MANUAL TRANSMITTAL

10.8.50

Department of the Treasury
Internal Revenue Service

MARCH 11, 2024

EFFECTIVE DATE

(03-11-2024)

PURPOSE

(1) This transmits revised Internal Revenue Manual (IRM) 10.8.50, *Information Technology (IT) Security, Enterprise Incident, Vulnerability, and Security Patch Management.*

MATERIAL CHANGES

(1) IRM 10.8.50, formerly titled *Servicewide Security Patch Management*, has been renamed to *Enterprise Incident, Vulnerability, and Security Patch Management*.

(2) 10.8.50.1, Program Scope and Objectives - Subsection updated to align with standard security policy language.

(3) 10.8.50.1.1, Background - Subsection updated to align with standard security policy language.

(4) 10.8.50.1.1.1, Scope - Subsection removed to align with standard security policy language and IRM 1.11.2.2.4, *Address Management and Internal Controls*.

(5) 10.8.50.1.1.2, Objectives - Subsection removed to align with standard security policy language and IRM 1.11.2.2.4.

(6) 10.8.50.1.2, Authority - Subsection updated to align with standard security policy language.

(7) 10.8.50.1.3 (relocated from 10.8.50.2), Roles and Responsibilities - Updated to include Treasury IRP.

(8) 10.8.50.1.3.1 (relocated from 10.8.50.2.1), IRS Patch and Vulnerability Group (PVG) - Removed IRM 10.8.2-duplicated requirements. Added a reference for Exhibit 10.8.50-3, Security Notifications.

(9) 10.8.50.1.3.2 (relocated from 10.8.50.2.2), Authorizing Official (formerly Information System Owner) - Removed IRM 10.8.2-duplicated requirements. Updated subsection title. Updated Security Control family identifiers to align with NIST SP 800-53 Rev 5.1.1.

(10) 10.8.50.1.3.3, IRS Information Technology (IT) Organization and other Business Functional Unit Owners - Relocated subsection from 10.8.50.2.3.

(11) 10.8.50.1.3.4 (relocated from 10.8.50.2.4), Computer Security Incident Response Center (CSIRC) - updated subsection title.

(12) 10.8.50.1.3.5 (relocated from 10.8.50.2.5), Information Systems Security Officer - updated to include incident and vulnerability management.

(13) 10.8.50.1.4, Program Management and Review - Added subsection to align with standard security policy language and IRM 1.11.2.2.4.

(14) 10.8.50.1.5, Program Controls - Added subsection to align with standard security policy language and IRM 1.11.2.2.4.

(15) 10.8.50.1.6, Terms and Acronyms - Added subsection to align with standard security policy language and IRM 1.11.2.2.4.

(16) 10.8.50.1.7, Related Resources - Added subsection to align with standard security policy language and IRM 1.11.2.2.4.

(17) 10.8.50.2 (relocated from 10.8.50.1.3), Risk Acceptance and Risk-Based Decisions - Updated URL.

(18) 10.8.50.3 (relocated from 10.8.50.3), Incident, Vulnerability, and Security Patch Management - Updated title and content to include incident and vulnerability management. Updated references.

(19) 10.8.50.3.1, IRS Security Patch Management Approach - Subsection removed.

(20) 10.8.50.3.1, Incident Risk Responses - Added subsection to align with NIST SP 800-40 Section 2.1.

(21) 10.8.50.3.1.1, Incident Detection and Analysis - Added subsection to align with Treasury IRP Chapter 4.2 and Appendix D, Parts 1-6.

(22) 10.8.50.3.1.2, Major and Significant Incidents - Added subsection to align with Treasury IRP Chapter 4.2.3.1. Add TSSSOC responsibilities.

(23) 10.8.50.3.1.2.1, Incident Containment - Added subsection to align with Treasury IRP Chapter 4.3 and Appendix D, Part 7.

(24) 10.8.50.3.1.2.2, Incident Eradication - Added subsection to align with Treasury IRP Chapter 4.4.1 and Appendix D, Part 8.

(25) 10.8.50.3.1.2.3, Incident Recovery - Added subsection to align with Treasury IRP Chapter 4.4.2 and Appendix D, Part 9.

(26) 10.8.50.3.1.2.4, Post-Incident Activity - Added subsection to align with Treasury IRP Chapter 4.5 and Appendix D, Part 10.

(27) 10.8.50.3.1.3, Breach Risk/Harm Assessment - Added subsection to align with Treasury IRP Chapter 4.2.2.2. Added PGLD requirements.

(28) 10.8.50.3.2, Vulnerability Management - Added subsection to align with NIST SP 800-40 Section 2.2.

(29) 10.8.50.3.2.1, Reducing the Significant Risk of Known Exploited Vulnerabilities (KEVs) - Added subsection to align with IG Memo *Reducing the Significant Risk of Known Exploited Vulnerabilities*, Control Number: IT-10-1123-0008. Relocated CISA BOD 19-02 requirements from Security Patch Management subsection.

(30) 10.8.50.3.3, IRS Security Patch Management Approach - Relocated subsection from 10.8.50.3.1.

(31) 10.8.50.3.3.1 (relocated from 10.8.50.3.1.1), Assess Phase - Updated to align with Treasury IRP and NIST SP 800-40 Sections 2.2 and 3.3.

(32) 10.8.50.3.3.3 (relocated from 10.8.50.3.1.3), Evaluate and Plan Phase - Updated to align with NIST SP 800-40 v4 Section 2.3.1.

(33) 10.8.50.3.3.4 (relocated from 10.8.50.3.1.4), Deploy Phase - Updated to align with NIST SP 800-40 v4 Section 2.3.2.

(34) 10.8.50.3.3.5 (relocated from 10.8.50.3.1.5), Next Steps Phase - Updated to align with NIST SP 800-40 Sections 2.2 and 2.3.4.

(35) 10.8.50.3.4 (relocated from 10.8.50.3.2), Software Inventory - Updated to align with NIST SP 800-40 Sections 3.2, 3.4, 3.5, 3.5.1, 3.5.2, 3.5.3, 3.5.4, 3.5.5, and 3.7.

(36) 10.8.50.4, Operational Approach - Updated to use “IRS-defined” reference.

(37) 10.8.50.4.1, Security Patch Implementation Policy and Procedures - Updated to align with NIST SP 800-40 Section 3.1.

(38) 10.8.50.4.2, Assign Severity Levels - Updated to use “IRS-defined” reference.

(39) 10.8.50.4.3, Preparation of Security Patch Advisories - Updated to use “IRS-defined” reference.

(40) 10.8.50.4.4, Security Patch Advisory Acknowledgement of Receipt - Updated to use “IRS-defined” reference.

(41) 10.8.50.4.5, Patch Processing Metrics - Updated to use “IRS-defined” reference. Updated to align with NIST SP 800-40 Section 3.6.

(42) Exhibit 10.8.50-1, Sample IRS CSIRC Security Patch Advisory - Updated to use recent advisory for Oracle Enterprise Manager Vulnerabilities as a sample.

(43) Exhibit 10.8.50-2, CSIRC Vulnerability Ranking Matrix - Updated to align with IRS CSIRC.

(44) Exhibit 10.8.50-3, Security Notifications - Updated to align with IRS CSIRC and IG Memo *Reducing the Significant Risk of Known Exploited Vulnerabilities*, Control Number: IT-10-1123-0008. Updated to align with NIST SP 800-53 Rev 5.1.1.

(45) Exhibit 10.8.50-4, Updated title to Terms and Acronyms. Updated to add terms Actor Characterization, Breach, CISA, CMMI, CNSI, Compliance, Compliance mapping, Cross-Sector Dependency, CTI, Cyber Event, DISA, DNA, DNS, DoS, EO, Event Detected, Event Investigation Opened, Event Occurred, FedRAMP, FNA, FTP, Functional Impact, Hotwash, IG, IM, Incident, Incident Confirmed, Incident Resolved, Information Impact, IOC, IoT, IRP, ITIL, KEV, LSS, Major Incident, NARA, NCATS, NCCIC, NISTIR, Notable Cyber Event, Observed Activity – Location, Observed Effect/Consequence, Observed Engagement, Observed Notable Security Event, Observed Preparation, Observed Presence, ODNI, OMB, OT, PGLD, PII, Potential Impact, PPD, RDP, Recoverability, Risk, SaaS, SBU, Significant Cyber Incident, SMTP, Software Product, SSN, Suspected Breach, Suspected Incident, Suspected Incident Identified, TD, Threat, Threat Actor, TSSSOC, TTP, UTC, VAC, and VPN.

(46) Exhibit 10.8.50-5, Updated title to Related Resources. Updated release versions and release dates for references. Added references CISA BOD 22-01, Document 13347, Document 13347-A, IRM 10.5.4, IRM 10.8.24, IRM 11.3.38, NIST SP 800-61 Rev 2, NISTIR 8011, and PPD-41. Removed DISA as a reference.

(47) Interim Guidance Memoranda IT-10-1123-0008, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, dated January 1, 2024, incorporates Cybersecurity and Infrastructure Security Agency (CISA) Binding Operational Directive (BOD) 22-01 guidance to reduce the significant risk of known exploited vulnerabilities.

(48) Updated “section” to “subsection” throughout the IRM, as appropriate.

(49) Updated use of “shall” and “should” to “must” throughout the IRM.

(50) Editorial changes (including grammar, spelling, and minor clarifications) were made throughout the IRM.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes all prior versions of IRM 10.8.50, *Servicewide Security Patch Management* dated November 25, 2020. Additionally, this IRM was updated to incorporate Interim Guidance Memoranda Control

Number IT-10-1123-0008. This IRM supplements IRM 10.8.1, *Information Technology (IT) Security Policy and Guidance*; and IRM 10.8.2, *Information Technology (IT) Security, Information Technology Security Roles and Responsibilities*

AUDIENCE

The provisions in this manual apply to:
a) All offices and business, operating, and functional units within the IRS.
b) IRS personnel and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, which use or operate systems that store, process, or transmit IRS information or connect to an IRS network or system.

Rajiv Uppal
Chief Information Officer

10.8.50
Enterprise Incident, Vulnerability, and Security Patch Management

Table of Contents

Exhibits

10.8.50.1 (03-11-2024) Program Scope and Objectives

(1) **Overview:** This IRM lays the foundation to implement and manage security controls and guidance for the use of IRS incident, vulnerability, and security patch management within the IRS.

a. This policy is subordinate to IRM 10.8.1*, Information Technology (IT) Security, Policy and Guidance* and augments the existing requirements identified within IRM 10.8.1, as they relate to IRS incident, vulnerability, and security patch management.

(2) **Purpose of the Program:** Develop and publish security policies to protect the IRS against potential IT threats and vulnerabilities and ensure compliance with federal mandates and legislation.

(3) **Audience:** The provisions in this policy apply to:

a. All offices and business, operating, and functional units within the IRS.
b. IRS personnel and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, which use or operate systems that store, process, or transmit IRS Information or connect to an IRS network or system.

(4) **Policy Owner:** Chief Information Officer

(5) **Program Owner:** Cybersecurity Threat Response and Remediation (an organization within Cybersecurity)

(6) **Program Goals:** To protect the confidentiality, integrity, and availability of IRS information and information systems.

10.8.50.1.1 (03-11-2024) Background

(1) This IRM defines management of malicious activity and reduction of functional and information impact of cyber events through incident response and vulnerability management.

(2) This IRM defines the security patch management process to ensure the timely implementation of security patches for all IRS computers, networks, Commercial Off-The-Shelf (COTS) software, and IRS developed applications and software.

a. This document describes the internal policy with regards to the notification, testing, and installation of security-related patches for both software products and operating systems. While non-security related patches are important, their installation and testing are system and application dependent and, therefore, are not covered by this policy. This policy specifically relates to security-related patches. Organizations that maintain custom developed systems, network components, and applications are responsible for the maintenance and assessment of security patches that impact systems under their management and supervision.

(3) IRM 10.8.50 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS IT Cybersecurity.

10.8.50.1.2
(03-11-2024)
Authority

(1) All IRS systems and applications must be compliant with Executive Orders (EOs), Office of Management and Budget (OMB), Federal Information Security Modernization Act of 2014 (FISMA), National Institute of Standards and Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA), National Archives and Records Administration (NARA), Department of the Treasury, and IRS guidelines as they apply.

10.8.50.1.3
(03-11-2024)
Roles and Responsibilities

(1) IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities* defines IRS-wide roles and responsibilities related to IRS information and information system security and is the authoritative source for such information.

(2) The supplemental roles and responsibilities provided below are specific to the implementation of incident, vulnerability, and security patch management.

(3) The Treasury Departmental Incident Response Plan (IRP) provides guidance for preparation for incident response via roles and responsibilities. (Treasury IRP: Section 4.1)

a. Refer to IRM 10.8.2 for roles with incident response responsibilities.

(4) Due to the criticality of the patch management process, collaboration between multiple business units and information system owners is required. Stakeholders responsible for patch management operations process must:

a. Provide oversight of the patch management process including distribution and installation of patches.
b. Establish a formal operational agreement (e.g., service-level agreement (SLA), memorandum of understanding (MOU), concept of operations (CONOPS)). The agreement must be updated annually.
c. Develop and implement standard operating procedures (SOPs) on patch management, which must designate responsible organizations for carrying out each task. The SOPs must be updated annually.

10.8.50.1.3.1
(03-11-2024)
IRS Patch and Vulnerability Group (PVG)

(1) In accordance with NIST SP 800-40, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*, organizations must create a Patch and Vulnerability Group (PVG) to facilitate the identification and distribution of patches within the organization.

Note: This group may be an independent entity, or its duties may be performed by existing group(s) (e.g., Configuration Control Boards).

(2) The following functions must be performed by the designated IRS IT organization responsible for management and operations of the IRS IT resources.

(3) The PVG (or similar entity) must communicate any impact to businesses through the IRS Security Project Management Office (PMO).

(4) Members of groups or boards with patch management oversight responsibilities must sign up for an email distribution list to receive Computer Security Incident Response Center's (CSIRC) notifications and advisories. Refer to Exhibit 10.8.50-3, Security Notifications, for more information.

10.8.50.1.3.2
(03-11-2024)
Authorizing Official

(1) The appropriate authorizing official (AO) must approve new patch management technologies and services based on the assessment of risk. Refer to IRM 10.8.1 for Enterprise Life Cycle (ELC) and Business Impact Analysis guidance. Refer to IRM 10.8.1 for PM-05 Information System Inventory and PM-08 Critical Infrastructure Plan guidance.

10.8.50.1.3.3
(03-11-2024)
IRS Information Technology (IT) Organization and other Business Functional Unit Owners

(1) The IRS IT organization and other business and functional unit owners, that maintain systems, networks, IRS applications and COTS, must:

a. Develop implementation policies and procedures for managing security patches for the systems and applications which they are responsible for.
b. Review various sources for security-related patches specific to their systems and applications.
c. Notify CSIRC prior to working on each set of their pending patch activities.
d. Maintain hardware/software inventories.
e. Coordinate their patch activities with other information system owners.

(2) Business and functional unit owners must be represented on the PVG (or other entity).

10.8.50.1.3.4
(03-11-2024)
Computer Security Incident Response Center (CSIRC)

(1) The IRS IT organization's CSIRC must assist information system owners and other patch management stakeholders in defining relevant patches, prompting their implementation, and reporting their disposition.

(2) In accordance with Treasury Directive Publication (TD P) 85-01 and IRM 10.8.1 CSIRC must:

a. Publish vulnerability alerts, advisories, and bulletins on the CSIRC web site, to be used by information system owners and other patch management stakeholders. Refer to Exhibit 10.8.50-1, Sample IRS CSIRC Security Patch Advisory, for a sample advisory.
b. Designate which patches are security-related patches subject to enterprise security patch management policies and procedures.
c. Notify IRS management of critical vulnerabilities and patches to facilitate timely actions.
d. Review various sources for security-related system and application patches.
e. Coordinate with external (to IRS) organizations to remain current on known vulnerabilities, exploits, and patches.
f. Provide educational materials and information for distribution.
g. Maintain a Security Notification Mailing List, which includes the email addresses of all designated personnel with patch management responsibilities.
h. Assign a criticality level and associate an implementation schedule with each advisory.
i. Follow the procedures in this policy for advisory processing.
j. Send approved advisories as email messages to the PVG. The email subject line of an advisory must contain, IRS Patch Advisory <Advisory Number> <Alert Level> <Color Code> <Title>. Refer to IRM 10.8.50.5.2 Assign Severity Levels subsection within this IRM for additional information.

Note: Advisories published by CSIRC are not the all-inclusive authoritative source for vulnerabilities and patches. The advisories must be used by information system owners in collaboration with advisories from product vendors, Department of Homeland Security, and other relevant sources.

Note: This group may be an independent entity, or its duties may be performed by existing group(s) (e.g., Configuration Control Boards).

10.8.50.1.3.5
(03-11-2024)
Information Systems Security Officer

(1) Information systems security officer (ISSO) roles must be determined as needed to support incident, vulnerability, and patch management operational processes by the Associate Chief Information Officer (ACIO) of Cybersecurity and applicable AO.

10.8.50.1.4
(03-11-2024)
Program Management and Review

(1) The IRS Security Policy Program establishes a framework of security controls to ensure the inclusion of security in the daily operations and management of IRS IT resources. This framework of security controls is provided through the issuance of security policies via the IRM 10.8 series and the development of technology specific security requirement checklists. Stakeholders are notified when revisions to the security policies and security requirement checklists are made.

(2) It is the policy of the IRS:

a. To establish and manage an Information Security Program within all its offices. This policy provides uniform policies and guidance to be used by each office.
b. To protect all IT resources belonging to, or used by, the IRS at a level commensurate with the risk and magnitude of harm that could result from loss, misuse, or unauthorized access to that IT resource.
c. To protect its information resources and allow the use, access, disposition, and disclosure of information in accordance with applicable laws, policies, federal regulations, OMB guidance, TDs, NIST Publications, NARA guidance, other regulatory guidance, and best practice methodologies.
d. To use best practices methodologies (such as Capability Maturity Model Integration (CMMI), Enterprise Life Cycle (ELC), Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve IRS IT process and service efficiency and effectiveness.

10.8.50.1.5
(03-11-2024)
Program Controls

(1) Each IRM in the 10.8 series is assigned an author who reviews the IRM to ensure accuracy. The IRM authors continuously monitor federal guidance (e.g., OMB, CISA, NIST, Defense Information Systems Agency (DISA)) for potential revisions to security policies and security requirement checklists. Revisions to security policies and checklists are reviewed by the security policy team, in collaboration with applicable stakeholders, for potential impact to the IRS operational environment.

(2) Security Policy provides a report identifying security policies and security requirement checklists that have recently been revised or are in the process of being revised.

(3) This IRM applies to all IRS information and information systems, which include IRS production, development, test, and contractor systems. For systems that store, process, or transmit classified national security information, refer to IRM 10.9.1, *Classified National Security Information (CNSI)*, for additional guidance for protecting classified information.

(4) This IRM establishes the minimum baseline security policy and requirements for all IRS IT assets in order to:

a. Protect the critical infrastructure and assets of the IRS against attacks that exploit IRS assets.
b. Prevent unauthorized access to IRS assets.
c. Enable IRS IT computing environments to meet the security requirements of this policy and support the business needs of the organization.

(5) In the event there is a discrepancy between this policy and IRM 10.8.1, IRM 10.8.1 has precedence, unless the security controls/requirements in this policy are more restrictive.

10.8.50.1.6
(03-11-2024)
Terms and Acronyms

(1) Refer to Exhibit 10.8.50-4, Terms and Acronyms, for a list of terms, acronyms, and definitions.

10.8.50.1.7
(03-11-2024)
Related Resources

(1) Refer to Exhibit 10.8.50-5, Related Resources, for a list of related resources and references.

10.8.50.2
(03-11-2024)
Risk Acceptance and Risk-Based Decisions

(1) Any exception to this policy requires the AO to make a Risk-Based Decision (RBD).

(2) Users must submit RBD requests in accordance with Cybersecurity's Security Risk Management (SRM) Risk Acceptance Process documented in the Risk Based Decision Standard Operating Procedures (SOP).

# # # # #

(3) Refer to IRM 10.8.1 for additional guidance on Risk Acceptance.

10.8.50.3
(03-11-2024)
Incident, Vulnerability, and Security Patch Management

(1) Incident, Vulnerability, and Security Patch Management focuses on the management of incidents, vulnerabilities, and security patches in regard to risk associated with an application or system and the management of computer security controls to mitigate that risk. Refer to IRM 10.8.1 for general information and computer security management control requirements. (IRS-defined)

(2) Procedures for evaluating, approving, and installing security patches must be in place to ensure that the patches are installed within the patch severity timeframe and in conformance with appropriate configuration management plans, in accordance with IRM 10.8.1. (IRS-defined)

(3) The IRS must develop and implement incident, vulnerability, and security patch management plans for all of IRS IT systems and networks in accordance with: (IRS-defined)

- CISA Binding Operational Directive (BOD) 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*
- CISA BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*
- Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* and applicable controls listed in the following:
- NIST Special Publication (SP) 800-128, *Guide for Security-Focused Configuration Management of Information Systems*
- NIST SP 800-40 Rev 4, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology*
- NIST SP 800-53 Rev 5.1.1, *Security and Privacy Controls for Federal Information Systems and Organizations*
- NIST SP 800-70 Rev 4, *National Checklist Program for IT Products-Guidelines for Checklist Users and Developers*
- Appendix C of TD P 85-01 (TD P 85-01 Section 3.5)
- NIST Interagency Report (NISTIR) 8011, *Automation Support for Security Control Assessments*, Volume 1

10.8.50.3.1
(03-11-2024)
Incident Management

(1) Incident management must include risk response approaches of risk acceptance, risk mitigation, risk transference, and risk avoidance. (NIST SP 800-40: Section 2.1)

a. Planning for a risk response involves assessing the risk the vulnerability poses to the IRS, choosing which form of risk response (or combination of forms) to use, and deciding how to implement the risk response. (NIST SP 800-40: Section 2.2)

(2) When appropriate, a risk response may be “*Accept the Risk*.” The IRS may accept the risk from vulnerable software as is, such as by relying on existing security controls to prevent vulnerability exploitation or by determining that the potential impact is low enough that no additional action is needed. (NIST SP 800-40: Section 2.1)

(3) When appropriate, a risk response may be “*Mitigate the Risk*.” The IRS may reduce the risk by eliminating the vulnerabilities (e.g., patching the vulnerable software, disabling a vulnerable feature, or upgrading to a newer software version without the vulnerabilities) and/or deploying additional security controls to reduce vulnerability exploitation (e.g., using firewalls and network segmentation to isolate vulnerable assets, thus reducing the attack surface). (NIST SP 800-40: Section 2.1)

Note: Immediately patching, updating, or upgrading vulnerable software is sometimes not viable. Examples of why include the following:
(a) A patch may not be available yet. For example, a vulnerability may be announced before a patch is ready, and it could be days, weeks, or months before the patch is released.
(b) The vendor may no longer support the vulnerable software, meaning that a patch for it will never be released because the software is at end-of-life.
(c) The organization may need to wait for a scheduled outage window, perform testing first, update other software that interacts with the software to

be patched, or train employees on new features or interfaces.
(d) Some patches may be considered a higher priority, so other patches are delayed due to limited resources.
(e) The manufacturer may require customers to update the software on a delayed schedule, such as for assets with human safety implications in a highly regulated sector, because of the extensive testing and certification that must be performed first. In these cases, organizations that choose to implement updates on their own may be voiding the product warranty and preventing future support from the manufacturer.
(f) The organization may need to comply with specific legal, regulatory, or business requirements. For example, an organization may need to use FIPS-validated cryptographic modules for protecting data, but the cryptographic modules in the upgraded software are not yet FIPS-validated.

(4) When appropriate, a risk response may be "*Transfer the Risk*." The IRS may reduce the risk by sharing some of the consequences with another party, such as by purchasing cybersecurity insurance or by replacing conventional software installations with software-as-a-service (SaaS) usage where the SaaS vendor/managed service provider takes care of patching. (NIST SP 800-40: Section 2.1)

(5) When appropriate, a risk response may be "*Avoid the Risk*." The IRS may ensure that the risk does not occur by eliminating the attack surface, such as by uninstalling the vulnerable software, decommissioning assets with the vulnerabilities, or disabling computing capabilities in assets that can function without them. (NIST SP 800-40: Section 2.1)

(6) Refer to IRM 10.8.1 for additional guidance on Incident Response.

10.8.50.3.1.1
(03-11-2024)
Incident Detection and Analysis

(1) The IRS shall report breaches or incidents – regardless of severity or priority, whether confirmed or suspected, to the Treasury Shared Service Security Operations Center (TSSSOC) (portal: *https://treasury.servicenowservices.com/*) as quickly as possible after discovery and in no more than one business day. Bureaus shall not wait for absolute confirmation of a breach or incident before reporting. Analysis is often an ongoing process, and the IRS must not hold up reporting due to an inability to provide complete information. (Treasury IRP: Section 4.2)

Note: Incidents, breaches, and events may be detected by various means and by any individual personnel, as well as by IT and security teams through different methods such as antivirus systems, firewalls, intrusion detection systems, system log review, or observation by personnel.

Note: TSSSOC can provide investigative assistance to the IRS upon request including but not limited to host forensics, network forensics, log analysis, malware analysis, and cyber threat intelligence (CTI).

(2) The IRS must declare the incident by taking the following actions: (Treasury IRP: Section 4.2)

a. Perform initial categorization of incident. (OMB M-20-04)
b. Designate IRS incident coordination lead.
c. Notify CISA and, if applicable, law enforcement.

(3) The IRS must determine investigation scope by taking the following actions: (Treasury IRP: Section 4.2)

a. Identify the type and extent of the incident.
   i. Document (and provide to TSSSOC) contact information for both the impacted and reporting organizations.
   ii. Document (and provide to TSSSOC) description of what did or is suspected to have occurred, including impact.
   iii. Document (and provide to TSSSOC) date/time of occurrence, including time zone.
   iv. Document (and provide to TSSSOC) date/time of detection and identification, including time zone.
   v. Document (and provide to TSSSOC) associated system name (as tracked in TFIMS).
   vi. Document (and provide to TSSSOC) physical system location(s) (e.g., Washington, DC, Los Angeles, CA).
b. Assess operational or informational impact on IRS mission.
   i. Document (and provide to TSSSOC) functional impact.
   ii. Document (and provide to TSSSOC) information impact.
   iii. Document (and provide to TSSSOC) recoverability.

(4) The IRS must collect and preserve data by taking the following actions: (Treasury IRP: Section 4.2)

a. Collect and preserve the data necessary for incident verification, categorization, prioritization, mitigation, reporting, attribution, and as potential evidence in accordance with NIST SP 800-61, *Computer Security Incident Handling Guide*.
   i. Document (and provide to TSSSOC) mitigation actions taken or planned, if applicable.
   ii. Document (and provide to TSSSOC) impact assessment (i.e., number of records and/or users affected).
   iii. If applicable, document (and provide to TSSSOC) data elements/information types involved (e.g., social security number (SSN), name, phone numbers, taxpayer information, medical/health information, financial information).
   iv. If applicable, document (and provide to TSSSOC) information regarding vulnerable populations involved (e.g., children, active-duty military, government officials in sensitive positions, senior citizens, individuals with disabilities, confidential informants, witnesses, certain populations of immigrants, non-English speakers, and victims of certain crimes such as identity theft, child abuse, trafficking, domestic violence, or stalking).
   v. Document (and provide to TSSSOC) observed activity, if known.
   vi. Document (and provide to TSSSOC) free-form data or analyst comments and any of the following optional documentation:

- Related indicators (e.g., hostnames, domain names, network traffic characteristics, registry keys, X.509 certificates, MD5 file signatures)
- Details describing any vulnerabilities involved (i.e., Common Vulnerabilities and Exposures (CVE) identifiers)
- Source and destination Internet Protocol (IP) address, port, and protocol
- Operating System(s) affected
- Mitigating factors (e.g., full disk encryption or two-factor authentication)
- Device function(s) (e.g., web server, domain controller, or workstation)

- Sources, methods, or tools used to identify the incident (e.g., Intrusion Detection System or audit log analysis)

Note: The IRS is not required or expected to provide Actor Characterization, Cross-Sector Dependency, or Potential Impact information. These are assessed independently by National Communications, Coordination, and Integration Center (NCCIC)/CISA incident handlers and analysts. Additionally, Observed Activity is not currently required and is based on the attack vector, if known, and maps to the Office of the Director of National Intelligence (ODNI) Cyber Threat Framework.

b. Log all evidence and note how the evidence was acquired, when it was acquired, and who acquired the evidence.

(5) The IRS must perform technical analysis by taking the following actions: (Treasury IRP: Section 4.2)

a. Develop a technical and contextual understanding of the incident.
b. Based on analysis thus far and available CTI, form a hypothesis of what the adversary was attempting to access/accomplish.
c. Update scope as investigation progresses and information evolves. Report most recent findings and incident status to CISA.
d. Terminating condition: Technical analysis is complete when the incident has been verified, the scope has been determined, the method(s) of persistent access to the network has/have been identified, the impact has been assessed, a hypothesis for the narrative of exploitation has been cultivated (tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs)), and all stakeholders are proceeding with a common operating picture.
e. Correlate events and document timeline.
i. Analyze logs to correlate events and adversary activity.
ii. Establish an incident timeline that records events, description of events, date-time group (using Coordinated Universal Time (UTC)) of occurrences, impacts, and data sources. Keep updated with all relevant findings.
f. Identify anomalous activity.
i. Assess affected systems and networks for subtleties of adversary behavior which often may look legitimate.
ii. Identify deviations from established baseline activity - particularly important to identify attempts to leverage legitimate credentials and native capabilities and tools (i.e., living off the land techniques).
g. Identify root cause and enabling conditions.
i. Attempt to identify the root cause of the incident and collect threat information that can be used in further searches and inform subsequent response efforts.
ii. Identify and document the conditions that enabled the adversary to access and operate within the environment.
iii. Assess networks and systems for changes that may have been made to either evade defenses or facilitate persistent access.
iv. Identify attack vector. This includes how the adversary accessing the environment (e.g., malware, Remote Desktop Protocol (RDP), Virtual Private Network (VPN)).
v. Assess access (depth and breadth). This includes all compromised systems, users, services, and networks.

h. Gather Incident Indicators.
    i. Review available CTI for precedent of similar activity.
    ii. Analyze adversary tools. Assess tools to extract IOCs for short-term containment.
    iii. Identify and document indicators that can be used for correlative analysis on the network.
    iv. Share extracted threat information (atomic, computed, and behavioral indicators, context, and countermeasures) with internal response teams and CISA.

i. Analyze for common adversary TTPs.
    i. Identify initial access techniques (e.g., spear phishing, supply chain compromise).
    ii. If access is facilitated by malware, identify associated command and control (e.g., identify port, protocol, profile, domain, IP address).
    iii. Identify the techniques used by the adversary to achieve code execution.
    iv. Assess compromised hosts to identify persistence mechanisms.
    v. Identify lateral movement techniques. Determine the techniques used by the adversary to access remote hosts.
    vi. Identify the adversary's level of credential access and/or privilege escalation.
    vii. Identify the method of remote access, credentials used to authenticate, and level of privilege.
    viii. Identify mechanism used for data exfiltration.

j. Validate and refine investigation scope.
    i. Identify new potentially impacted systems, devices, and associated accounts.
    ii. Feed new IOCs and TTPs into detection tools.
    iii. Continue to update the scope and communicate updated scope to all stakeholders to ensure a common operating picture.

(6) The IRS must determine if third-party support is needed. (Treasury IRP: Section 4.2)

a. Identify if third-party analysis support is needed for incident investigation or response. CISA may recommend use of another agency or a third-party for intrusion detection and incident response support services.
b. Invoke Federal Network Authorization (FNA) to enable CISA incident response and hunt assistance. (CISA Services Catalog, First Edition: Autumn 2020)
c. Coordinate and facilitate access if incorporating third-party analysis support into response efforts.
d. Coordinate response activities with IRS service providers for systems hosted outside of the IRS.

(7) The IRS must adjust tools by taking the following actions: (Treasury IRP: Section 4.2)

a. Tune tools to slow the pace of advance and decrease dwell time by incorporating IOCs to protect/detect specific activity.
b. Introduce higher-fidelity modifications to tools. Tune tools to focus on tactics that must be used by the adversary to obtain operational objectives (e.g., execution, credential access, and lateral movement).

10.8.50.3.1.2
(03-11-2024)
Major and Significant Incidents

(1) To facilitate appropriate escalation, TSSSOC will use a color-coded severity schema to categorize incident, breach, and event reports. The IRS must include their perceived severity as of the time of the initial report to TSSSOC using the following: (Treasury IRP: Section 4.2.3.1)

Severity	Criteria (any that apply)
Red (High)	1. ″Major″ or “significant cyber” incident 2. Functional impact = ”Significant Impact to Critical Services” or “Denial of Critical Services / Loss of Control” 3. Information impact = “Critical Systems Data Breach” or “Core Credential Compromise” or “Destruction of Critical System” 4. Personally Identifiable Information (PII) loss >=100,000 records
Orange (Medium)	1. Functional impact = “Minimal Impact to Critical Services” or “Significant Impact to Non-Critical Services” 2. Recoverability = Not Recoverable 3. PII loss >= 100 records 4. Non-PII loss >= 100 records 5. Number of Users Affected >= 100
Yellow (Low)	1. Confirmed or suspected incident 2. Confirmed or suspected breach 3. Notable cyber event
White (Baseline)	1. Cyber event 2. Other tracked activities

(2) If an incident or breach constitutes a “major incident” and/or a “significant cyber incident” (Orange or Red incident), the IRS must perform incident containment, incident eradication, incident recovery, and post-incident activity. (Treasury IRP: Chapters 4.3, 4.5.1, 4.5.2)

(3) The IRS must implement a risk response. Examples of this include distributing and installing a patch, purchasing cybersecurity insurance, deploying additional security controls, and changing asset configurations and state (e.g., software reset, platform reboot). Any issues that occur during implementation must be resolved. (NIST SP 800-40: Section 2.2)

10.8.50.3.1.2.1
(03-11-2024)
Incident Containment

(1) If an incident or breach constitutes a “major incident” and/or a “significant cyber incident” (Orange or Red incident), the IRS must contain activity by taking the following actions: (Treasury IRP: Section 4.3)

a. Determine appropriate containment strategy, including consideration given to:

- Requirement to preserve evidence
- Availability of services (e.g., network connectivity, services continuity)
- Resource constraints

- Duration of containment steps

b. Perform system backup(s) to preserve evidence and continued investigation.
c. Coordinate with law enforcement to collect and preserve evidence prior to eradication, if applicable.
d. Isolate affected systems and networks including:

- Perimeter containment
- Internal network containment
- Host-based/Endpoint containment
- Temporarily disconnect public-facing systems from the Internet, etc.

e. Close specific ports and mail servers. Update firewall filtering.
f. Change system admin passwords, rotate private keys and service/application account secrets where compromise is suspected. Revoke privileged access.
g. Perform blocking (and logging) of unauthorized accesses, malware sources, and egress traffic to known attacker IP addresses.
h. Prevent Domain Name Server (DNS) resolution of known attacker domain names.
i. Prevent compromised system(s) from connecting to other systems on the network.
j. As needed, direct adversary to sandbox to monitor activity, gather additional evidence, and identify TTPs.
k. Monitor for signs of threat actor response to containment activities.
l. Report updated timeline and findings (including new atomic and behavioral indicators) to CISA.
m. If new signs of compromise are found, return to technical analysis to re-scope the incident.
n. Terminating condition: Upon successful containment (i.e., no new signs of compromise), preserve evidence for reference and law enforcement investigation (if applicable), adjust detection tools, and move to eradication.

10.8.50.3.1.2.2
(03-11-2024)
Incident Eradication

(1) If an incident or breach constitutes a “major incident” and/or a “significant cyber incident” (Orange or Red incident), the IRS must execute an eradication plan by taking the following actions: (Treasury IRP: Section 4.4.1)

a. Develop a well-coordinated eradication plan that considers scenarios for threat actor use of alternative attack vectors and multiple persistence mechanisms.
b. Provide incident status to CISA until all eradication activities are complete.
c. Remove artifacts of the incident from affected systems, networks, etc.
d. Reimage affected systems from clean backups (i.e., ‘gold’ sources).
e. Rebuild hardware (if rootkits involved).
f. Scan for malware to ensure removal of malicious code.
g. Monitor closely for signs of threat actor response to eradication activities.
h. Allow adequate time to ensure all systems are clear of threat actor persistence mechanisms (such as backdoors) since adversaries often use more than one mechanism.
i. Update the timeline to incorporate all pertinent events from this step.
j. Complete all actions for eradication.

k. Continue with detection and analysis activities after executing the eradication plan to monitor for any signs of adversary re-entry or use of new access methods.
l. If new adversary activity is discovered at the completion of the eradication step, contain the new activity and return to technical analysis until the true scope of the compromise and infection vectors are identified.
m. If eradication is successful, move to recovery.

10.8.50.3.1.2.3
(03-11-2024)
Incident Recovery

(1) If an incident or breach constitutes a “major incident” and/or a “significant cyber incident” (Orange or Red incident), the IRS must execute a recovery plan by taking the following actions: (Treasury IRP: Section 4.4.1)

a. Restore IRS systems to operational use: recovering mission/business data.
b. Revert all changes made during the incident.
c. Reset passwords on compromised accounts.
d. Implement multi-factor authentication for all access methods.
e. Install updates and patches.
f. Tighten perimeter security (e.g., firewall rulesets, boundary router access control lists) and zero trust access rules.
g. Test systems thoroughly (including security controls assessment) to validate systems are operating normally before bringing back online in production networks.
h. Consider emulating adversarial TTPs to verify countermeasures are effective.
i. Review all relevant CTI to ensure situational awareness of the threat actor activity.
j. Update incident timeline to incorporate all pertinent events from the recovery step.
k. Complete all actions for recovery.

10.8.50.3.1.2.4
(03-11-2024)
Post-Incident Activity

(1) If an incident or breach constitutes a “major incident” and/or a “significant cyber incident” (Orange or Red incident), the IRS must document the incident, inform IRS leadership, harden the environment to prevent similar incidents, and apply lessons learned to improve the handling of future incidents. (Treasury IRP: Section 4.5)

(2) The IRS must adjust sensors, alerts, and log collection by taking the following actions: (Treasury IRP: Section 4.5)

a. Add enterprise-wide detections to mitigate against adversary TTPs that were successfully executed.
b. Identify and address operational “blind spots” to adequate coverage moving forward.
c. Continue to monitor the IRS environment for evidence of persistent presence.

(3) The IRS must finalize reports by taking the following actions: (Treasury IRP: Section 4.5)

a. Provide post-incident updates as required by law and policy.
b. Publish post-incident report. Provide a step-by-step review of the entire incident and answer the Who, What, Where, Why, and How questions.

c. Provide CISA with a post-incident update within seven days of resolution or as directed by CISA in the Federal Incident Notification Guidelines.
d. Work with CISA to provide required artifacts, close the ticket, and/or take additional response action.

(4) The IRS must perform hotwash by taking the following actions: (Treasury IRP: Section 4.5)

a. Conduct lessons learned analysis with all involved parties to assess existing security measures and the incident handling process recently experienced.
b. Identify if IRS incident recovery processes were followed and if they were sufficient.
c. Identify any policies and procedures in need of modification to prevent similar incidents from occurring.
d. Identify how information sharing with CISA and other stakeholders can be improved during incident recovery.
e. Identify any gaps in incident responder training.
f. Identify any unclear or undefined roles, responsibilities, interfaces, and authorities.
g. Identify precursors or indicators that must be monitored to detect similar incidents.
h. Identify if IRS infrastructure for defense was sufficient. If not, identify the gaps.
i. Identify if additional tools or resources are needed to improve detection and analysis and help mitigate future incidents.
j. Identify any deficiencies in the IRS incident response planning process. If no deficiencies identified, identify how the IRS intends to implement more rigor in its incident recovery planning.

(5) The IRS will maintain detailed summaries of incidents and breaches and their subsequent investigations within the incident reporting system to assist the Treasury to track and monitor the following: (Treasury IRP: Section 4.5)

- The total number of incidents and breaches reported over a given period of time.
- The status for each reported incident, including whether the Bureau's response to that incident is ongoing or has concluded.
- The time elapsed:
  - From incident occurrence to detection.
  - From detection to initial investigation.
  - From initial investigation until report to TSSSOC.
  - From TSSSOC report receipt to CISA report (where applicable).
  - From initial investigation until resolution.
- For at least all Red and Orange incidents, a damage assessment, to include:
  - Service outage or system downtime periods.
  - Costs incurred, including hardware, software, labor, service, or any other applicable costs.
- In the event of a breach:
  - The number of individuals potentially affected by each reported breach.
  - The types of PII potentially compromised by each reported breach.
  - Whether the Bureau, after assessing the risk of harm, provided notifi-

cation to the individuals potentially affected by a breach.
- If notifications were sent, the elapsed time between breach confirmation and notification issuance.

10.8.50.3.1.3
(03-11-2024)
Breach Risk/Harm Assessment

(1) TSSSOC is the primary party responsible for ensuring appropriate Departmental (e.g., Treasury, TIGTA) and external resources (e.g., CISA, OMB, Congress) are engaged during an incident. (Treasury IRP: Section 4.2.3.2)

(2) For breaches that involve PII, the IRS must evaluate and assess the nature of the following data elements subject to the breach: (Treasury IRP: Section 4.2.2.2)

a. Single data elements that contain PII (e.g., SSNs, passport numbers, driver’s license numbers, state identification numbers, bank account numbers, passwords, and biometric identifiers).
b. Combination of non-sensitive data elements that when combined contain PII.

(3) For PII breaches, the IRS must evaluate and assess the following characteristics of the PII subject to the breach: (Treasury IRP: Section 4.2.2.2)

a. PII that may subject an individual to embarrassment, blackmail, or emotional distress (e.g., personnel or criminal information, personal debt and finances, medical conditions, treatment for mental health, pregnancy related information including pregnancy termination, sexual history or sexual orientation, adoption or surrogacy information, and immigration status).
b. PII that may subject an individual to identity theft or other financial risk (e.g., SSNs, bank account numbers, credit card numbers (especially when combined with the expiration date and security code), bank card pin numbers, passwords, or tax identification numbers).
c. PII that cannot be changed (e.g., permanent biometric information including fingerprints, hand geometry, retina or iris scans, and Deoxyribonucleic Acid (DNA) or other genetic information (considering both current and future uses).

(4) For PII breaches, the IRS must determine context by considering all relevant facts and circumstances regarding the breach and the PII involved in the breach. (Treasury IRP: Section 4.2.2.2)

a. Context must be considered in assessing risk (e.g., the name of an individual on a list of personnel who attended a meeting on tax policy vs. a name of an individual on a request for an accommodation for a disability).
b. Context including an assessment of the vulnerabilities of potentially affected individuals (e.g., children, active-duty military, government officials in sensitive positions, senior citizens, individuals with disabilities, confidential informants, witnesses, certain populations of immigrants, non-English speakers, and victims of certain crimes such as identity theft, child abuse, trafficking, domestic violence, or stalking) must be considered.

(5) For PII breaches, the IRS must determine the likelihood that the breached PII is accessible to and usable by those with unauthorized access to it. (Treasury IRP: Section 4.2.2.2)

a. Identify all security tools used to protect the data.

Note: This includes an analysis of all of the security features available in the format or media type involved, how long the PII was exposed, whether encryption was used, the likelihood that any encryption keys were exposed during the breach, whether PII was capable of and actually remotely wiped, and whether data masking, redaction, truncation, or anonymization were used (assuming the information underlying these techniques [e.g., redacted information available in the system to some but not all users] was not itself exposed during the breach).

b. Determine how long the PII was exposed.
c. Assess whether evidence of misuse already exists.

(6) For PII breaches, the IRS must assess whether the breach was intentional or unintentional by reviewing the following: (Treasury IRP: Section 4.2.2.2)

a. Evidence of intent to target the information or device may elevate risk.
b. Lack of evidence of intent to target the information or device may still reveal a high risk.
c. Evidence that the PII was disclosed to a known or unknown recipient.

(7) Data breaches (incidents involving PII) must be reported to Privacy, Governmental Liaison and Disclosure (PGLD)/Incident Management (IM) immediately upon discovery using the PII Breach Reporting form. Refer to the PGLD website at https://irsgov.sharepoint.com/sites/PGLD. (IRS-defined)

a. PGLD's Incident Management Program includes the management of the IRS data breach reporting process, as well as the risk assessment and tracking of IRS data breaches and notification to individuals potentially impacted by IRS data breaches.
b. Refer to IRM 10.5.4, *Privacy and Information Protection, Incident Management Program*; Document 13347, *Data Breach Response Playbook*; Document 13347-A, *IRS Data Breach Response Plan*; and the Report Losses, Thefts or Disclosures page located at https://irsgov.sharepoint.com/sites/ETD-KMT-KB003/SitePages/Privacy/Report_Losses_Thefts_Disclosures/Report_Losses_Thefts_Disclosure.aspx in the Disclosure and Privacy Knowledge Base site for additional information about PGLD's Incident Management Intake, Risk Assessment, and Notification process.
c. Refer to IRM 11.3.38, *Disclosure of Official Information, Role and Responsibilities of Disclosure*, for additional information on Reporting Suspected Willful Unauthorized Accesses or Disclosures.

(8) For PII breaches, the IRS must determine the capability of the IRS to independently mitigate the harm resulting from the breach. (Treasury IRP: Section 4.2.2.2)

10.8.50.3.2 (03-11-2024) Vulnerability Management

(1) The IRS must know when new software vulnerabilities affect IRS assets, including applications, operating systems, and firmware. This involves knowing what assets the IRS uses and which software and software versions those assets run down to the level of packages and libraries, as well as keeping track of new vulnerabilities in that software. For example, the IRS might subscribe to vulnerability feeds from software vendors, security researchers, and the National Vulnerability Database (NVD). (NIST SP 800-40: Section 2.2)

10.8.50.3.2.1 (03-11-2024) Reducing the Significant Risk of Known Exploited Vulnerabilities (KEVs)

(1) Common secure configurations (Common Configuration Enumerations (CCEs)) must be established and applied to prevent attackers from compromising a system or device which in turn may be used as a platform to compromise other systems or devices. (NISTIR 8011 Vol 1)

(2) Software and firmware vulnerabilities (CVEs) must be identified and patched to prevent attackers from compromising a system or device which in turn may be used to compromise other systems or devices. (NISTIR 8011 Vol 1)

Note: The NVD provides a library of vulnerabilities mapped to vulnerable software. Responses may include applying patches, installing more secure versions, or accepting the risk. Common Weakness Enumeration (CWE) scanning tools may identify poor coding practices that are directly associated with conditions that often manifest themselves as vulnerabilities that are discovered and assigned a CVE.

(3) The IRS must perform the following actions, for vulnerability remediation requirements for internet-accessible systems: (CISA BOD 19-02)

a. Ensure Cyber Hygiene access and verify scope:
i. Remove Cyber Hygiene source IP addresses from block lists to ensure Cyber Hygiene scanning access;
ii. Notify CISA at NCATS@hq.dhs.gov within five working days of any modification(s) to IRS Internet-accessible IP addresses; and

Note: This includes newly acquired Internet-accessible IP addresses or reassigned Internet-accessible IP addresses that are no longer part of the IRS asset inventory.

iii. Submit updated Cyber Hygiene agreements to NCATS@hq.dhs.gov upon request from CISA.

b. Review and remediate critical and high vulnerabilities:
i. Review Cyber Hygiene reports issued by CISA upon receipt;
ii. Remediate the critical and high vulnerabilities detected on IRS Internet-accessible systems; and
-- 1. Critical vulnerabilities must be remediated within 15 calendar days of initial detection.
-- 2. High vulnerabilities must be remediated within 30 calendar days of initial detection.

Note: Initial detection dates for identified vulnerabilities are included within Appendix G of the Cyber Hygiene report.

iii. Review CISA remediation plans identifying all overdue, in-scope vulnerabilities.
-- 1. Complete the following fields within the remediation plan:

------ a. Vulnerability remediation constraints;
------ b. Interim mitigation actions to overcome constraints; and
------ c. Estimated completion dates to remediate the vulnerability.
-- 2. Return completed remediation plans within three days of receipt to FNR.BOD@hq.hds.gov.

Note: Refer to CISA BOD 19-02 Frequently Asked Questions for guidance on resolving “false positives” of Cyber Hygiene-identified vulnerabilities.

Note: Refer to CISA BOD 19-02 for additional guidance: *https://cyber.dhs.gov/bod/19-02/*.

c. Coordinate with the affected ACIO area to minimize impact to operations and restoration of lost capabilities. (IRS-defined)

(4) The IRS must perform the following actions, in accordance with CISA guidance for reduction of significant risk of known exploited vulnerabilities (KEVs): (CISA BOD 22-01)

a. Document vulnerability management procedures, for the following actions, by January 3, 2022:
i. Establishing a process for ongoing remediation of vulnerabilities that CISA catalogs and within remediation timeframes set forth by CISA;
ii. Assigning roles and responsibilities for ongoing remediation of vulnerabilities that CISA catalogs and within remediation timeframes set forth by CISA;
iii. Defining necessary actions required to enable prompt response to remediation actions required by CISA;
iv. Establishing internal validation and enforcement procedures to ensure adherence to remediation of vulnerabilities that CISA catalogs; and
v. Setting internal tracking and reporting requirements to evaluate adherence to remediation of vulnerabilities that CISA catalogs and to provide reporting to CISA.

Note: CISA provides a catalog, or repository, of known exploited vulnerabilities at the web site: *https://cisa.gov/known-exploited-vulnerabilities*.

b. Remediate all vulnerabilities identified within the CISA-managed vulnerability catalog according to the timelines set forth in the catalog.

> ***Note:*** The default remediation timeline requirements are to remediate within 6 months for vulnerabilities having a CVE ID assigned prior to 2021 and within two weeks for all other vulnerabilities. These default timelines may be adjusted by CISA in the case of grave risk to the Federal Enterprise.

> ***Note:*** CISA provides a catalog, or repository, of KEVs at the web site: *https://cisa.gov/known-exploited-vulnerabilities*.

c. Report on the status of vulnerabilities listed in the CISA catalog.
i. The IRS must automate data exchange and report implementation status through the Continuous Diagnostics and Mitigation (CDM) Federal Dashboard.
ii. Prior to October 1, 2022, the IRS must submit quarterly reports either through CyberScope submissions or through the CDM Federal Dashboard.
iii. Starting on October 1, 2022, if the IRS has not yet automated report-

ing to the CDM Federal Dashboard, the IRS must update status through CyberScope bi-weekly, until that automation, through the CDM Federal Dashboard, occurs.

Note: Refer to CISA BOD 22-01 for additional guidance: *https://cyber.dhs.gov/bod/22-01/*.

(5) Refer to IRM 10.8.1 for additional guidance on Flaw Remediation.

10.8.50.3.3
(03-11-2024)
IRS Security Patch Management Approach

(1) In accordance with TD P 85-01, the IRS security patch management program must:

a. Ensure patch development is controlled as programs progress through testing to final approval.
b. Ensure test plan standards have been developed for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, and library control).
c. Ensure detailed system specifications are prepared by the programmer and reviewed by a programming supervisor.
d. Ensure patch test plans are documented and approved defining responsibilities for each party involved (e.g., users, systems analysts, programmers, auditors, quality assurance, and library control).
e. Ensure unit, integration, and system patch testing are performed and approved in accordance with the test plan and applying a sufficient range of valid and invalid conditions.
f. Ensure a comprehensive set of patch test transactions and data is developed representing the various activities and conditions that will be encountered in processing.
g. Ensure live data is not used in patch testing of program changes, except to build patch test data files.

Note: Refer to IRM 10.5.8, *Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments*, for additional clarification on exceptions for use of live data.

(2) The IRS approach to security patch management must be applied through the implementation of controls consisting of five phases: (IRS-defined)

- Assess
- Identity
- Evaluate and Plan
- Deploy
- Next Steps

10.8.50.3.3.1
(03-11-2024)
Assess Phase

(1) During the Assess phase, the IRS must define baseline systems and networks before an incident occurs to understand the basics of “normal” activity (Treasury IRP: Section 4.1):

a. Assess the current production environment:
   i. Identify business-critical assets.
   ii. Determine which systems and applications are in the production environment.

b. Determine security threats and vulnerabilities:
   i. Determine the threats to, and vulnerabilities of, the production environment.
c. Develop a plan to implement new security patches:
   i. Determine which systems and applications can automatically receive security patches and those systems that require manual installation.
   ii. Ensure that security patch distribution tools are configured, maintained, and able to support normal and emergency security patch installations.
d. Ensure that technical personnel have assigned roles and responsibilities and that they know how to deal with the security patch update and how to mitigate its impact.

(2) The IRS must prepare for risk responses. This encompasses any preparatory activities, such as acquiring, validating, and testing patches for the vulnerable software; deploying additional security controls to safeguard the vulnerable software; or acquiring a replacement for a legacy asset that cannot be patched. It might also include scheduling the risk response and coordinating deployment plans with enterprise change management, business units, and others. (NIST SP 800-40: Sections 2.2, 3.3)

10.8.50.3.3.2
(04-26-2016)
Identify Phase

(1) During the Identify phase, the IRS must: (IRS-defined)

a. Identify new security patch updates in a reliable way:
   i. Ensure that a mechanism is available to be notified of all security patch updates.
   ii. Confirm that security patch update notification comes from an authorized source.
b. Determine if the security patch updates are relevant to the production environment:
   i. Ensure that the security patch update is relevant to systems in the IRS production environment.
   ii. Obtain the security patch update source files and confirm that they are virus free.
c. Determine the urgency of the security patch update:
   i. Determine whether the patch update is an emergency and submit a Request for Change (RFC) to deploy it into production.
   ii. Ensure the receipt and verification of relevant security patch updates, and that they are safe to deploy.

10.8.50.3.3.3
(03-11-2024)
Evaluate and Plan Phase

(1) During the Evaluate and Plan phase, the IRS must: (IRS-defined)

a. Evaluate security patches to determine the implication of an implementation.
b. Develop a strategy to deploy security patches:
   i. Establish a formal process to determine whether it is in the best interests of the IRS to deploy the security patch updates.
   ii. Determine the owner of the security patch update(s) who will be responsible for ensuring that it is deployed.
   iii. Develop a systemic approach for rolling out the patch to the production environment.
c. Prioritize security patches based upon effectiveness of patches and upon criticality of assets. (NIST SP 800-40: Section 2.3.1)
d. Schedule security patch deployment as part of IRS change management activities. (NIST SP 800-40: Section 2.3.1)

e. Acquire the security patch through being downloaded from the internet, built internally by developers or system administrators, or provided through removable media. (NIST SP 800-40: Section 2.3.1)
f. Validate the security patch to determine the patch's authenticity and integrity, preferably by automated means. (NIST SP 800-40: Section 2.3.1)
g. Test security patches in a test environment prior to deploying security patches into the production environment to reduce operational risk and to ensure the security patch does not compromise business critical systems and applications. Testing may be performed manually or through automated methods. (NIST SP 800-40: Section 2.3.1)
h. Survey the production environment to ensure the system or application will handle the security patch updates.

10.8.50.3.3.4
(03-11-2024)
Deploy Phase

(1) During the Deploy phase, the IRS must: (IRS-defined)

a. Distribute the patch. (NIST SP 800-40: Section 2.3.2)
b. Validate the patch. (NIST SP 800-40: Section 2.3.2)
c. Install the patch. (NIST SP 800-40: Section 2.3.2)
d. Change software configuration and state. (NIST SP 800-40: Section 2.3.2)
e. Resolve any issues. (NIST SP 800-40: Section 2.3.2)
f. Verify deployment. Rescan the environment to assess success, and patch any computers or applications that failed to install the security patch updates. (NIST SP 800-40: Section 2.3.3)
g. Ensure that the security patch update installation is successful.
h. Perform a review of the security patch management process once the deployment is complete.

10.8.50.3.3.5
(03-11-2024)
Next Steps Phase

(1) Once IRS personnel have deployed the security patch update, the IRS must: (IRS-defined)

a. Inventory/discover existing computing assets.
b. Assess security threats and vulnerabilities.
c. Determine the best source for information about patch updates.
d. Assess the existing software distribution infrastructure.
e. Assess operational effectiveness.

(2) The IRS must verify the risk response. This step involves ensuring that the implementation has been completed successfully. For patching, this means confirming that the patch is installed and has taken effect. For deploying additional security controls, ensure they are functioning as intended. For risk avoidance, verify that vulnerable assets were decommissioned or replaced. (NIST SP 800-40: Section 2.2)

(3) The IRS must continuously monitor the risk response**.** Make sure that the risk response continues to be in place: no one uninstalls the patch, deactivates the additional security controls, lets the cybersecurity insurance lapse, or restarts the decommissioned asset. (NIST SP 800-40: Sections 2.2, 2.3.4)

10.8.50.3.4
(03-11-2024)
Software Inventory

(1) As part of an effective Patch Management Program, software inventory and baseline configurations must be established and maintained in accordance with IRM 10.8.1, for physical and virtual computing assets, including operational technology (OT), Internet of Things (IoT), and container assets. (NIST SP 800-40: Section 3.2)

a. At a minimum, the inventory must contain:

- Operating systems
- Versions of all software
- Patch levels
- Installed applications
- Mission/business characteristics

b. The inventory must be updated as software is added or deleted from the baseline.
c. Changes to the baseline must be documented in a timely manner.
d. The baseline inventory must be managed by version control to provide a record of changes over time.

(2) The IRS must use the software inventories, technical and business/mission characteristics, and risk response scenarios to assign each asset to a maintenance group. Sample maintenance groups may be any of the following: (NIST SP 800-40: Section 3.4)

- Mobile workforce laptops for standard end users
- On-premises datacenter (including servers, network equipment, storage, etc.)
- Legacy OT assets
- Smartphones for the mobile workforce
- On-premises servers for automated software testing
- Containers with customer-facing applications in the public cloud

(3) The IRS must define a maintenance plan for each maintenance group for each applicable risk response scenario. (NIST SP 800-40: Section 3.5)

a. For routine patching, the IRS must consider adopting phased deployments for routine patching in which a small subset of the assets to be patched receive the patch first. (NIST SP 800-40: Section 3.5.1)
b. For routine patching, the IRS must offer flexibility with how soon routine patches are to be installed, while also forcing installation after a grace period has ended. (NIST SP 800-40: Section 3.5.1)
c. For emergency patching, the IRS must consider using the same general approach for emergency patching as for routine patching, except with a highly accelerated schedule. (NIST SP 800-40: Section 3.5.2)
d. For emergency mitigation, the IRS must plan for the quick implementation of multiple types of emergency mitigations to protect vulnerable assets. (NIST SP 800-40: Section 3.5.3)
e. For emergency mitigation, the IRS must plan to replace emergency mitigations with permanent fixes. (NIST SP 800-40: Section 3.5.3)
f. For assets that are not patchable, the IRS must plan to implement multiple types of mitigations, including long-term risk mitigation methods, to protect vulnerable assets. (NIST SP 800-40: Section 3.5.4)
g. For assets that are not patchable, the IRS must plan on periodically re-evaluating alternatives to patching. (NIST SP 800-40: Section 3.5.4)

(4) The IRS must closely track and monitor all exceptions to maintenance plans. (NIST SP 800-40: Section 3.5.5)

(5) The IRS must take software maintenance into consideration when procuring software. (NIST SP 800-40: Section 3.7)

10.8.50.4 (03-11-2024) **Operational Approach**

(1) The Operational approach is detailed through the following steps: (IRS-defined)

- Security patch implementation policy and procedures
- Assign severity levels, preparation of security patch advisories
- Security patch advisory acknowledgment of receipt, and patch processing metrics

The following subsections define the requirements for the patch management process.

10.8.50.4.1 (03-11-2024) **Security Patch Implementation Policy and Procedures**

(1) IRS IT organization or the appropriate information system owner must: (IRS-defined)

a. Document formal security patch implementation change requests in accordance with the Configuration Management process.
b. Implement security patches automatically and/or manually.
c. Implement security patches in a timely manner for all systems and applications within the owner’s control.
d. Identify resources that cannot be patched from a central location.
e. Provide a prioritization scheme for systems and applications (i.e., making a distinction between servers and end-user systems when servers are often of higher priority).
f. Ensure security patches are tested before distribution.
g. Integrate security patch processes with relevant configuration management policies and procedures.
h. Ensure tracking mechanism captures compliance and non-compliance to meet system security requirements and latest patching requirements. Reporting requirements include (but are not limited to) providing information reported during the daily Leadership Review and FISMA metrics.

(2) Security patch management procedures must: (IRS-defined)

a. Implement security patches in accordance with IRS Security Patch Advisories.
b. Identify vulnerabilities and security patches associated with systems and applications not monitored by CSIRC.
c. Provide CSIRC with updates on any additional identified vulnerabilities for further assessment, in accordance with established procedures.

(3) The IRS must reduce patching-related disruptions by implementing the following steps: (NIST SP 800-40: Section 3.1)

a. Striving to decrease the number of vulnerabilities introduced into their environments.
b. Considering deploying applications in ways that make patching less likely to disrupt operations.

10.8.50.4.2
(03-11-2024)
Assign Severity Levels

(1) The information system owner must collaborate with information system security management (ISSM)/ISSO to complete in-depth vulnerability analysis focusing on the precise versions of applications or operating systems affected to validate its applicability to IRS systems environment. (IRS-defined)

Note: Due to the large volume of vulnerabilities that create risks to IRS systems and networks, it is necessary to prioritize vulnerabilities, assigning criticality levels to ensure security patches associated with the vulnerabilities can be installed effectively.

(2) All vulnerabilities must be assigned a criticality ranking based on a specific criteria and formula. Refer to the *"CSIRC Vulnerability Ranking Matrix"* in Exhibit 10.8.50-2 for the criteria and formula. (IRS-defined)

(3) TD P 85-01 requires that agencies test and install security patches on a timeline in accordance with the criticality of the patches.

(4) Refer to Exhibit 10.8.50-3, Security Notifications, for a table of criticality rankings and distribution schedules.

Note: Operational impact of not deploying a patch must be considered using the Risk-Based Decision and Risk Acceptance process.

10.8.50.4.3
(03-11-2024)
Preparation of Security Patch Advisories

(1) The CSIRC must prepare and send out security patch advisories. (IRS-defined)

(2) Security patch advisories must include (as information is available): (IRS-defined)

- A unique identifier
- A unique title
- Which computer or network systems are affected
- Version numbers for all affected software
- A description of the vulnerability and how it might be exploited
- A description of the solution and how it works
- A link to the corrective patch
- A color-coded severity level
- Instructions for what to do if assistance is required

10.8.50.4.4
(03-11-2024)
Security Patch Advisory Acknowledgement of Receipt

(1) Point of Contacts (POCs) receiving an advisory must provide acknowledgment of receipt to the PVG, depending on severity, using the following schedule: (IRS-defined)

Note: This group may be an independent entity, or its duties may be assumed by multiple existing groups (Configuration Control Boards, Steering Committees, etc.)

Color	Priority	Acknowledgement Timeframe
Red	Critical	1 Hour
Orange	High	2 Hours
Yellow	Medium	24 Hours

Color	Priority	Acknowledgement Timeframe
Green	Low	None

10.8.50.4.5
(03-11-2024)
Patch Processing Metrics

(1) Cybersecurity must identify the program metrics that will help manage the strengths and weaknesses, as well as trends in the IRS patch management program and security posture of the Enterprise, and means of delivering these metrics. The IRS must choose actionable enterprise-level patching metrics by implementing the following steps: (NIST SP 800-40: Section 3.6)

a. Taking advantage of low-level metrics that they already collect when developing enterprise-level metrics to capture patching performance.
b. Utilizing their existing low-level metrics to develop enterprise-level metrics that reflect the relative importance of each vulnerability and patch.
c. Frequently updating their low-level metrics and striving for them to be as accurate as possible in order to improve the enterprise-level metrics based on them.

Note: An example of mitigation metrics is to correlate the relative importance of the assets (low, moderate, or high) and the vulnerabilities (low, medium, high, or critical). The metrics for each correlation may reflect the percentage of assets that were patched by the corresponding maintenance plans' deadlines, as well as the average (mean) time and median time for patching.

(2) Cybersecurity must collect metrics data at a minimum, on a monthly basis for the following purposes: (IRS-defined)

- Annual FISMA Reporting
- Quarterly reports for senior leadership
- Treasury Cyber Analysis and Reporting Dashboard (CARD)
- IRS IT organization's internal dashboard
- Ad-hoc reporting

(3) The process and procedures for collecting patch and vulnerability metrics (based on Treasury and NIST guidance) must be defined in standard operating procedures. (IRS-defined)

This Page Intentionally Left Blank

Exhibit 10.8.50-1 (03-11-2024)

Sample IRS CSIRC Security Patch Advisory

IRS CTFC VAC Advisory – 10182023-003-Critical (Red) Oracle Enterprise Manager Vulnerabilities
Cyber Threat Fusion Center (CTFC) / Vulnerability Analysis Cell (VAC)

Brief Description
The CTFC VAC has been made aware of multiple vulnerabilities in Oracle Enterprise Manager, which can be exploited by malicious actors to disclose sensitive information, bypass certain security restrictions, and cause a DoS (Denial of Service)

Severity
These vulnerabilities are rated as critical and can be exploited by remote and local actors.

Solution
Apply update. See vendor reference for details.

Systems Affected

- Linux Enterprise 64-bit (RHEL)(v6.x)
- Linux Enterprise 64-bit (RHEL)(v7.x)
- Linux Enterprise 64-bit (RHEL)(v8.x)
- Linux z Enterprise 64-bit (RHEL)(v7.x)
- Linux z Enterprise 64-bit (RHEL)(v8.x)

Products Affected

- Oracle Enterprise Manager 13.x
- Oracle Enterprise Manager 12.x

CSIRC Distribution

- &&CSIRC-Critical Advisory Distribution
- &&CSIRC-Tier 1 Advisory Distribution
- &&CSIRC-Tier 2 Advisory Distribution
- &&CSIRC-Linux Advisory Distribution

References
CVE-2023-28322, CVE-2023-27533, CVE-2023-28321, CVE-2022-30115, CVE-2022-27781, CVE-2022-27782, CVE-2023-23914, CVE-2022-27780, CVE-2023-28320, CVE-2022-43551, CVE-2023-23915, CVE-2022-42915, CVE-2023-28319, CVE-2023-23916, CVE-2022-23990, CVE-2021-40690

Vendor's Link:
https://www.oracle.com/security-alerts/cpuoct2023.html#AppendixEM

Notes
CTFC VAC does not endorse the application of any referenced patch without the proper testing in its applicable environment. CTFC VAC urges administrators of systems for which a fix is not yet available to routinely check for patch availability.

Exhibit 10.8.50-2 (03-11-2024)

CSIRC Vulnerability Ranking Matrix

The advisory severity rating assigned to each advisory is based on a vulnerability metric calculation derived from the seven questions listed in the CSIRC Vulnerability Ranking Matrix. The seven questions assess the vulnerability based on three key characteristics:

- **Threat -** An activity with the potential of causing harm to a computer system or network.
- **Exposure -** A flaw, misconfiguration, or weakness that allows the violation of security.
- **Severity -** A measure of how important or valuable a system is to the organization's mission.

The formulas for calculating the vulnerability metric and its associated color code are:

- **Threat =** cubed root of ((Q1 x Q2 x Q3)) where Q1, Q2, etc. receive assigned rating values based on the CSIRC Vulnerability Ranking Matrix table that follows.
- **Severity =** square root of ((Q4 x Q5))
- **Exposure =** square root of ((Q6 x Q7))
- **Vulnerability Metric =** Threat * Severity * Exposure

The resulting calculations produce a value ranging from 0 to 1000. See the CSIRC Vulnerability Ranking Matrix to determine the value associated with each question (e.g., Q1, Q2, etc.). Then see the Advisory Security Rating table to establish the rating and color code for an advisory based on the final calculation, Advisory Rating, compared to the rating ranges in the Rating table. In both tables, below, one (1) is lowest and ten (10) is highest.

CSIRC Vulnerability Ranking Matrix

Question	Risk Category	Rating
1. Is the vulnerability widely known?	Only IRS and the vendor know	1
	Only a few individuals are aware of	2
	Workarounds and/or patches are publicly available	3
	General concept of the vulnerability is public	5
	Exploit discussions are on the web	8
	Exploit code is publicly available	10
2. Is exploitation of the vulnerability being reported?	No exploit reports received	1
	Exploit report from a single unofficial non-government source	3
	Exploit reports from multiple unofficial sources	5
	Exploit report from a single trusted security industry source	7
	Exploit reports from multiple trusted security industry sources	9
	Exploit detected internally in the IRS Enterprise	10

Exhibit 10.8.50-2 (Cont. 1) (03-11-2024)
CSIRC Vulnerability Ranking Matrix

CSIRC Vulnerability Ranking Matrix		
Question	**Risk Category**	**Rating**
3. How difficult is it to exploit the vulnerability?	Must convince a System Administrator to take a specific action	1
	Must convince a System User to take a specific action	2
	Need assembler/protocol expertise	3
	Must create a custom IP packet	4
	Attackers can customize a toolkit	5
	Attackers can use plausible-sounding social engineering	6
	Instructions are available as a complex set of commands	7
	Instructions are available as 1-2 simple commands	9
	Publicly available Graphic User Interface (GUI) toolkit	10
4. Is the IRS infrastructure at risk? (If more than one category applies to the vulnerability, select the highest value of valid options)	Vulnerable application not on the IRS network	0
	Obscure application or service in Enterprise vulnerable	2
	Default Linux/UNIX (non-Solaris) configuration vulnerable	3
	Default Solaris configuration vulnerable	5
	Common internal service vulnerable (Web, File Transfer Protocol (FTP), NetBIOS, Tivoli, etc.)	6
	Major internal service vulnerable (DNS, routers, PDC/BDC, Exchange, etc.)	7
	Default Windows configuration vulnerable	8
	COE image configuration vulnerable	9
	Public-access service vulnerable (Web Servers, FTP Servers, Simple Mail Transfer Protocol (SMTP), etc.)	10

Exhibit 10.8.50-2 (Cont. 2) (03-11-2024)
CSIRC Vulnerability Ranking Matrix

CSIRC Vulnerability Ranking Matrix		
Question	**Risk Category**	**Rating**
5. What is the potential impact on the IRS Enterprise if vulnerability is exploited?	Minimal impact	1
	Annoyance to users	2
	Degraded system performance	3
	Temporary denial of service on systems accessed only by internal users	7
	Temporary denial of service on systems accessed by the public	8
	Enterprise-wide downtime required to contain and recover systems	9
	Compromise or destruction of data	10
6. How many systems are vulnerable?	None	0
	1-4	1
	5-19	2
	20-49	4
	50-99	6
	100-199	9
	1000 or more	10
7. What is the access level required to exploit the vulnerability?	Must have privileged access	1
	Another trusted host is required	3
	Local access to a user account is required	5
	Another nearby host is required (i.e., on the same subnet)	7
	None required. Any remote user accessing network services or protocols (e.g., Structured Query Language (SQL), Hypertext Transfer Protocol (HTTP)) that are not vendor default or are not IRS standard	9
	None required. Any remote user accessing network services or protocols (e.g., telnet, NetBIOS) that are vendor default or are IRS standard	10

Advisory Security Rating		
Rating	**Color Code**	**Value Range**
None	None	0

Exhibit 10.8.50-2 (Cont. 3) (03-11-2024)
CSIRC Vulnerability Ranking Matrix

Advisory Security Rating		
Rating	**Color Code**	**Value Range**
Low	Green	1-99
Medium	Yellow	100-199
High	Orange	200-499
Critical	Red	500-1000

Exhibit 10.8.50-3 (03-11-2024)
Security Notifications

As new threats emerge and vulnerabilities are discovered, CSIRC provides security notifications to the enterprise using advisories. These advisories contain one of three levels of warning:

Warning	Description
Alerts	The highest level of warning. Address a major threat or incident information concerning imminent or in-progress attacks targeting specific national networks, critical infrastructures or the IRS enterprise.
Advisories	Address significant threat or incident information that suggests a change in readiness posture, protective options, and/or response.
Bulletins	The lowest level of warning. Address general incidents or issue awareness information and analysis that are significant and current, but that do not necessarily suggest immediate action.

CSIRC employs a **vulnerability metric** to assign a severity rating and distribution schedule to each advisory using the following scale:

Code	Priority	**Remediation Timelines:** *** Remediation begins when a vulnerability is discovered ***
Red	Critical	CISA KEV catalog vulnerabilities – **KEV remediation date** Internet-Accessible systems identified in Cyber Hygiene Reports – **15 days** All other systems - **30 days**
Orange	High	CISA KEV catalog vulnerabilities – **KEV remediation date** Internet-Accessible systems identified in Cyber Hygiene Reports – **30 days** High Value Assets (HVAs) - **60 days** All other systems - **90 days**
Yellow	Medium	CISA KEV catalog vulnerabilities – **KEV remediation date** All other systems - **120 days**
Green	Low	CISA KEV catalog vulnerabilities – **KEV remediation date** All other systems - **180 days**

(CISA BOD-19-02; CISA BOD-22-01; SI-02_N.02; SI-02(2)_T.255; SI-02(2)_T.256; FY2019 FISMA Metrics; IRS-defined)

Note: Operational impact of not deploying a patch must be: (i) considered using Risk Based Decision and Risk Acceptance process; or (ii) documented in a POA&M and the information system's System Security Plan.

Note: CISA provides a catalog, or repository, of KEVs at the web site: *https://cisa.gov/known-exploited-vulnerabilities*.

Note: Refer to IRM 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy*, for vulnerability remediation guidance for off-premise cloud models (Federal Risk and Authorization Management Program (FedRAMP)).

Exhibit 10.8.50-3 (Cont. 1) (03-11-2024)
Security Notifications

Advisory Distribution Mailing Lists:

CSIRC maintains distribution lists for each Advisory category listed below. Please complete the **Subscription Form**, available for download on the CSIRC web site if you wish to join or leave any of the Advisory Distribution Lists.

#

- **&&CSIRC-Tier 1 Advisory Distribution -** Mainframe - The Tier I Infrastructure supports the following main functions: Master File processing (IBM), Collection processing (IBM), IDRS *http://aba.web.irs.gov/abaroadmap/APPL134248291.html*and Campuses support (Unisys), SACS *http://aba.web.irs.gov/abaroadmap/APPL134248723.html* (IBM) and other different tax administration and internal management applications (IBM).
- **&&CSIRC-Tier 2 Advisory Distribution -** Unix/Linux/Windows - The Tier II Infrastructure supports the large array of servers located at the IRS Service Centers (Campuses) and consist of Legacy, Consolidation and Modernization domains.
- **&&CSIRC-Tier 3 Advisory Distribution -** Wintel - The Tier III Infrastructure supports tax process filing, post-filing, compliance and internal management applications consisting of desktops & laptops, office servers (file, print, applications), local peripherals and Enterprise applications.
- **&&CSIRC-Tier 4 Advisory Distribution -** Telecommunications - The Tier IV infrastructure supports the enterprise routing and switching providing for data traversal for applications.
- **&&CSIRC-Linux Advisory Distribution -** LINUX without UNIX
- **&&CSIRC-Web Advisory Distribution -** All the web environments (i.e., Intranet and Internet)
- **&&CSIRC-DB Advisory Distribution -** All databases
- **&&CSIRC-MAC Advisory Distribution -** All MAC operating systems
- **&CSIRC - Cloud Advisory Distribution -** Distribution list for Cloud Services
- **&CSIRC - Development Advisory Distribution -** Distribution list for Development tools users
- **&CSIRC - Vendor Partner Advisory Distribution -** Distribution list for vendor partners
- **&CSIRC - BOD 2201 POC Distribution -** Distribution list for updates and announcements related to CISA BOD 22-01: *Reducing the Significant Risk of Known Exploited Vulnerabilities* (*https://www.cisa.gov/news-events/directives/bod-22-01-reducing-significant-risk-known-exploited-vulnerabilities*) and *Known Exploited Vulnerabilities Catalog* (*https://www.cisa.gov/known-exploited-vulnerabilities-catalog*)

Exhibit 10.8.50-4 (03-11-2024)
Terms and Acronyms

Terms and Acronyms	
Term	**Definition or Description**
ACIO	Associate Chief Information Officer
Advisories	The CSIRC communication for a patch. These advisories include vendor information about their alerts, and their own vendor advisories. For purposes of this IRM, advisories only relate to the CSIRC patch communications.
AO	Authorizing Official
Application	Any data entry, update, query, report, or program that processes data for the user. It includes not only the generic productivity software (spreadsheets, word processors, database programs, etc.) but also custom and packaged programs for payroll, billing, inventory, and other accounting purposes.
BOD	Binding Operational Directive
Breach	The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) an authorized user accesses PII for an other than authorized purpose (i.e., a purpose unrelated to their official duties/functions). (Also, refer to Suspected Breach) (OMB M-17-12) ***Note:*** A breach is a type of incident that involves PII.
CARD	Cyber Analysis and Reporting Dashboard
CCE	Common Configuration Enumeration
CISA	Cybersecurity and Infrastructure Security Agency
CDM	Continuous Diagnostics and Mitigation
CMMI	Capability Maturity Model Integration
CNSI	Classified National Security Information
Compliance	Adherence with governing applicable laws, policies, federal regulations, OMB, TDs, NIST Publications, and NARA.
Compliance Mapping	The process of correlating CCE settings with the security control identifiers. (NISTIR 7511)
CONOPS	Concept of Operations
COTS	Commercial Off-the-shelf, as in software readily available on the market.
CSIRC	IRS Computer Security Incident Response Center
CTFC	Cyber Threat Fusion Center
CTI	Cyber Threat Intelligence

Exhibit 10.8.50-4 (Cont. 1) (03-11-2024)
Terms and Acronyms

Terms and Acronyms	
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
Cyber Event	Any observable occurrence in a network or system that may indicate a cyber incident has occurred. (Also, refer to Notable Cyber Event) (Treasury IRP)
Cyber Hygiene Report	A weekly report by CISA, which operates under DHS. Cyber Hygiene leverages the Common Vulnerability Scoring System (CVSS), which is a vulnerability scoring system designed to provide a universally open and standardized method for rating IT vulnerabilities. CVSS helps organizations prioritize vulnerability management strategies by providing a score representative of the base, temporal, and environmental properties of vulnerabilities. (CISA BOD 19-02)
CyberScope	The system designed to handle manual and automated inputs of agency data for FISMA reporting.
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DNA	Deoxyribonucleic Acid
DNS	Domain Name Server
DoS	Denial of Service
ELC	Enterprise Life Cycle
EA	Enterprise Architecture
EO	Executive Order
EOPS	Enterprise Operations
ESP	Enterprise Standards Profile
Feature	A basic element through which artifacts are compared (NIST)
FedRAMP	Federal Risk and Authorization Management Program
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
FNA	Federal Network Authorization
FTP	File Transfer Protocol

Exhibit 10.8.50-4 (Cont. 2) (03-11-2024)
Terms and Acronyms

Terms and Acronyms	
Functional Impact	A measure of the impact to business functionality or ability to provide services: • No Impact – Event has no impact. • No Impact to Services – Event has no impact to any business or Industrial Control Systems (ICS) services or delivery to entity customers. • Minimal Impact to Non-Critical Services – Some small level of impact to non-critical systems and services. • Minimal Impact to Critical Services – Minimal impact but to a critical system or service, such as email or active directory. • Significant Impact to Non-Critical Services – A non-critical service or system has a significant impact. • Denial of Non-Critical Services – A non-critical system is denied or destroyed. • Significant Impact to Critical Services – A critical system has a significant impact, such as local administrative account compromise. • Denial of Critical Services/Loss of Control – A critical system has been rendered unavailable. (Treasury IRP)
GUI	Graphical User Interface
High Value Asset	Are those assets, federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. HVAs may contain sensitive controls, instructions, data used in critical federal operations, or unique collections of data (by size or content), or support an agency's mission essential functions, making them of specific value to criminal, politically motivated, or states-sponsored actors for either direct exploitation or to cause a loss of confidence in the U.S. Government. (OMB M-17-09)
Host	A computer that acts as a source of information or signals. The term can refer to almost any kind of computer, from a centralized mainframe that is a host to its terminals, to a server that is host to its clients, or to a desktop personal computer (PC) that is host to its peripherals. In network architectures, a client station (user's machine) is also considered a host because it is a source of information to the network in contrast to a device such as a router or switch that directs traffic.
Hotfix	A hotfix is a single, cumulative package that includes one or more files that are used to address a problem in a product. Hotfixes address a specific customer situation and may not be distributed outside the customer organization.
Hotwash	Hotwash is the process of assessing and improving incident response procedures following a major or significant cyber incident.

Exhibit 10.8.50-4 (Cont. 3) (03-11-2024)
Terms and Acronyms

Terms and Acronyms	
HTTP	Hypertext Transfer Protocol
IG	Interim Guidance
Incident	An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. (Also, refer to Major Incident, Significant Cyber Incident, Suspected Incident). (Treasury IRP)
Incident Attributes	- Location of Observed Activity: Where the observed activity was detected in the network. • Level 1 – BUSINESS DEMILITARIZED ZONE – Activity was observed in the business network’s demilitarized zone (DMZ). • Level 2 – BUSINESS NETWORK – Activity was observed in the business or corporate network of the victim. These systems would be corporate user workstations, application servers, and other non-core management systems. • Level 3 – BUSINESS NETWORK MANAGEMENT – Activity was observed in business network management systems such as administrative user workstations, active directory servers, or other trust stores. • Level 4 – CRITICAL SYSTEM DMZ – Activity was observed in the DMZ that exists between the business network and a critical system network. These systems may be internally facing services such as SharePoint sites, financial systems, or relay “jump” boxes into more critical systems. • Level 5 – CRITICAL SYSTEM MANAGEMENT – Activity was observed in high-level critical systems management such as human-machine interfaces (HMIs) in industrial control systems. • Level 6 – CRITICAL SYSTEMS – Activity was observed in the critical systems that operate critical processes, such as programmable logic controllers in industrial control system environments. • Level 7 – SAFETY SYSTEMS – Activity was observed in critical safety systems that ensure the safe operation of an environment. One example of a critical safety system is a fire suppression system. • Unknown – Activity was observed, but the network segment could not be identified. - Actor Characterization: The type of actor(s) involved in the incident (if known). This element is not selected by the reporting entity. - Cross-Sector Dependency - A weighting factor that is determined based on cross-sector analyses conducted by the DHS Office of Critical Infrastructure Analysis (OCIA). - Potential Impact - An estimate of the overall national impact resulting from a total loss of service from the affected entity. This element is not selected by the reporting entity. (Treasury IRP)

Exhibit 10.8.50-4 (Cont. 4) (03-11-2024)
Terms and Acronyms

Terms and Acronyms	
Incident State	• Event Occurred - The event took place. • Event Detected - The event was detected or discovered. This could be something like an alert from a security tool fired, a user submitted a report, a system administrator flagged something suspicious, etc. This is the catalyst event that triggers opening an investigation; however, not all detections will end up becoming investigations. • Event Investigation Opened - Appropriate staff determined the detected event was worth investigating and took action to begin gathering or analyzing information. • Suspected Incident Identified - The investigation reaches a point where (1) the Bureau or TSSSOC has a reasonable suspicion an incident has occurred or (2) the event cannot be easily ruled out as a false positive or other non-incident in a timely fashion and therefore indicates an incident may have occurred or (3) the Bureau has decided to execute a specific remediation action out of an abundance of caution (e.g., reimaging a possibly infected server). • Incident Confirmed - Evidence that confirms that an actual incident or breach has occurred. • Incident Resolved - The mitigation and response actions and required data gathering, such as impact assessments, are complete. (Treasury IRP)
Information Impact	Describes the type of information lost, compromised, or corrupted: • No Impact – No known data impact. • Suspected But Not Identified – A data loss or impact to availability is suspected, but no direct confirmation exists. • Privacy Data Breach – The confidentiality of personally identifiable information (PII) or personal health information (PHI) was compromised. • Proprietary Information Breach – The confidentiality of unclassified proprietary information, such as protected critical infrastructure information (PCII), intellectual property, or trade secrets was compromised. • Destruction of Non-Critical Systems – Destructive techniques, such as master boot record (MBR) overwrite, have been used against a non-critical system. • Critical Systems Data Breach - Data pertaining to a critical system has been exfiltrated. • Core Credential Compromise – Core system credentials (such as domain or enterprise administrative credentials) or credentials for critical systems have been exfiltrated. • Destruction of Critical System – Destructive techniques, such as MBR overwrite; have been used against a critical system. (Treasury IRP)

Exhibit 10.8.50-4 (Cont. 5) (03-11-2024)
Terms and Acronyms

Terms and Acronyms	
Internet-Accessible System	An Internet-Accessible System is any system that is globally accessible over the public internet. It has a publicly routed IP address or a hostname that resolves publicly in DNS to such an address. It doesn't pertain to infrastructure that is internal to a bureau network that enables endpoints to be accessible over the internet, systems reachable from the internet but that require special configuration or access controls (e.g., via a Virtual Private Network), or shared services.
IOC	Indicator of Compromise
IoT	Internet of Things
IP	Internet Protocol
IRM	Internal Revenue Manual
IRP	Incident Response Plan
IRS	Internal Revenue Service
ISSM	Information System Security Management
ISSO	Information Systems Security Officer
IT	Information Technology
ITIL	Information Technology Infrastructure Library
KEV	Known Exploited Vulnerabilities
LSS	Lean Six Sigma
Major Incident	A major incident is either: Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. OR, A breach that involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. An unauthorized modification of, unauthorized deletion of, unauthorized exfiltration of, or unauthorized access to 100,000 or more individuals' PII constitutes a "major incident". (Treasury IRP)
MOU	Memorandum of Understanding
NARA	National Archives and Records Administration
NCATS	National Cybersecurity Assessment and Technical Services
NCCIC	National Communications, Coordination, and Integration Center
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency Report

Exhibit 10.8.50-4 (Cont. 6) (03-11-2024)
Terms and Acronyms

Terms and Acronyms	
Notable Cyber Event	Any deviation from the norm or observable occurrence in a network or system that could have led to a cyber incident but was otherwise mitigated and the source or threat vector poses an ongoing risk to the Department. (Treasury IRP)
NVD	National Vulnerability Database
Observed Activity	• Observed Preparation - Activities undertaken by a threat actor, their leadership and/or sponsor to prepare for conducting malicious cyber activities, e.g., establish governance and articulating intent, objectives, and strategy; identify potential victims and attack vectors; securing resources and develop capabilities; assess intended victim's cyber environment; and define measures for evaluating the success or failure of threat activities. • Observed Engagement - Threat actor activities taken prior to gaining but with the intent to gain unauthorized access to the intended victim's physical or virtual computer or information system(s), network(s), and/or data stores. • Observed Presence - Actions taken by the threat actor once unauthorized access to victim(s)' physical or virtual computer or information system has been achieved that establishes and maintains conditions or allows the threat actor to perform intended actions or operate at will against the host's physical or virtual computer or information system, network and/or data stores. • Observed Effect - Outcomes of threat actor actions on a victim's physical or virtual computer or information system(s), network(s), and/or data stores. • Observed Notable Security Event - Cyber events that do not become incidents but do show adversarial activity especially when unique or advanced tactics were attempted. (Treasury IRP)
OCIA	Office of Critical Infrastructure Analysis
ODNI	Office of the Director of National Intelligence
OMB	Office of Management and Budget
OT	Operational Technology: Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. (NIST SP 800-40)

Exhibit 10.8.50-4 (Cont. 7) (03-11-2024)
Terms and Acronyms

Terms and Acronyms	
Patch	A patch is a small file that when executed will patch or fix specific problems in a target file or application. The benefit of a patch is that it is smaller in size than a full software update, and saves the user from downloading redundant, previously functioning files. The limitation of patching is that the process is often version-specific. In other words, the patch is targeted to work only if the user has a particular version installed. For purposes of this policy, hotfixes, patches, service packs, workarounds and other related corrections and updates to systems and applications will be termed, ″patch(es).″ This policy is only concerned with security-related patches.
PBX	Public Branch Exchanges
PC	Personal Computer
PGLD	Privacy, Governmental Liaison and Disclosure
PII	Personally Identifiable Information - Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (OMB Circular No. A-130)
PMO	Project Management Office
POA&M	Plan of Action and Milestones
POC	Point of Contact
PPD	Presidential Policy Directive
PVG	Patch and Vulnerabilities Group
RBD	Risk-Based Decision
RDP	Remote Desktop Protocol
Recoverability	Scope of resources needed to recover from an incident: • REGULAR – Time to recovery is predictable with existing resources. • SUPPLEMENTED – Time to recovery is predictable with additional resources. • EXTENDED – Time to recovery is unpredictable; additional resources and outside help are needed. • NOT RECOVERABLE – Recovery from the incident is not possible (e.g., sensitive data exfiltrated and posted publicly).
RFC	Request for Change
Risk	A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. (NIST SP 800-53 Rev. 5)

Exhibit 10.8.50-4 (Cont. 8) (03-11-2024)
Terms and Acronyms

Terms and Acronyms	
SA&A	Security Assessment and Authorization
SAAS	Software-as-a-Service
SBU	Sensitive But Unclassified
Service Pack	A Service Pack (more commonly, SP) is a software program that corrects known bugs, problems, or adds new features. Companies that produce large applications (e.g., Microsoft Windows XP®) typically release a service pack when the number of individual patches to the application becomes too large. Service Packs are easier to install than groups of patches, especially with multiple computers that need to be updated over a network.
Shockwave	A multimedia platform for building interactive multimedia applications and video games. Such content can be viewed in a web browser on any computer with the Shockwave Player plug-in installed.
Significant Cyber Incident	A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. (Treasury IRP) ***Note:*** All major incidents are also deemed significant cyber incidents. However, only when a breach of PII that constitutes a "major incident" is the result of a cyber incident will it meet the definition of a "significant cyber incident" and trigger the coordination mechanisms outlined in PPD-41.
SLA	Service-level Agreement
SMTP	Simple Mail Transfer Protocol
SOP	Standard Operating Procedure
Software Product	A version, release, patch level, and other differentiators of a software. (NISTIR 8011 Vol 1)
SP	Special Publication
SQL	Structured Query Language
SSN	Social Security Number
Suspected Incident	An occurrence or alert that is under investigation as a potential incident but has yet to be confirmed. (Treasury IRP)
Suspected Breach	An occurrence or alert that is under investigation as a potential breach but has yet to be confirmed. (Treasury IRP)
System	Refer to host
TD	Treasury Directive

Exhibit 10.8.50-4 (Cont. 9) (03-11-2024)
Terms and Acronyms

Terms and Acronyms	
TD P	Treasury Directive Publication
Threat	Any circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (NIST SP 800-53 Rev. 5)
Threat Actor	A threat actor is a person who conducts malicious cyber activities, e.g., establishes governance and articulates intent, objectives, and strategy; identifies potential victims and attack vectors; secures resources and develops capabilities; assesses intended victim’s cyber environment; and defines measures for evaluating the success or failure of threat activities (Treasury IRP)
TSSSOC	Treasury Shared Service Security Operations Center
TTP	Tactics, Techniques, and Procedures
URL	Uniform Resource Locator is the term for the World Wide Web address that is used in a web browser to navigate to other locations.
UTC	Coordinated Universal Time
VAC	Vulnerability Analysis Cell
VPN	Virtual Private Network
Vulnerability	Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.
WebDAV	Web-based Distributed Authoring and Versioning, WebDAV is a platform-independent extension of HTTP that allows users to collaborate and manage files on Web servers.

Exhibit 10.8.50-5 (03-11-2024)
Related Resources

1. Department of the Treasury
    - TD P 85-01, Version 3.1.2, - *Treasury Information Technology Security Program*, November 3, 2020
    - Department of the Treasury Memorandum, TCIO M 19-03, *Update to Treasury Directive Publication 85-01 Appendix A – System and Information Integrity*
    - *Departmental Incident Response Plan (IRP)*, Rev 4.0, June 2023
2. Internal Revenue Service
    - Document 13347, *Data Breach Response Playbook*
    - Document 13347-A, *IRS Data Breach Response Plan*
    - IRM 10.5.4,*Privacy and Information Protection, Incident Management Program*
    - IRM 10.5.8, *Sensitive But Unclassified (SBU) Data Policy: Protecting SBU in Non-Production Environments*
    - IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*
    - IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*
    - IRM 10.8.24,*Information Technology (IT) Security, Cloud Computing Security Policy*
    - IRM 10.9.1, *Classified National Security Information (CNSI)*
    - IRM 11.3.38,*Disclosure of Official Information, Role and Responsibilities of Disclosure Managers*
3. National Institute of Standards and Technology (NIST)
    - NIST SP 800-40 Rev 4, *Guide to Enterprise Patch Management Technologies*, April 2022
    - NIST SP 800-53 Rev 5.1.1, *Security and Privacy Controls for Federal Information Systems and Organizations*, November 7, 2023
    - NIST SP 800-61 Rev 2,*Computer Security Incident Handling Guide*, August 6, 2012
    - NIST SP 800-70 Rev 4, *National Checklist Program for IT Products-Guidelines for Checklist Users and Developers*, February 15, 2018
    - NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, August 2011 (Updated October 10, 2019)
    - FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 01, 2006
4. Other
    - FY 2019 CIO FISMA Metrics V1, December 2018
    - Public Law 107-347, **E-Government Act of 2002** , December 17, 2002
    - CISA, BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible Systems*, April 29, 2019
    - CISA, BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, November 3, 2021
    - NISTIR 8011, Volume 1, *Automation Support for Security Control Assessments*, June 2017
    - OMB M-17-09, *Management of Federal High Value Assets*
    - OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*
    - Presidential Policy Directive 41 (PPD-41), *United States Cyber Incident Coordination*, July 26, 2016