****2****	**************2************** **************2**************	*********2********* *********2*********
******2*****	****2****	**************2************** **************2**************	*********2********* *********2*********
******2*****	****2****	**************2************** **************2**************	*********2********* *********2*********
******2*****	****2****	**************2************** **************2**************	*********2********* *********2*********

*************************************2************************************ **********2***********.

*************************************2***********,[8] ***********2************* *************************************2************************************* *************************************2************************************* *************************************2************************************* *************************************2************************************* *************************************2************************************* *************************************2*******************************.

For the RUP environment, ****10**** prepared and the IRS agreed to implement the IEP Continuous Monitoring Plan, dated April 8, 2016. This plan provided an effective approach to update the security patch management plan, scan for vulnerabilities, and maintain secure configurations and the overall secure posture of the IRS IEP. Specifically, it instructed the contractor to follow the Plan of Action and Milestones (POA&M) process when potential system weaknesses or deficiencies were identified. The POA&M is used to document and manage the

[7] **************2*************.
[8] **************2*************.

issue and to ensure that it is eventually resolved. The IEP Continuous Monitoring Plan further states that the remediation time frame for the POA&Ms that have been identified is the same as those in Figure 1. The POA&M is closed when the IRS approves it after the contractor has provided supporting artifacts, such as updated documentation, screenshots, and reports, verifying that proper remediation steps have been taken and appropriate changes have been put in place.

The IEP Continuous Monitoring Plan also references service level objectives (SLO) as pertinent to the success of IEP security. These SLOs are directly associated with and affected by the continuous monitoring program and are reported directly to IEP stakeholders. For security configuration compliance and security vulnerability remediation, the SLOs have been set at a compliance score of *******2*******.

*************************************2************************************
*************************************2************************************
*************************************2************************************
*************************************2************************************
*************************************2************************************
****************2******************,[9] ******************2******************
*************************************2***********************************.

****2**** configuration scan results showed that high-risk configuration weaknesses were not always remediated and were not always timely corrected

We reviewed the contractor's ****2**** Configuration Compliance reports from February 2016 through May 2017 and identified a total of **2** high-risk configuration weaknesses. ***2*** *************************************2************************************ *************************************2**************************. We found that **2** (*2* percent) of **2** high-risk configuration weaknesses were remediated by the contractor. Conversely, this means that *2* (*2* percent) high-risk configuration weaknesses were not corrected as of May 24, 2017. Further analysis showed that these *2* configuration weaknesses ****************************2************************************ *************************************2********************. Figure 2 shows a description of the vulnerability types along with the number of occurrences and the date they were first identified.

[9] *************2*************.

Figure 2: Unique High-Risk Configuration Weaknesses Identified in the *************2***************** That Were Unresolved As of May 2017**

Number	Date the Configuration Weaknesses Were First Identified[10]	Description of the Unique Configuration Weakness	Number of Occurrences
1	*********2*********	*********************2******************** *********************2******************** *****2*****.	**2**
2	*********2*********	*********************2******************** *********************2********************.	**2**
3	*********2*********	*********************2******************** *********************2******************** *********************2******************** *********************2******************** *****2*****.	**2**
4	*********2*********	*********************2******************** *********************2********************.	**2**
5	*********2*********	*********************2******************** *********************2********************.	**2**
6	*********2*********	*********************2******************** *********************2******************** *********************2******************** *********************2******************** *********************2******************** *********************2********************.	**2**
7	*********2*********	*********************2******************** *****2*****.	**2**
		Total	****2****

*Source: Treasury Inspector General for Tax Administration's (TIGTA) analysis of ***2*** Configuration Reports from February 2016 through May 2017.*

The Cybersecurity organization's April 2017 annual Security Assessment Report of the IEP that was conducted from October 5, 2016, through January 11, 2017, identified ********2******** ************************************2*********************************** ************************************2*******************************. Of the remaining *2* types, *2* was not found in the Cybersecurity organization's results because the date (March 22, 2017) was outside the review period. We believe *****2***** was due to the IRS's sampling methodology. The Cybersecurity organization recommended that the IRS's

[10] The dates are of the oldest weakness in each unique type.

authorizing official ensure that configuration settings are configured to the most restrictive mode, are enforced, and are documented for all system components. The Cybersecurity organization also recommended ensuring that all vulnerabilities identified by policy checkers are reviewed, analyzed, and appropriately addressed in accordance with IRM 10.8.1, *Information Technology Security, Policy and Guidance*.

2*************, we found a POA&M that was created on May 8, 2017. However, the POA&M was closed on May 23, 2017, showing that the weaknesses were closed because of an approved risk-based decision that establishes a minimum baseline requirement of a *2* percent compliance level with no high-risk or critical findings. To support the closure of the weakness, the contractor was to provide the risk-based decision document with a ***2*** Configuration Compliance report showing that the contractor met or exceeded the **2** percent compliance level with no high-risk failing checks. ***2*** ******************2*******************, we were unable to locate the required POA&Ms.

We reviewed the February and March 2016 ***2*** Configuration Compliance reports and determined that the contractor did not meet the SLO of *2* percent. For April and May 2016, the SLO did not apply because of ***********************2***************************** ******************2************. For June 2016 through April 2017, the contractor met the SLO; however, we identified high-risk failed configuration weaknesses. Therefore, the risk-based decision should not have been applied, and the POA&M should not have been closed.

After we provided our findings to the IRS and the contractor in July 2017, the IRS authorized the retraction of the risk-based decision document, and the POA&M was listed as “in-progress” in the Department of the Treasury’s management system.

<u>**Management Action**</u>**:** After the completion of fieldwork, the contractor’s employees provided evidence that they had corrected all ******************2*****************************. According to the contractor, *************2************ were now compliant with the configuration setting requirements. Because the corrections were provided to us after the end of our fieldwork, we did not verify that the configuration weaknesses were addressed *****2***** *****************2****************. The Cybersecurity organization’s Security Risk Management office conducts periodic risk assessments of agency operations or assets and should include the verification in its next periodic assessment of the IEP.

For the **2** high-risk configuration weaknesses *************2************ that the contractor remediated, we found *2* (*2* percent) high-risk configuration weaknesses that were remediated within 31 to 447 calendar days.[11] These servers support IEP-RUP applications, *e.g.*, Modernized Electronic Filing and Foreign Account Tax Compliance Act,that taxpayers and

[11] **2** **2** *********************2***********************.

tax practitioners use to obtain and transmit tax return information. Figure 3 shows the range of calendar days for the vulnerabilities.

Figure 3: High-Risk Configuration Weaknesses *************2***************** ***2*** That Were Not Remediated Within 30 Calendar Days***

Range in Calendar Days to Remediate Identified Weakness	Configuration Weaknesses
*********2*********	**2**
*********2*********	**2**
*********2*********	**2**
*********2*********	**2**
*********2*********	**2**
Total	****2****

*Source: TIGTA's analysis of ****2**** Configuration Reports from February 2016 through May 2017.*

************************************2*********************************** ************************************2*********************************** ***********2**********. In addition, the fact that the contractor closed the **2** weaknesses in less than **2** calendar days of the date we conducted our analysis and brought the high-risk configuration weaknesses to its attention sheds additional light on the length of time it takes to close high-risk configuration weaknesses during its day-to-day operations.

When we discussed our concerns over the length of time it took to remediate configuration weaknesses with the IRS and the contractor, ****2********************************** ************************************2*********************************** ******************2*******************. We referred them to the contractually bound IEP Continuous Monitoring Plan, which was created by the contractor and signed by the IRS in April 2016, for reference to the timeliness criteria and its applicability to configuration weaknesses and the POA&Ms. Upon reviewing the plan, the IRS and the contractor stated that the remediation time frame was an error and they would remove the remediation time frame reference.

************************************2*********************************** ************************************2*********************************** ************************************2*********************************** ************************************2*********************************** ************************************2*********************************** ************************************2*********************************** ************************************2***********************************

***************************************2**************************************
*********2*********.

2 vulnerability scan results showed that vulnerabilities were ********2********** ***2*** *****************2********************

From the contractor's **2** vulnerability scan results for October 2016 and February 2017, we identified *2* systems and system components, *e.g.*, hypervisors, firewalls, and embedded systems, that were scanned in both reports. For these *2* systems and system components, the scan reports presented information on **2** vulnerabilities, *i.e.*, critical, high-, medium-, and low-risk severity ratings, of which **2** (*2* percent) were remediated. Figure 4 provides the remediation status of the vulnerabilities by severity rating.

Figure 4: The Remediation Status of ***2* Scanned Vulnerabilities by Severity Rating for October 2016 and February 2017**

2 Scan Vulnerability Severity Ratings	Vulnerabilities	Count and Percentage of Vulnerabilities Remediated		Count and Percentage of Vulnerabilities Not Remediated	
Critical	**2**	**2**	**2**	**2**	**2**
High	**2**	**2**	**2**	**2**	**2**
Medium	**2**	**2**	**2**	**2**	**2**
Low	**2**	**2**	**2**	**2**	**2**
Total	****2****	****2****	****2****	****2****	****2****

Source: TIGTA's analysis of Nessus scan results for October 2016 and February 2017.

While the contractor can improve on its overall *2* percent remediation rate, we found that the remediation rate for the critical and high-risk vulnerabilities was at *2* percent (****2**** **************2******************). The remaining ***2*** vulnerabilities were not corrected in the **2** calendar days between ***********2***********. We used the date the October 2016 **2** scan was completed and the end of the **2** scan in February 2017 to compute the number of calendar days the **2** vulnerabilities had not been remediated because the first date each vulnerability was identified and actually remediated were unknown, with the exception of those addressed later in this section.

Initially, we focused our attention on the **2** critical and the **2** high-risk vulnerabilities because of their severity rating. ***********2**************************************
**************2*************.

- *******************************2**************************************
********2*************.

- ******************************2************************************
  ************2***********.

  ******************************2************************************
  ******************************2************************.

- ******************************2************************************
  ******************************2************************************
  ******************************2***************************.

<u>The **2 critical-severity vulnerabilities that were not remediated were reevaluated, and the severity ratings were changed to medium and low</u>.** When we presented our audit results to the contractor, the contractor explained that the **2**-identified critical-severity vulnerabilities were reevaluated using the Cybersecurity organization's *********2*********
**********************2*********************, and the severity ratings were changed to medium and low. The matrix consists of seven questions that the contractor answered about each of the vulnerabilities based on the contractor's knowledge of the actions needed to protect the systems and its components. The seven questions included the following three:

1) *Is the vulnerability widely known?*
2) *Is the exploitation of the vulnerability being reported?*
3) *How many systems are vulnerable?*

For each question, a numeric rating range between one and 10 was considered to determine the overall severity rating. At the completion of our fieldwork, the contractor shared its answers, and we determined the numeric ratings based on the contractor's answers for each severity rating that was changed. We did not conduct a comprehensive and detailed review of each of the answers and the numeric ratings. Regarding the **2** vulnerabilities:

- ******************************2************************************
  ******************************2************************************
  ******************************2************************************
  ******************************2********************.

- ******************************2************************************
  ******************************2************************************
  ******************************2************************************
  ******************************2************************************
  ****2****.

- ******************************2************************************
  ******************************2************************************
  ******************************2************************************
  ******************************2************************************

> *******************************2**************************************
> *******************************2**************************************
> *******************************2**************************************
> *******************************2*********************.

***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
*****2*****.

***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2************************************.

We reviewed the April 2016 security patch management plan and did not find the agreement the contractor referenced regarding the reevaluated vulnerabilities. Because we concluded that the ***2*** scan vulnerability rating of critical was still applicable to *********2*********, due to the lack of historical evidence to support the contractor's reevaluated rating, ******2****** ***************************************2****.

While we agreed with the reasoning for changing the severity ratings **********2*********** ********2********, we have concerns with the remediation process that was used. ****2**** ***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************
***************************************2**************************************

*************************************2*************************************
*************************************2*************************************
2.

*************************************2*************************************
*************************************2*************************************
*************************************2*************************************
*************************************2*************************************
*************************************2*************************************
**************2**************.

During our review of the August 2016 through May 2017 Vulnerability Assessment Reports, we noted that the vulnerability was reclassified from open to a POA&M. We researched the Department of the Treasury FISMA [Federal Information Security Modernization Act of 2014][12] Inventory Management System and did not find a POA&M for the vulnerability. Because vulnerability assessment reports show that the vulnerability is open to a POA&M, we believe one should be created or the contractor needs to create a risk-based decision because of the recurring vulnerability. In addition, while it is concerning that reports shared with the IRS are incorrect, we have an additional concern that the attention to the accuracy of the reports may be minimized because of the lower severity rating.

<u>The *2* high-risk vulnerabilities that were not remediated were reevaluated, and the severity ratings were changed to medium and low</u>. For the *2* vulnerabilities found on both the October 2016 and the February 2017 scan results, with the oldest vulnerabilities dating back to March 2013, we believe they should have been resolved long before February 2017. These **2** vulnerabilities stemmed from six unique vulnerabilities.[13] The largest group, consisting of *2* (*2* percent) of the *2* vulnerabilities, were related to ************2**************. *************************************2*************************************
*************************************2*************************************
*************************************2*************************************
*************************************2*************************************
*********2***********. Figure 5 presents information on all *2* vulnerabilities, including the descriptive name of the vulnerability, the date it was first identified, and the ******2****** identification number for the vulnerability.

[12] 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.
[13] The unique vulnerabilities can be identified in multiple systems or system components.

Figure 5: Details About the **2 High-Risk Vulnerabilities Identified by the ****2**** Scan That Were Reevaluated to Medium- or Low-Risk**

Number	Date the Vulnerabilities Were First Identified[14]	Nessus Identification Number	Descriptive Name or Description of the Unique Vulnerability	Vulnerabilities
1	*********2*********	****2****	*****************2*****************	**2**
2	*********2*********	****2****	*****************2***************** *****************2***************** *****************2**********.	**2**
3	*********2*********[15]	****2****	*****************2***************** *****************2***************** *****************2**********.	**2**
4	*********2*********	****2****	*****************2***************** *****************2***************** *****************2**********.	**2**
5	*********2*********	****2****	*****************2***************** *****************2***************** *****************2**********.	**2**
6	*********2*********	****2****	*****************2***************** *****************2***************** *****************2**********.	**2**
			Total	**2**

*Source: TIGTA's analysis of the October 2016 and February 2017 **2** vulnerability scan results.*

When we brought the *2* high-risk vulnerabilities to the attention of the contractor and the IRS, they explained that the ***2***-identified high-risk severity vulnerabilities were reevaluated using the Cybersecurity organization's *********************2************************ *************2************, and the severity ratings were changed to medium and low. The contractor used the same seven questions presented earlier in this report to determine the overall severity rating. At the completion of our fieldwork, the contractor provided us with its answers, and we determined the numeric ratings based on the contractor's answers for each severity rating that was changed. We did not conduct a comprehensive and detailed review of each of the contractor's answers and the numeric ratings. For the numeric ratings we did not agree with, we

[14] The date of the oldest vulnerability in each unique type.

[15] The vulnerabilities were first identified on ******2******, and subsequently closed *********2********* *****2****. The vulnerabilities *************2*************; therefore, we used this date for the date first identified.

would have selected a higher numeric rating or there was insufficient information available to assess the rating.

- *******************************2**************************************
  *******************************2**************************************.
- *******************************2**************************************
  *******************************2**************************************.
- *******************************2**************************************
  *******************************2**************************************
  *******************************2**************************************
  *******************************2**************************************.
- *******************************2**************************************
  *******************************2**************************************.
- *******************************2**************************************
  *******************************2**************************************.
- *******************************2**************************************
  *******************************2**************************************
  2.

*************************************2*********************, which resulted in *2* vulnerabilities, the contractor resolved the vulnerabilities in May 2017. However, the contractor took 223 calendar days from the time the vulnerability reappeared to the date the contractor stated that it resolved the vulnerability. We reviewed the October 2016 IEP Vulnerability Assessment report and found the following explanation on the delay in resolving this vulnerability: **********************2************************************** *************************************2************************************** *************************************2**********. Although the contractor noted in the Vulnerability Assessment report that ***********2**************, the contractor did not provide a***********2************** for our review.

While we generally agreed with the reasoning for changing the severity ratings for the remaining five unique vulnerabilities previously discussed, we have concerns with the remediation process that was used.

- *******************************2**************************************
  *******************************2**************************************
  *******************************2**************************************
  *************2**************.
- *******************************2**************************************
  *******************************2**************************************

*******************************2**************************************
*****2******.

- *******************************2**************************************
*******************************2**************************************
*******************************2**************************************
*********************2*******************.
- *******************************2**************************************
*******************************2**************************************
*******************************2**************************************
*******************************2**************************************
*******************************2**************************************
******2*****.

Lastly, we are concerned with the timeliness to remediate the vulnerabilities, the oldest of which was initially discovered in March 2013. While the contractor provided some ***2*** and we observed a reference to a POA&M, the contractor did not account for the length of time spent remediating these vulnerabilities.

From the aforementioned Vulnerability Assessment reports for the months of October 2016 and February 2017, we found the following explanations in the October 2016 report ******2****** ***************************************2************************************** ***************************************2************************************** ***************************************2************************************** ***************************************2******************** In July 2017, we presented our concerns to the IRS regarding the processing of ***2*** vulnerabilities, specifically, the IRS's involvement in the internal risk-based decision process. The Enterprise Technology Implementation Division Director stated that the IRS receives the internal ***2***, and that they are reviewed annually and are *********2**********.

While the IRS and its contractor continue their efforts to protect and provide access to systems that store and process taxpayer information through the IEP-RUP, our audit identified areas that should be improved in configuring systems, timely patching identified vulnerabilities, and following established procedures for monitoring and tracking security weaknesses. Failure to properly configure system components to the most restrictive settings compromises the security posture of the system that can lead to unauthorized access, increased vulnerability to attacks, and unauthorized data sharing and data exploitation, all of which compromise the integrity, confidentiality, and availability of the system.

Recommendations

The Chief Information Officer should:

Recommendation 1: Establish a policy for the contractor that ***********2************** ***************************************2***********************. In addition, correct the POA&Ms remediation time frame in the IEP Continuous Monitoring Plan that references the ****2**** and ***2*** schedule in ******2******.

Management's Response: The IRS agreed with this recommendation. The Cybersecurity organization plans to establish a policy for the contractor and has corrected the POA&M remediation time frames within the Continuous Monitoring Plan.

Recommendation 2: Ensure that the Cybersecurity organization validates that the contractor corrected the **************2***************** weaknesses and that the servers are compliant with the configuration setting requirements during its next scheduled assessment.

Management's Response: The IRS agreed with this recommendation. As part of the annual security review for the IEP information system, the Cybersecurity organization plans to validate that the *2* vulnerabilities have been remediated.

Recommendation 3: Ensure that when the contractor identifies potential system weaknesses or deficiencies from the *******2******* scans, the contractor complies with the POA&M process to document, manage, and eventually resolve the vulnerability. This process should also be used when the contractor meets the 90 percent SLO. For the **2** scan deficiencies, ensure that the contractor is more compliant with the ****2**** schedule outlined in ******2*****.

Management's Response: The IRS agreed with this recommendation. The Enterprise Operations organization created an updated vulnerability remediation SLO for vulnerability management and developed an IRS POA&M standard operating procedure that provides guidance for the handling of scan findings.

Recommendation 4: Ensure that the contractor creates and maintains documentation of its *************2**************** vulnerabilities in which the contractor provided us an incorrect ***2***. In addition, ensure that, before the **************2***************** ***************************************2************************************** ***************************************2************************************** ********************2*******************.

Management's Response: The IRS agreed with this recommendation. The Enterprise Operations organization updated the new patch management plan to show that the process has been revamped to ensure greater Federal oversight of the *****2*****.

Office of Audit Comment: The IRS's response did not address the *******2******* vulnerabilities for which the contractor provided TIGTA an incorrect ***2***. When we followed up and requested the correct **2**, the IRS could not immediately provide the information and stated it plans to add the requested information in the Department of the Treasury Joint Audit Management Enterprise System when it closes the planned corrective action for this recommendation.

Recommendation 5: Ensure that a risk-based decision is prepared for IRS approval for the ********2********* (because its severity rating is critical) as well as for *******2********* ***************************************2**************************. For the ********2*********, ensure that the contractor's technical team remediates the vulnerabilities as suggested by the industry leader (**********2************************************).

Management's Response: The IRS partially disagreed with this recommendation. The IRS stated that the ********2********* that TIGTA cited was downgraded from critical to moderate in accordance with the *****************2******************* *********************************2***********************. Per the approved IRS patch management plan, moderate vulnerabilities do not require risk-based decisions. In addition, the IRS stated that ********2********* was resolved on September 17, 2017, and has not appeared on the report since that time. Therefore, a risk-based decision is no longer required. If this vulnerability were to reappear on the **2** report, it would be triaged and handled according to its *****2**** severity level and a new risk-based decision document would be developed for appropriate approvals. Lastly, the IRS agreed with the recommendation on the ********2********* and the Enterprise Operations organization will remediate them.

Office of Audit Comment: We requested that the IRS provide documentation for the actions it claimed in its response. ***********2**************, the contractor only maintained documentation of the final decision to downgrade the vulnerability and explained why there was no historical data available for our review. The contractor used historical source data to answer the **2** questions to support the downgraded medium severity rating and provided them for our review. After reviewing the additional documentation provided, we still maintain that the **2** scan vulnerability rating of critical was still applicable to ********2*********** due to the lack of historical evidence to support the contractor's reevaluated rating. Therefore, we continue to believe that a risk-based decision should be created for IRS approval. ********2********** ****2****, the IRS provided supporting information to show that the vulnerability was resolved on September 25, 2017.

Recommendation 6: Ensure that the Enterprise Technology Implementation Division conducts a review of all internal risk-based decisions to ensure that: 1) at least a ***2*** exists for the vulnerabilities; 2) the *******2**********; and 3) the ***2*** accurately reflect the type of vulnerabilities that the technical team is addressing.

Management's Response: The IRS agreed with this recommendation. The Enterprise Operations organization updated the patch management plan to show that the process has been revamped to ensure greater Federal oversight of the ******2******.

Recommendation 7: Ensure that the contractor provides an accurate accounting of the status of vulnerabilities in reports that it shares with the IRS.

> **Management's Response:** The IRS agreed with this recommendation. The Enterprise Operations organization plans to ensure that thorough reviews are performed of monthly status reports and plans to conduct monthly stakeholder meetings prior to approval of the reports.

Improvement Is Needed to Ensure That the Information System Component Inventory Is Accurate and Complete

The contractor is contractually obligated to maintain an Information System Component Inventory, which includes physical servers, network devices, and virtual servers. The **2** *****2***** for the IEP requires the contractor to maintain a perpetual inventory of IEP components within the Configuration Management Database (CMDB). Additionally, the IEP inventory is to be ************************2************************************** ***2*** to the IEP environment take place. The inventory is to include the following items:

- *******2*******
- *******2*******
- *******2*******
- *******2*******
- *******2*******
- *******2*******
- *******2*******
- *******2*******
- *******2*******
- *******2*******

In September 2016, we obtained and reviewed the Information System Component Inventory provided by the contractor for the IEP-RUP infrastructure. We identified missing ***2*** ***2*** for all *2* physical servers and *2* network devices that included hardware and **2** ***2***. In addition, **********************2*************************************** ******2****** were missing for some of the physical servers and network devices. For the server inventory, we identified *******2******.

The contractor attributed the missing information to limitations of the discovery device used to identify the inventory components. For the major components in the server inventory, the contractor provided server naming conventions to assist with identifying the components. For the missing ******2******, the contractor attributed it to the process they used for extracting the information.

During our audit, the contractor worked to locate all missing information on its inventory. Specifically, the contractor admitted that correcting the inventory in the CMDB is largely a manual process. The contractor met with each team responsible for the various components to have them verify their devices line by line. All of the information was then entered into the

CMDB to achieve a correct inventory. The contractor stated that the reconciliation process would need to be a regular, recurring activity because it took a long time to perform it and provide us with an accurate inventory. The contractor further stated that if the reconciliation was performed at the end of each patching cycle, it could better keep up with the reconciliations (for example, looking for duplicate identifications and missing fields). The contractor stated that this was the first time it had performed this type of inventory reconciliation.

We reviewed the Cybersecurity organization's March 2015 IEP Security Assessment Report and found that the Cybersecurity organization also reported that the IEP inventory did not include the level of detail necessary for tracking and reporting and did not include necessary information to support component accountability. The report recommended that the authorizing official ensure that the inventory was accurate and was appropriately updated when components were installed, removed, and updated. A POA&M was created for this issue in April 2015. In November 2015, after conducting a follow-up review, the Cybersecurity organization validated that the issue was closed. We reviewed the artifacts that the Cybersecurity organization used to close the POA&M and found similar types of missing information that we found during our review more than a year later. One particular passage read as follows.

> *For example, in the installed devices, we identified the model number missing in *2* (*2* percent) of the *2* hardware and virtual devices listed in the inventory. The *****************2****************** was missing in *2* (*2* percent) of the *2* devices. For the installed servers, the ***********2************ were missing in *2* (*2* percent) of the *2* servers, and *******2******* ********2********** was missing in *2* (*2* percent) of the *2* servers.*

Cybersecurity organization officials stated that they had closed the POA&M as completed because they felt that the inventory file and the CMDB, as maintained by the portals, were sufficient to trace IEP assets. They added that their team validated the closure of the POA&M based on the fact that sufficient information was presented to attribute a hardware/server device to an owner. In addition to reviewing the IEP inventory file, the team also examined the CMDB tool that the contractor uses to manage the inventory to reach their conclusion. We reviewed the January 2016 Security Assessment Report and found it did not mention the issues reported for the IEP-RUP inventory.

2*
2*
2*
2*
2*
2*
2*
2*
2*

*************************************2****************. Failure to maintain a correct inventory of all components within the authorization boundary puts the system at risk of having insecure components that can introduce vulnerabilities into the system.

Recommendations

The Chief Information Officer should:

Recommendation 8: Ensure that the contractor performs, at a minimum, an annual reconciliation of the IEP inventory in the CMDB to ensure that it includes the components outlined in the System Security Plan and ******2****** to support effective component accountability.

> **Management's Response:** The IRS agreed with this recommendation. The Enterprise Operations organization plans to review the monthly inventory reports for accuracy and plans to make the report a formal deliverable for the IEP Security team.
>
> **Office of Audit Comment:** The IRS's response did not address our recommendation to perform, at a minimum, an annual reconciliation of the IEP inventory in the CMDB. When we followed up and requested an explanation for the missing information, the IRS stated it plans to add the requested information in the Department of the Treasury Joint Audit Management Enterprise System when it closes the planned corrective action for this recommendation.

Recommendation 9: Ensure that the Cybersecurity organization validates that the system inventory is reviewed as part of its next annual security assessment to ensure that it includes the component information deemed necessary as outlined in ********2******** and *******2*******.

> **Management's Response:** The IRS agreed with the recommendation. As part of the annual security review for the IEP information system, the Cybersecurity organization plans to review the IEP inventory and validate that it is in compliance with the **2**.

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to determine whether the IRS's IEP-RUP offering external web services to the public is timely patched and remediated when vulnerabilities or misconfigurations are identified.[1] To achieve our objective, we:

I. Determined whether the contractor maintained an inventory list of the physical and virtual hardware and operating software in the RUP.

A. Obtained the current, detailed inventory of all information technology assets for the IEP-RUP, including hardware and software from the contractor, and determined the accuracy of the data provided.

B. Interviewed IRS Cybersecurity organization personnel to determine whether they have any concerns about the information technology asset inventory for the IEP-RUP and whether they periodically validate it.

II. Determined whether the IEP-RUP components, *e.g.*, servers, routers, and switches, and databases have security patches installed and misconfigurations timely remediated in accordance with IRM and applicable Federal Government requirements.

A. Obtained the ***2*** Configuration Compliance Reports from the IRS's Enterprise Technology Implementation Division and the contractor, ***10***. To perform our analyses, we obtained the following data fields:

Field Name	Description
The Environment	Portal environment, *e.g.*, the RUP.
The Node Name	The system name of the specific inventory component.
The Node Type	The general categorization of the system, *e.g.*, *****2***** ***********2***********.
The Policy	The specific policy for the related requirement, *e.g.*, the IRS's IRM and NIST Special Publication 800-53.[2]
The Result Time	The last time the ****2**** scan identified a change in the configuration.
The Parent Test Group	The specific check to be performed.

[1] See Appendix IV for a glossary of terms.

[2] NIST Special Publication 800-53 Rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (Apr. 2013) (includes updates as of January 22, 2015).

Field Name	Description
The Result State	Passed or failed the configuration check.
The Description	A synopsis of the nature of the test.
The Actual Value	The result of the test.

1. To perform the data reliability and validation for configuration weaknesses, compared the results of the commercially available configuration compliance monitoring tool for each month between February 2016 and May 2017. For example, we reviewed for the proper report dates in the tool and that the data were for the RUP Portal.
2. Interviewed managers and contractor personnel who were knowledgeable about the report data and scanning processes. The data were used to identify configuration weaknesses and whether they were remediated and unresolved in the IEP-RUP components.
3. Conducted extensive analyses to determine the number of high-risk configuration weaknesses that were remediated and unresolved.

B. Evaluated monthly configuration and vulnerabilities scan reports to determine whether the IEP-RUP inventory components were properly configured and patched timely. We evaluated the reliability of the data and concluded that the reports were sufficiently reliable to identify the configuration weaknesses and missing patches associated with the IEP-RUP.

C. Obtained and tested 100 percent of the vulnerabilities identified by the ***2*** ********2******** on both the October 2016 and the February 2017 **2** scans.

1. To perform the data reliability and validation for the vulnerabilities, obtained the raw scan data from the commercially available vulnerability scanning tool, extracted the needed fields, and compared the results of the scans for October 2016 and February 2017. For example, we conducted a visual check by comparing some of the records from the extracted fields to the raw scan data. We also verified the record count between the extracted tools prior to use. As a result, we determined that the data were sufficiently reliable for purposes of this report.
2. Conducted extensive analyses to determine the number of critical, high-, medium-, and low-risk vulnerabilities that were remediated and unresolved from the scans. We further reviewed the high- and critical-severity *******2******* vulnerabilities that were open during the October 2016 scan and were still open in the February 2017 scan.

D. Determined the cause of the missing patches by interviewing ****10**** personnel responsible for the operations and maintenance of the IEP-RUP, and obtained copies of the support detailing why the patches had not been applied.

E. Obtained and reviewed the IEP contract between the contractor and the IRS to determine what scanning should be conducted of RUP components, *e.g.*, servers, routers, and switches, and ensured that patching and other vulnerabilities, *e.g.*, configuration errors, were timely identified.

F. Determined whether ***********2*********** results were improperly downgraded.

G. Determined whether the contractor's time frames for remediation of improperly downgraded vulnerabilities identified were in accordance with IRM 10.8.50, *Information Technology Security, Servicewide Security Patch Management.*

H. Determined whether improperly downgraded uninstalled patches have a formal risk-based decision, ***2****, or a documented mitigation strategy.

I. Determined whether patches were applied and misconfigurations were corrected timely to ensure protection of IRS computing components and information.

III. Determined whether automated patching was implemented for the IEP-RUP.

A. Determined whether the contractor has implemented automated patching for virtual machine-ware and ***********2*********** and any other components of critical infrastructure.

IV. Determined whether the unsupported information system software, *e.g.*, operating systems and databases, are in use in the IEP-RUP environment.

A. Identified operating systems and software for which the vendor no longer provides standardized technical support or for which such support will be ending in the immediate future.

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 IRMs for information technology security, policy, and guidance; the Task Order 21 Performance Work Statement; the System Security Plan; applicable NIST guidance, and the IEP Continuous Monitoring Plan. We evaluated these controls by interviewing the contractor and management in the Enterprise Technology Implementation Division. In addition, we reviewed POA&Ms in the Department of the Treasury FISMA Inventory Management System, ***********2*********** Configuration

Compliance Reports, Vulnerability Assessment Reports, the contractor's Information System Component Inventory, and the Cybersecurity organization's 2015 and 2016 Security Assessment Reports.

Appendix II

Major Contributors to This Report

Danny R. Verneuille, Assistant Inspector General for Audit (Security and Information Technology Services)
Kent Sagara, Director
Deborah Smallwood, Audit Manager
Charles Ekunwe, Lead Auditor
Linda Nethery, Information Technology Audit Specialist
Larry Reimer, Information Technology Audit Specialist

Appendix III

Report Distribution List

Deputy Commissioner for Operations Support
Chief Information Officer
Deputy Chief Information Officer for Operations
Associate Chief Information Officer, Cybersecurity
Associate Chief Information Officer, Enterprise Operations
Director, Office of Audit Coordination

Appendix IV

Glossary of Terms

Term	Definition
********2********	***************************2****************************** ***************************2****************************** ***************************2******************************.
Authorization Boundary	All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.
********2********	***************************2****************************** ***************************2****************************** ***************************2******************************.
Department of the Treasury FISMA Inventory Management System	The official FISMA repository tool for all Department of the Treasury bureaus. It is housed and maintained by the Department of the Treasury and is only accessible via an Internet Explorer link and approved access. No IRS data feed directly into it. Data are uploaded via user input into this tool as part of the efforts to comply with the E-Government Act of 2002,[1] NIST, and Office of Management and Budget regulations and guidance.
Disk Operating Systems	Operating systems used on computer systems with one or more disk drives.
Elevated Privilege	Any user right assignment that is above the baseline.
Embedded Systems	Some combination of computer hardware and software, either fixed in capability or programmable, that is designed for a specific function(s) within a larger system. Embedded systems are computing systems, but they can range from having no user interface to complex graphical user interfaces, such as in mobile devices.
Executable Files	Files that are used to perform various functions or operations on a computer.
Exploit	A general term for any method used by hackers to gain unauthorized access to computers, the act itself of a hacking attack, or a hole in a system's security that opens a system to an attack.

[1] Pub. L. No. 107-374.

Term	Definition
Federal Information Security Modernization Act	The FISMA of 2014[2] requires that Federal agencies have an annual independent evaluation performed of their information security programs and practices to determine the effectiveness of such programs and practices and to report the results to the Office of Management and Budget.
File Permissions	System settings that determine who can access specified files and what they can do with those files.
********2********	****************************2******************************* ****************************2*******************************.
Firewall	A gateway that limits access between networks in accordance with local security policy.
Firmware	Computer programs and data stored in hardware – typically in read-only memory or programmable read-only memory – such that the programs and data cannot be dynamically written or modified during execution of the programs.
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.
Guest Operating Systems	Operating systems running within virtual servers.
Hardening	Providing various means of protection in a computer system. Protection is provided in various layers and is often referred to as "defense in depth." Protecting in layers means to protect at the host level, the application level, the operating system level, the user level, the physical level, and all the sublevels in between. A hardened computer system is a more secure computer system.
********2********	****************************2******************************* ****************************2*******************************.
Host	A workstation or server.

[2] Pub. L. No. 113-283.

Term	Definition
Hypervisor	The virtualization component that manages the guest operating systems on a host and controls the flow of instructions between the guest operating systems and the physical hardware. It is also described as software that allows a single host to run one or more guest operating systems as well as can be referred to as a virtual machine manager.
Information System Component Inventory	An inventory of information system components that accurately reflects the current information system, includes all components within the authorization boundary of the information system, and includes all IRS-defined information deemed necessary to achieve effective information system component accountability.
Internet Explorer	A series of graphical web browsers developed by the Microsoft Corporation and included as part of the Microsoft Windows operating system.
Managed Service	The practice of outsourcing day-to-day management responsibilities and functions as a strategic method for improving operations and cutting expenses.
********2********	***************************2****************************** ***************************2****************************** ***************************2******************************.
********2********	***************************2****************************** ***************************2******************************.
Operating Systems	The master control program that runs a computer. The most important program process on a computer because it runs other programs. Operating systems also are responsible for security, such as ensuring that unauthorized users do not access the system.
********2********	***************************2****************************** ***************************2****************************** ***************************2******************************.
Packet	The unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network.
Packet-switched	A description of the type of network in which relatively small units of data called packets are routed through a network based on the destination address contained within each packet.

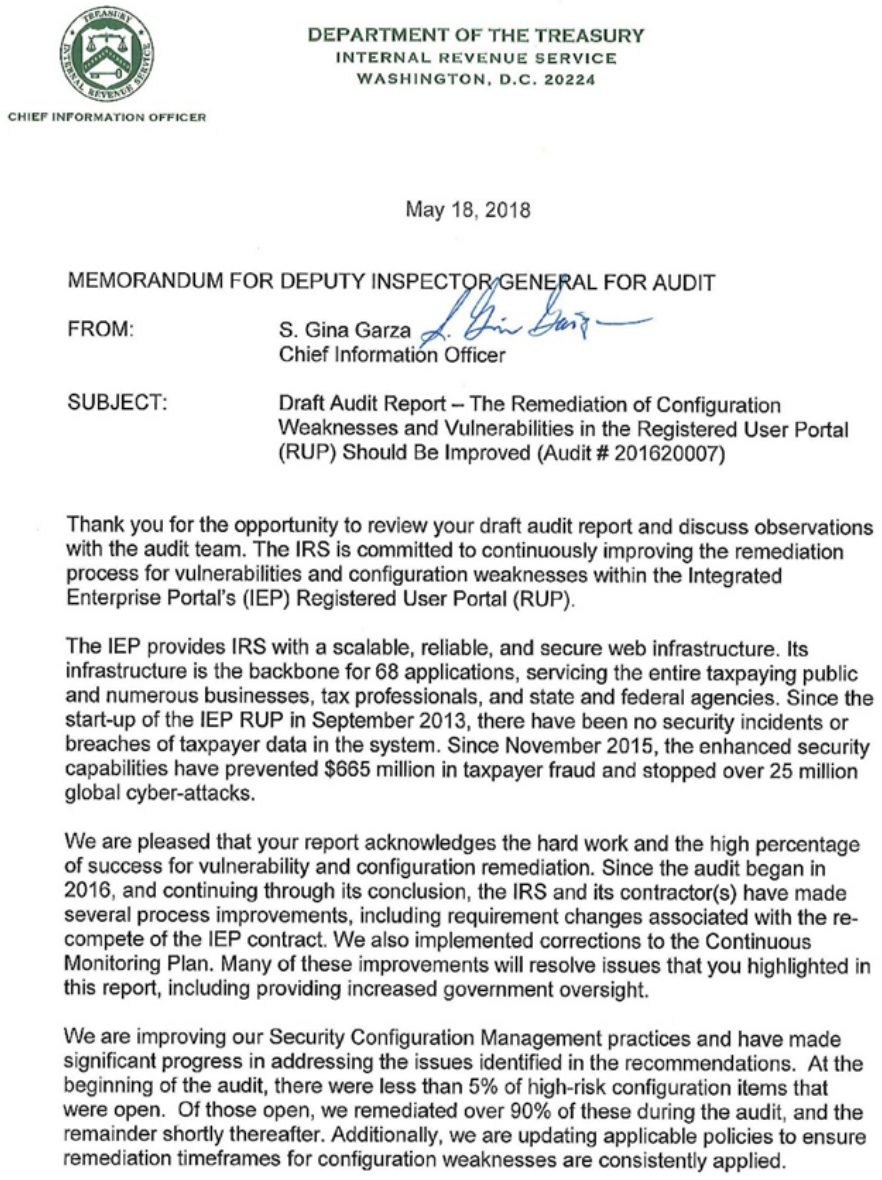
Term	Definition
********2********	*************************2**************************** *************************2**************************** *************************2****************************.
Physical Servers	A server (physical computer) on which an operating system,****2**** ***2***, runs just as on any other computer. The physical servers are in almost all aspects like desktop computers.
Policy Checkers	Validates the operating system security configuration of computers to IRS policy.
Portal	The web-based infrastructure (hardware and software) that serves as the entry point for web access to IRS applications and data.
Private Cloud	The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple consumers, *e.g.*, business units. It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off the organization's premises.
Reciprocity	The mutual agreement among participating organizations to accept each other's security assessments in order to reuse information system resources or to accept each other's assessed security posture in order to share information. Reciprocity is best achieved by promoting the concept of transparency, *i.e.*, making sufficient evidence regarding the security state of an information system available so that an authorizing official from another organization can use that evidence to make credible, risk-based decisions regarding the operation and use of that system or the information it processes, stores, or transmits.
********2********	*************************2**************************** *************************2**************************** *************************2**************************** *************************2****************************.
Remediation	The act of correcting a vulnerability or eliminating a threat through activities such as installing a patch, adjusting configuration settings, or uninstalling a software application.
********2********	*************************2**************************** *************************2**************************** *************************2****************************.
Router	A device or, in some cases, software on a computer, that determines the best way for a packet to be forwarded to its destination.

Term	Definition
Security Assessment Report	The purpose of the report is to provide the cyber executive and the authorizing official with a more holistic view of risk regarding a system that is being reviewed. It summarizes the risks associated with the vulnerabilities identified during the security assessment activities that were performed on the system. It provides the stakeholders with an assessment of the adequacy of the security and privacy controls used to protect the confidentiality, integrity, and availability of the system and the data it stores, transmits, or processes.
********2********	***************************2******************************.
Service Level Objective	A key element of a service level agreement between a service provider and a customer. The SLOs are agreed as a means of measuring the performance of the service provider and are outlined as a way of avoiding disputes between the two parties based on misunderstanding. The SLOs are pertinent to the success of IEP security and are directly reported to IEP stakeholders.
********2********	***************************2****************************** ***************************2******************************.
Switches	Small hardware devices that join multiple computers together with local area networks.
System Security Plan	A plan developed and documented for each General Support System and major application consistent with guidance issued by the NIST. It documents the current and planned controls for the information system and addresses security concerns that may affect the system's operating environment.
Task Order	An order for services placed against an established contract or with Government sources.
Tenable Security Center	An industry leading technology for host- and network-based vulnerability scanning. The Security Center consolidates and evaluates vulnerability data across an organization, prioritizing security risks and providing a clear view of an organization's security posture.
********2********	***************************2****************************** ***************************2****************************** ***************************2****************************** ***************************2****************************** ***************************2****************************** ******2******.

Term	Definition
********2********	***************************2****************************** ***************************2****************************** ***************************2******************************.
********2********	***************************2****************************** ***************************2****************************** ***************************2****************************** ***************************2****************************** ***************************2****************************** ***************************2******************************. ***************************2****************************** .
Virtual Machines	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.
Web Server	Can refer to either the hardware (the computer) or the software (the computer application) that helps to deliver content that can be accessed through the Internet.

Appendix V

Management's Response to the Draft Report



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

CHIEF INFORMATION OFFICER

May 18, 2018

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: S. Gina Garza
Chief Information Officer

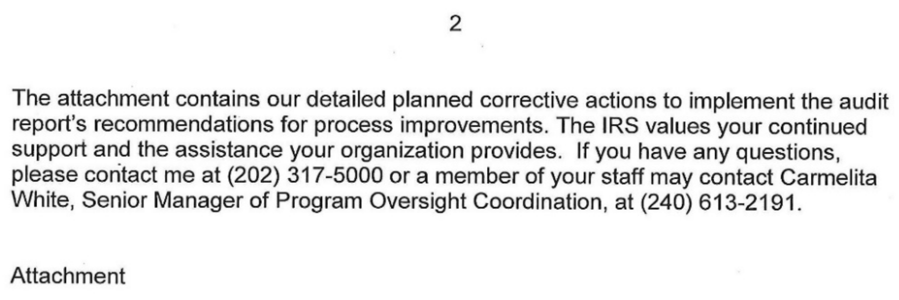
SUBJECT: Draft Audit Report – The Remediation of Configuration Weaknesses and Vulnerabilities in the Registered User Portal (RUP) Should Be Improved (Audit # 201620007)

Thank you for the opportunity to review your draft audit report and discuss observations with the audit team. The IRS is committed to continuously improving the remediation process for vulnerabilities and configuration weaknesses within the Integrated Enterprise Portal's (IEP) Registered User Portal (RUP).

The IEP provides IRS with a scalable, reliable, and secure web infrastructure. Its infrastructure is the backbone for 68 applications, servicing the entire taxpaying public and numerous businesses, tax professionals, and state and federal agencies. Since the start-up of the IEP RUP in September 2013, there have been no security incidents or breaches of taxpayer data in the system. Since November 2015, the enhanced security capabilities have prevented $665 million in taxpayer fraud and stopped over 25 million global cyber-attacks.

We are pleased that your report acknowledges the hard work and the high percentage of success for vulnerability and configuration remediation. Since the audit began in 2016, and continuing through its conclusion, the IRS and its contractor(s) have made several process improvements, including requirement changes associated with the re-compete of the IEP contract. We also implemented corrections to the Continuous Monitoring Plan. Many of these improvements will resolve issues that you highlighted in this report, including providing increased government oversight.

We are improving our Security Configuration Management practices and have made significant progress in addressing the issues identified in the recommendations. At the beginning of the audit, there were less than 5% of high-risk configuration items that were open. Of those open, we remediated over 90% of these during the audit, and the remainder shortly thereafter. Additionally, we are updating applicable policies to ensure remediation timeframes for configuration weaknesses are consistently applied.



2

The attachment contains our detailed planned corrective actions to implement the audit report's recommendations for process improvements. 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 Carmelita White, Senior Manager of Program Oversight Coordination, at (240) 613-2191.

Attachment

Attachment

Draft Audit Report - The Remediation of Configuration Weaknesses and Vulnerabilities in the Registered User Portal Should Be Improved

RECOMMENDATION 1: The Chief Information Officer should establish a policy for the contractor that **2*************************************. ********************2******************** In addition, correct the POA&Ms remediation time frame in the IEP Continuous Monitoring Plan that references the ******2****** and ******2****** schedule in the *******2*******.

CORRECTIVE ACTION 1: We agree with the recommendation. We will establish a policy for the contractor. In addition, we have corrected the POA&M remediation timeframes within the Continuous Monitoring Plan.

IMPLEMENTATION DATE: October 15, 2018

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

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

RECOMMENDATION 2: The Chief Information Officer should ensure that the Cybersecurity organization validates that the contractor corrected the ******2****** and *****2***** configuration weaknesses and that the servers are compliant with the configuration setting requirements during its next scheduled assessment.

CORRECTIVE ACTION 2: We agree with the recommendation. As part of the annual security review for the IEP information system Cyber will validate that the **2** vulnerabilities have been remediated.

IMPLEMENTATION DATE: September 15, 2018

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

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

RECOMMENDATION 3: The Chief Information Officer should ensure that when the contractor identifies potential system weaknesses or deficiencies from the *******2******* *****2***** scans, the contractor complies with the POA&M process to document, manage, and eventually resolve the vulnerability. This process should also be used when the contractor meets the ***2*** percent SLO. For the ****2**** scan deficiencies, ensure that the contractor is more compliant with the ***2*** schedule outlined in *****2*****.

Attachment

Draft Audit Report - The Remediation of Configuration Weaknesses and Vulnerabilities in the Registered User Portal Should Be Improved

CORRECTIVE ACTION 3: We agree with the recommendation regarding vulnerability management. An updated vulnerability remediation SLO has been created for vulnerability management. We agree with the recommendation regarding configuration management. We developed an IRS POA&M SOP that provides guidance for the handling of scan findings.

IMPLEMENTATION DATE: August 15, 2018

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Enterprise Operations

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 ensure that the contractor creates and maintains documentation of its *******************2******************** vulnerabilities in which the contractor provided us an incorrect *****2*****. In addition, ensure that, before the **********************2***
***2**
***2**
2****.

CORRECTIVE ACTION 4: We agree with this recommendation.We updated the new Patch Management Plan to show the process has been revamped to ensure greater Federal oversight of the ******2******.

IMPLEMENTATION DATE: August 15, 2018

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Enterprise Operations

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 - The Remediation of Configuration Weaknesses and Vulnerabilities in the Registered User Portal Should Be Improved

RECOMMENDATION 5: The Chief Information Officer should:

A. Ensure that a risk-based decision is prepared for IRS approval for the ******2******* ****2***** (because its severity rating is critical);

B. Ensure that a risk-based decision is prepared for IRS approval the *****2***** ***2** ******2******.

C. For the *********2**********, ensure that the contractor's technical team remediates the vulnerabilities as suggested by the industry leader (*****2****** ***********************2********************************).

CORRECTIVE ACTION 5A: The IRS disagrees with this recommendation. The ***********2********** that TIGTA cited was downgraded from critical to moderate in accordance with the *************************2*************************************** *****2*****. Per the approved IRS Patch Management Plan, Moderate Vulnerabilities do not require RBD's. The IRS can provide information that was used to downgrade the vulnerability.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL(S): N/A

CORRECTIVE ACTION MONITORING PLAN: N/A

CORRECTIVE ACTION 5B: We disagree with this portion of the recommendation. The **************2************** was resolved on September 17, 2017 and has not appeared on the report since September 2017. We will provide documentation to support this action. Therefore, a risk-based decision is no long required. If this vulnerability was to re-appear on the ***2*** report, it will be triaged and handled according to its *****2***** severity level and a new risk based decision document will be developed for appropriate approvals.

IMPLEMENTATION DATE: N/A

RESPONSIBLE OFFICIAL(S): N/A

CORRECTIVE ACTION MONITORING PLAN: N/A

CORRECTIVE ACTION 5C: We agree with this part of the recommendation. The *********2********** will be remediated.

IMPLEMENTATION DATE: August 15, 2018

Attachment

Draft Audit Report - The Remediation of Configuration Weaknesses and Vulnerabilities in the Registered User Portal Should Be Improved

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

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 6: Ensure that the Enterprise Technology Implementation Division conducts a review of all internal risk-based decisions to ensure that: 1) at least a *****2***** exists for the vulnerabilities; 2) the ************2************; and 3) the *****2***** accurately reflect the type of vulnerabilities that the technical team is addressing.

CORRECTIVE ACTION 6: We agree with this recommendation. The Patch Management Plan has been updated to show the process has been revamped to ensure greater Federal oversight of the ******2******.

IMPLEMENTATION DATE: August 15, 2018

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

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 7: The Chief Information officer should ensure that the contractor provides an accurate accounting of the status of vulnerabilities in reports that it shares with the IRS.

CORRECTIVE ACTION 7: We agree with this recommendation. We will ensure thorough review of monthly status reports and conduct monthly stakeholder meetings prior to approval of the reports.

IMPLEMENTATION DATE: February 15, 2019

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

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 - The Remediation of Configuration Weaknesses and Vulnerabilities in the Registered User Portal Should Be Improved

RECOMMENDATION 8: The Chief Information Officer should ensure that the contractor performs, at a minimum, an annual reconciliation of the IEP inventory in the CMDB to ensure that it includes the components outlined in the System Security Plan and ***********2*********** to support effective component accountability.

CORRECTIVE ACTION 8: We agree with this recommendation. We will review the monthly inventory reports for accuracy. The Inventory Report will now be made a formal deliverable for the IEP Security team.

IMPLEMENTATION DATE: May 15, 2019

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

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 9: The Chief Information Officer should ensure that the Cybersecurity organization validate that the system inventory is reviewed as part of its next annual security assessment to ensure that it includes the component information deemed necessary as outlined in ***********************2*************************.

CORRECTIVE ACTION 9: We agree with the recommendation. As part of the annual security review for the IEP information system, Cybersecurity will review the IEP inventory and validate it is in compliance with the IRMs.

IMPLEMENTATION DATE: September 15, 2018

RESPONSIBLE OFFICIALS: Associate Chief Information Officer, Cybersecurity

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