INFORMATION TECHNOLOGY

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

June 24, 2026

Control #: IT-10-0626-0001
Affected IRM: 10.8.1
Affected IRM: 10.8.50

MEMORANDUM FOR DISTRIBUTION

FROM: Houman Rasouli
Chief Information Security Officer (CISO)
Coordinating Director (CD) for Cybersecurity, Information Technology

Houman Rasouli Digitally signed by Houman Rasouli Date: 2026.06.24 12:10:43 -04'00'

SUBJECT: Updated Vulnerability Remediation, Security Patch Management Requirements, and POA&M Creation

Purpose
The Internal Revenue Service (IRS) Cybersecurity organization has conducted a review of existing vulnerability remediation and Plan of Action and Milestones (POA&M) management requirements defined within IRM 10.8.1 and IRM 10.8.50.

As a result of this review, IRS Cybersecurity is implementing an updated risk-based approach to vulnerability remediation and POA&M management that prioritizes critical vulnerabilities, actively exploited threats, and publicly accessible systems.

This update strengthens the IRS security posture by focusing remediation efforts on vulnerabilities that present the greatest operational and cybersecurity risk while reducing administrative burden associated with lower-risk findings and activities.

All organizations governed by IRM 10.8.1 and IRM 10.8.50 are required to comply with the updated remediation timelines and POA&M requirements established in this memorandum.

This Interim Guidance Memo will be updated/revised as needed to align to Cybersecurity and Infrastructure Security Agency (CISA) BOD 26-04.

Key Outcomes
- Prioritizes remediation of critical vulnerabilities, internet-facing systems, and actively exploited threats
- Aligns remediation timelines with actual vendor patch availability
- Reduces administrative burden associated with low-risk and documentation-related POA&Ms
- Improves operational efficiency, consistency, and accountability for vulnerability remediation activities across IRS systems
- Strengthens enterprise vulnerability management through a threat-informed, risk-based approach

Vulnerability Remediation Requirements

Organizations are required to remediate vulnerabilities within the timelines established in this memorandum based on exploitability, system exposure, operational impact, and risk to IRS operations.

CISA Known Exploited Vulnerabilities (KEV)
Vulnerabilities listed in the Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerabilities (KEV) catalog represent actively exploited threats and must be remediated within the following timelines:

- By the CISA-mandated remediation due date
- If a KEV vulnerability is identified after the mandated due date, remediation must occur within 15 calendar days of discovery

Critical Vulnerabilities
Critical vulnerabilities must be remediated within the following timelines:

- Publicly accessible systems: 15 calendar days
- All other systems: 30 calendar days

High Vulnerabilities
High vulnerabilities must be remediated within the following timelines:

- Publicly accessible systems: 30 calendar days
- High Value Assets (HVAs): 60 calendar days
- FIPS 199 High and Moderate systems: 90 calendar days

Moderate Vulnerabilities
Moderate vulnerabilities affecting FIPS 199 High and Moderate systems must be remediated within 120 calendar days.

Vendor Patch Availability
For vulnerabilities requiring a vendor-issued patch, software update, or corrective fix, remediation timelines begin on the date the vendor makes the corrective action publicly available. This update aligns remediation expectations with operational reality and ensures organizations are measured based on their ability to implement available corrective actions.

POA&M Creation Requirements
POA&Ms are required when vulnerabilities are not remediated within the timelines established in this memorandum.

POA&Ms must be created for the following categories of vulnerabilities:

- Critical or high vulnerabilities identified through vulnerability scanning activities
- High or moderate vulnerabilities identified during FISMA assessment activities
- Vulnerabilities listed in the CISA KEV catalog
- Vulnerabilities identified on publicly accessible systems, including internet-facing web servers, email gateways, VPN infrastructure, and externally accessible services

Low Vulnerability Tracking
Low vulnerabilities identified through vulnerability scans or FISMA assessment activities, including findings associated with administrative or documentation-related updates, will not be entered into the Assessment, Authorization, and Risk Governance (AARG) tool as POA&Ms.

These findings must continue to be reviewed, tracked, and remediated through established continuous monitoring processes by System Owners in coordination with Information System Security Officers (ISSOs). This approach reduces unnecessary administrative overhead while maintaining accountability for remediation activities.

Background
Current POA&M management processes require organizations to track a broad range of vulnerabilities and assessment findings, including low-risk and administrative issues that may present limited cybersecurity risk. Over time, this approach has created significant administrative overhead and reduced the ability to prioritize remediation efforts toward the most critical and actively exploited vulnerabilities.

Additionally, existing remediation timelines often begin when a vulnerability is identified regardless of whether a vendor-issued patch or corrective action is available, creating situations where organizations may be unable to remediate within required timelines.

OMB Circular A-130, Treasury Directive Publication (TDP) 85-01, and IRS cybersecurity policies allow agencies to implement risk-based vulnerability management approaches aligned to operational risk, exploitability, and threat intelligence.

This updated guidance modernizes IRS vulnerability management by prioritizing critical vulnerabilities, internet-facing systems, High Value Assets (HVAs), and actively exploited threats while reducing unnecessary POA&M management overhead and aligning remediation timelines with vendor patch availability.

Roles & Responsibilities
- System Owners and Information System Security Officers (ISSOs): Responsible for ensuring vulnerabilities are remediated within required timelines and that POA&Ms are created when remediation timelines are exceeded.
- Cybersecurity Vulnerability Assessment & Testing Organizations: Responsible for identifying, reporting, and validating vulnerabilities in accordance with IRS vulnerability management processes.

Effective Date
This guidance is effective June 24, 2026, and remains in effect until this Interim Guidance Memo is updated to align to CISA BOD 26-04.

Points of Contact
- Primary: Pam.Eppel@irs.gov
- Secondary: Marcelo.Teixeira@irs.gov

Distribution
- Chief Information Officer (CIO)
- CIO Direct Reports
- System Owners
- System Authorization Branch
- Vulnerability Assessment & Testing Branch
- Cybersecurity Security Program Management Branch