



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.15

MAY 12, 2025

EFFECTIVE DATE

(05-12-2025)

PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.8.15, *Information Technology (IT) Security, General Platform Operating System Security Policy*.

MATERIAL CHANGES

- (1) IRM 10.8.15.1, Program Scope and Objectives:
 - a. Paragraph 1(a): Updated language to clarify when IRM 10.8.1 is to be used as the minimum baseline for a system, which IRM 10.8.15 is subordinate to.
 - b. Paragraph 1(b): Added language to clarify when IRM 10.8.24 is to be used as the minimum baseline for a system, which IRM 10.8.15 is also subordinate to.
- (2) IRM 10.8.15.1(3)(c), Program Scope and Objectives: Added language to indicate that IRM 10.8.15 applies to all NIST impact-level baselines unless a requirement indicates differently.
- (3) IRM 10.8.15.1.3(1), Roles and Responsibilities: Updated language to indicate that security roles must be implemented in accordance with federal law and IT security guidelines.
- (4) IRM 10.8.15.1.5, Program Controls:
 - a. Paragraph (5): Added new paragraph explaining security baseline, risk impact levels, and overlay designators.
 - b. Paragraph (6): Added new paragraph explaining newly implemented requirement citation system for the IRM 10.8 series.
- (5) IRM 10.8.15.1.7(1), Related Resources: Updated language to indicate that the IRM can contain guidance from IRS-defined policy, regulatory and mandated guidance, and policy from other sources beyond the federal guidance cited throughout the IRM.
- (6) IRM 10.8.15.4.1.6(1)(c), AC-10 Concurrent Session Control: Updated requirement to incorporate parameter value from DISA and indicate that the system owner must set limits in the system documentation.
- (7) IRM 10.8.15.4.1.7(1)(b), AC-11: Updated requirement to match text from DISA's General Purpose Operating System SRG text.
- (8) IRM 10.8.15.4.3.1(1), AU-03: Added a note providing clarifying information for audit record content.
- (9) IRM 10.8.15.4.3.2(1), AU-04: Updated requirement to match text from DISA's General Purpose Operating System SRG text.
- (10) IRM 10.8.15.4.3.3(1)(b), AU-05: Updated requirement to match text from DISA's General Purpose Operating System SRG text.
 - a. Paragraph (1)(b): Updated requirement to match text from DISA's General Purpose Operating System SRG text.
 - b. Paragraph (2): Removed by DISA, SRG-OS-000047-GPOS-00023, for being "inappropriate to define at the enterprise level."

- (11) IRM 10.8.15.4.3.6(3)(a), AU-08: Updated requirement to match text from DISA's General Purpose Operating System SRG text.
- (12) IRM 10.8.15.4.3.8, Windows Protection of Audit Information: Removed section as it repeats information from IRM 10.8.1 and is procedural in nature.
- (13) IRM 10.8.15.4.5.4, CM-07:
 - a. Paragraph (1)(b): Updated to refer reader to CSIRC, UNS, and vulnerability assessments when determining which functions, ports, protocols, and/or services should be prohibited or restricted.
 - b. Paragraph (4): New requirement added from the latest DISA General Purpose Operating System SRG.
- (14) IRM 10.8.15.4.5.6, CM-14 Signed Components: New subsection created to accommodate new requirements SRG-OS-000366-GPOS-00153 from the latest DISA General Purpose Operating System SRG.
- (15) IRM 10.8.15.4.7.1(8), IA-02: New requirement added from the latest DISA General Purpose Operating System SRG.
- (16) IRM 10.8.15.4.7.3(1), IA-04: Updated requirement to match text from DISA's General Purpose Operating System SRG text.
- (17) IRM 10.8.15.4.7.4, IA-05:
 - a. Paragraph (2): Added clarifying language that the requirement is for when a password is used.
 - b. Paragraph (3): Added clarifying language that the requirement is for when a password is used.
 - c. Paragraph (5): Added clarifying language that the requirement is for when a password is used. Also, the bullet list was updated to show parameters as defined by the DISA General Purpose Operating System SRG text and IRM 10.8.1 requirements.
 - d. Paragraph (6): Removed alpha list, requirement SRG-OS-000077-GPOS-00045 removed from IRM due to DISA removing it from the General Purpose Operating System SRG, requirement SRG-OS-000383-GPOS-00166 now the sole requirement for this paragraph.
 - e. Paragraph (7): New requirement SRG-OS-000710-GPOS-00160 added from the latest DISA General Purpose Operating System SRG.
 - f. Paragraph (8): New requirement SRG-OS-000720-GPOS-00170 added from the latest DISA General Purpose Operating System SRG.
 - g. Paragraph (9): New requirement SRG-OS-000725-GPOS-00180 added from the latest DISA General Purpose Operating System SRG.
 - h. Paragraph (10): New requirement SRG-OS-000730-GPOS-00190 added from the latest DISA General Purpose Operating System SRG.
- (18) IRM 10.8.15.4.7.7(2), IA-08 Identification and Authentication (Non-Organizational Users): New requirement, SRG-OS-000745-GPOS-00210 added from the latest DISA General Purpose Operating System SRG.
- (19) IRM 10.8.15.4.7.8(2), IA-11 Reauthentication: SRG-OS-000374-GPOS-00159 removed by DISA in the latest General Purpose Operating System SRG.
- (20) IRM 10.8.15.4.9.1, MA-03 Maintenance Tools: New subsection created with requirement SRG-OS-000755-GPOS-00220 added from the latest DISA General Purpose Operating System SRG.
- (21) IRM 10.8.15.4.9.2(2), MA-04 Non-Local Maintenance: Requirement SRG-OS-000126-GPOS-00066 removed by DISA in the latest General Purpose Operating System SRG.
- (22) IRM 10.8.15.4.18.6(1), SC-10 Network Disconnect: Added alpha list for parameters provided by DISA in the General Purpose Operating System SRG.

- (23) IRM 10.8.15.4.18.8, SC-17 Public Key Infrastructure (PKI) Certificates: New subsection created to add new requirement SRG-OS-000775-GPOS-00230 from the latest DISA General Purpose Operating System SRG.
- (24) IRM 10.8.15.4.18.12, SC-45 System Time Synchronization: New subsection created to accommodate NIST SP 800-53 Rev 5 control remapping.
 - a. Paragraph (1): Requirement SRG-OS-000355-GPOS-00143 moved from subsection AU-08
 - b. Paragraph (2): Requirement SRG-OS-000356-GPOS-00144 moved from subsection AU-08
 - c. Paragraph (3): New requirement SRG-OS-000785-GPOS-00250 added from latest DISA General Purpose Operating System SRG.
- (25) IRM 10.8.15.3.19.1, SI-02 Flaw Remediation: IG Memo IT-10-0224-0005, dated April 28, 2024 incorporated.
 - a. Paragraph (1): Requirement SRG-OS-000191-GPOS-00080 removed by DISA in the latest General Purpose Operating System SRG.
 - b. Paragraph (3): Modified requirement to remove naked link to internal URL.
- (26) IRM 10.8.15.4.19.2(3), SI-06 Security and Privacy Function Verification: Updated requirement to match DISA General Purpose Operating System SRG text.
- (27) IRM 10.8.15.4.20, SR-Supply Chain Risk Management: New subsection added to move this NIST control family into it's own subsection. It was erroneously placed under the SI control family subsections.
- (28) Exhibit 10.8.15-1(2)(b), Security Requirements Checklists: Removed "Containerization" from the list of available security requirements checklists. Containerization is covered under IRM 10.8.12.
- (29) Exhibit 10.8.15-2, Terms and Acronyms: Added entry for "FIPS-validated cryptography."
- (30) Exhibit 10.8.15-3, Related Resources: Added entries for FIPS 140-2 and FIPS 140-3 under the "National Institute of Standards and Technology (NIST) Publications" section.
- (31) Exhibit 10.8.15-3, Related Resources: Updated the version of the General Purpose Operating System SRG found under the "Defense Information System Agency (DISA) Publications" section.
- (32) Editorial changes made throughout the IRM for clarity. Reviewed and updated plain language, grammar, titles, website addresses, legal references and IRM references.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes the prior version of IRM 10.8.15 dated October 19, 2023. Additionally, this IRM was updated to incorporate Interim Guidance #IT-10-0224-0005, dated 04-28-2024. This IRM supplements IRM 10.8.1, *Security Policy*, IRM 10.8.2, *Information Technology (IT) Security IT Security Roles and Responsibilities*, and IRM 10.8.24, *Cloud Computing Security Policy*.

AUDIENCE

IRM 10.8.15 must be distributed to all personnel responsible for securing operating systems. This policy applies to all employees, contractors, and vendors of the IRS.

Rajiv Uppal
Chief Information Officer

General Platform Operating System Security Policy

10.8.15.1 Program Scope and Objectives

- 10.8.15.1.1 Background
- 10.8.15.1.2 Authority
- 10.8.15.1.3 Responsibilities
- 10.8.15.1.4 Program Management and Review
- 10.8.15.1.5 Program Controls
- 10.8.15.1.6 Terms and Acronyms
- 10.8.15.1.7 Related Resources
- 10.8.15.2 Risk Acceptance and Risk-Based Decisions
- 10.8.15.3 IT Security Roles and Responsibilities

[illegible]

[illegible]

#

Exhibits

#

- 10.8.15-2 Terms and Acronyms
- 10.8.15-3 Related Resources

10.8.15.1
(05-12-2025)
Program Scope and Objectives

- (1) **Overview:** This IRM lays the foundation to implement and manage security controls and guidance for the use of operating systems within the IRS.
 - a. This IRM is subordinate to IRM 10.8.1, *Security Policy*, and augments the existing requirements identified within IRM 10.8.1, as they relate to IRS operating systems for on-premises systems, including on-premises cloud deployments.
 - b. This IRM is subordinate to IRM 10.8.24, *Cloud Computing Security Policy* and augments the existing requirements identified within IRM 10.8.24, as they relate to IRS operating systems for off-premises cloud deployments.
- (2) **Program Purpose:** Develop and publish security policies to protect the IRS against potential security threats, risks, and vulnerabilities and ensure compliance with federal mandates and legislation.
- (3) **Audience:** The provisions within this IRM apply to:
 - a. All offices and businesses, 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.
 - c. All National Institute of Standards and Technology (NIST) impact-level baselines (i.e., Low, Moderate, High), unless a requirement indicates differently.
- (4) **Policy Owner:** Chief Information Officer (CIO)
- (5) **Program Owner:** Cybersecurity, Cybersecurity Threat Response and Remediation
- (6) **Program Goals:** To protect the confidentiality, integrity, and availability of IRS information and information systems.

10.8.15.1.1
(05-12-2025)
Background

- (1) This IRM defines the security controls for the use of operating systems within the IRS.
- (2) Federal Information Processing Standards (FIPS) 200 mandates the use of NIST Special Publication (SP) 800-53 as an initial set of baseline security controls for the creation of agency IT security policy.
- (3) IRM 10.8.15, *General Platform Operating System Security Policy* provides policy and guidance to be used by the IRS to carry out their representative responsibilities in information systems security regarding workstations and servers.
- (4) IRM 10.8.15 is part of the IRM 10.8 Information Technology (IT) Security series for IRS IT Cybersecurity.

10.8.15.1.2
(05-12-2025)
Authority

- (1) All IRS systems and applications are required to comply with executive orders (EOs), Office of Management and Budget (OMB), Federal Information Security Modernization Act of 2014 (FISMA), NIST, Cybersecurity and Infrastructure Security Agency (CISA), National Archives and Records Administration (NARA), Department of the Treasury, and IRS guidelines as they apply.

10.8.15.1.3
(05-12-2025)
Responsibilities

- (1) The IRS must implement security roles in accordance with federal law and IT security guidelines (e.g., FISMA, NIST, OMB) that are appropriate for their specific operations and missions. The roles and responsibilities are defined in IRM 10.8.2, *IT Security Roles and Responsibilities*.
- (2) Supplemental roles and responsibilities specific to the implementation of operating systems are located in IRM 10.8.15.3, *IT Roles and Responsibilities*.

10.8.15.1.4
(05-12-2025)
Program Management and Review

- (1) The IRS security policy program establishes a framework of controls to ensure the inclusion of security into the IRS IT environment. This framework is provided through the issuance of security policies via the IRM 10.8 series and the development of 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 to:
 - a. Establish and manage an information security program within its organizations. This IRM provides uniform policies and guidance to be used by each organization.
 - b. 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. Protect its information resources and allow the use, access, disposition, and disclosure of information in accordance with applicable laws, policies, federal regulations, OMB guidance, Treasury Directives (TDs), NIST Publications, NARA guidance, other regulatory guidance, and best practice methodologies.
 - d. Use best practices methodologies (such as Capability Maturity Model Integration (CMMI), Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve IRS IT processes and service efficiency and effectiveness.

10.8.15.1.5
(05-12-2025)
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 revision process.
- (3) 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 operating systems.

- (5) To define a security policy baseline for IRS systems, risk impact level and overlay designators may be assigned to a requirement and appear at the end of it in brackets, which will help identify if the requirement applies to a system.

Note: When there are sub-parts (e.g., a, b, i, ii) to a primary requirement and a designator is indicated for the primary requirement but not the sub-parts, the designator indicated for the primary applies to the sub-parts as well.

- a. A FIPS 199 security impact-level designator may be assigned to each requirement. This designator indicates that the requirement only applies to systems categorized at that FIPS 199 impact-level, thus establishing a baseline for each level.

Example: A requirement with an indicator of “H” indicates the requirement only applies to systems categorized as FIPS 199 impact-level HIGH.

- b. Controls designated as program-level controls are identified with an “O” indicator. The following apply for controls designated as program-level requirements:
- i. Implemented at the organization level
 - ii. Not directed at individual systems
 - iii. Independent of any system impact level
 - iv. Not associated with security control baselines

Note: This indicator is in place of the FIPS 199 designators previously defined.

- c. Control identifier as part of the privacy control baseline are identified with a “(P)” indicator.
- d. Controls designated as a critical infrastructure protection (CIP) overlay control are identified with a “CIP” indicator. Systems designated as cyber critical infrastructure assets must implement controls identified as CIP overlay controls.
- i. The critical infrastructure control overlay must be applied to all components within the designated cyber critical infrastructure asset system’s security boundary.

Note: Information systems normally consist of components (servers, routers, batch processing routines, mainframes, etc.) that when combined allow the overall system to perform its intended function. The intent is to increase the trustworthiness and resiliency of the overall system by applying the control overlay to all the components of the designated system, where applicable. It is understood that security controls are applicable only to information system components that provide or support the capability addressed by the controls. Document the implementation accordingly.

Note: CIP overlay controls may be tailored as long as the following criteria is met:

1. The authorizing official (AO), in coordination with the system and organizational officials determines that a control in the overlay is not to be implemented (also referred to as “tailoring-out”) on a designated cyber critical infrastructure asset.
2. The associated documentation for this risk-based decision not to implement must be submitted to the Department Cyber CIP Program Manager and the Departmental Chief Information Security Officer for review and approval.

- e. Controls designated as a high value asset (HVA) overlay control are identified with an “HVA” indicator. Systems designated as an HVA must implement security controls identified as HVA overlay controls.

Note: The PM (Program Management) and PT (Personally Identifiable Information Processing and Transparency) family of controls in the CISA government-wide baseline are excluded from the IRM 10.8.24 baseline.

Note: The HVA control overlay is defined by CISA.

- f. Controls designated as a critical software (CSW) overlay control are identified with a “CSW” indicator. Software designated as critical software and platforms hosting critical software must implement security controls identified as CSW overlay controls. [NIST: NIST Security Measures for EO-Critical Software use]

Note: Security controls identified as CSW align with the security measures defined by NIST.

Note: The following table provides explanations for the applicability of overlay indicators.

<u>Indicator</u>	<u>Applicability</u>
(L)	Applies to systems categorized as FIPS 199 impact-level LOW
(M)	Applies to systems categorized as FIPS 199 impact-level MODERATE
(H)	Applies to systems categorized as FIPS 199 impact-level HIGH
(CIP)	Overlay - Applies to systems identified as Cyber Critical Infrastructure Assets.
(HVA)	Overlay - Applies to systems identified as Cyber High Value Assets
(P)	Privacy Baseline Controls
(O)	Program-level Controls (i.e., Program Management (PM))
(CSW)	Overlay - Applies to software identified as Critical Software and systems hosting critical software

- (6) In an effort to provide an authoritative source for a requirement, a citation may be provided at the end of a requirement within brackets. If a NIST impact level baseline (i.e., L, M, H) or control overlay (i.e., CIP, HVA) applies to a requirement, they would be provided at the end of a requirement within brackets also. The citations, baselines, and overlays are broken down into two parts: the first

part is a generic identifier, such as NIST, DISA, Baseline, Overlay, etc.; the second part identifies the specific source, baseline or overlay that applies. Below are some examples of how a citation, baseline, and/or overlay may appear for a particular type of source:

a. Citations:

Note: The following table provides examples on how various citations would appear in the IRM.

<u>Citation</u>	<u>Example</u>
NIST Control	[NIST: SP 800-53, AC-02]
Treasury Control	[Treasury: TD P 85-01, AC-03_T.002]
Treasury Publication	[Treasury: TD P 15-71]
Federal	[Federal: P.L. 113-283]
U.S. Code	[USC: 44 USC 3551]
Executive Order	[EO: 14028]
OMB Memorandum	[OMB: M-22-09] or [OMB: M-22-09 (III)(D)(5)]
CISA	[CISA: BOD-23-01]
NIST Publication	[NIST: SP 800-40] or [NIST: SP 800-40, Section 3.5]
DISA STIG/SRG	[DISA: SRG-APP-000516-NDM-000350]
IRS Defined	[IRS: IRS-defined] or [CSIRC: IRS-defined]

b. Baseline:

Note: The following table provides an example of how baseline citations are used in the IRM.

<u>Baseline</u>	<u>Example</u>
NIST Baseline	[Baseline: P, L, M, H, O]

c. Overlay

Note: The following table provides an example of control overlays are presented in the IRM.

<u>Overlay</u>	<u>Example</u>
Control Overlay	[Overlay: CIP, HVA, CSW]

Example: How a source, baseline, overlay could appear at the end of a requirement: [NIST: SP 800-53, SA-15 | Baseline: M, H | Overlay: HVA]

Note: Citations correlate to a reference listed in Exhibit 10.8.15-3.

Note: The citation, baseline, and overlay are formatted to be simple enough for manual identification while being distinct enough for automated detection and extraction. This is intended to allow for easy identification and parsing by applications (manual or automated), using distinct patterns.

(7) 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 IRM are more restrictive.

10.8.15.1.6
(10-19-2023)
Terms and Acronyms

(1) Refer to Exhibit 10.8.15-2, Terms and Acronyms, for a list of terms, acronyms, and definitions.

10.8.15.1.7
(05-12-2025)
Related Resources

(1) In addition to the federal guidance cited throughout this IRM, this IRM incorporates IRS-defined policy, regulatory and mandated guidance, and policy from other sources. Refer to Exhibit 10.8.15-3, for a list of related resources and references.

10.8.15.2
(05-12-2025)
Risk Acceptance and Risk-Based Decisions

(1) Any exception to this IRM requires the authorizing official (AO) to make a risk acceptance decision.

#

(3) Refer to IRM 10.8.1 for additional guidance about risk acceptance.

10.8.15.3
(05-12-2025)
IT Security Roles and Responsibilities

(1) This IRM does not contain supplemental roles and responsibilities specific to the implementation of operating systems.

#

#

#

[illegible]

#####

##

#

[illegible]

#

[illegible]

#

##

#

#

#

[illegible]

[illegible]

##

```
# # #
# #
# # # # #
# # #
# # #
# #
# # # # #
# #
# # # # #
# #
# #
# # # # #
# #
```


##

#

[illegible]

Exhibit 10.8.15-2 (05-12-2025)**Terms and Acronyms****A**

Access Control - Process of granting access to information system resources only to authorized users, programs, processes, or other systems.

Active Directory (AD) - A directory service implemented by Microsoft for Windows domain networks. It is included in most Windows Server operating systems and runs as a Windows service. An AD domain controller authenticates and authorizes all users and computers in a Windows domain type network-assigning and enforcing security policies for all computers and installing or updating software.

Assessment, Authorization, and Monitoring - (Formerly known as Security Assessment & Authorization (SA&A)) – Assessment, Authorization, and Monitoring (AA&M) is a testing and evaluation process with a resulting authorization based on the NIST Special Publication 800-series; specifically, SP 800-37 and SP 800-53. The new AA&M process and terminology replaces the Security Assessment & Authorization process, which were based on earlier NIST SP 800 guidance.

Authorizing Official (AO) - Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Accountable for the security risks associated with information system operations. Previously known as the Designated Approving Authority.

Authentication - Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's identity.

B

BEARS - Business Entitlement Access Request System

C

Center for Internet Security (CIS) - A 501c3 nonprofit organization focused on enhancing the cybersecurity readiness and response of public and private sector entities, with a commitment to excellence through collaboration. CIS provides resources that help partners achieve security goals through expert guidance and cost-effective solutions.

Certification - A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of the security authorization process, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Security control assessment is included within the certification process.

Chief Information Officer (CIO)/Chief Technology Officer (CTO) - Refer to IRM 10.8.2 for a detailed description of responsibilities.

Chief Information Security Officer (CISO) - Refer to IRM 10.8.2 for a detailed description of responsibilities.

CIP - Critical infrastructure protection

CSW - Critical software, defined by NIST as any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes: · is designed to run with elevated privilege or manage privileges; · has direct or privileged access to networking or computing resources; · is designed to control access to data or operational technology; · performs a function critical to trust; or, · operates outside of normal trust boundaries with privileged access.

Exhibit 10.8.15-2 (Cont. 1) (05-12-2025)**Terms and Acronyms**

Configuration Management (CM) - A systems engineering process for establishing and maintaining consistency of a product's performance, functional and physical attributes with its requirements, design and operational information throughout its life.

Contingency Planning (CP) - A plan designed to take a possible future event or circumstance into account.

CPU – Central Processing Unit

D

Defense Information Systems Agency (DISA) - A U.S. combat support agency that connects the U.S. military and government through IT and communications support. Originally known as the Defense Communications Agency (DCA).

Denial of Service (DoS) – A cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

Department of Defense (DoD) - The executive department of the government of the United States charged with coordinating and supervising all agencies and functions of the government concerned directly with national security and the United States Armed Forces.

Department of Homeland Security (DHS) - A cabinet department of the United States federal government, with the primary responsibilities of protecting the United States and its territories (including protectorates) from and responding to terrorist attacks, man-made accidents, and natural disasters.

Dual Authorization – In the absence of an automatic process, a rule that requires the approval of two, (dual) authorized individuals to execute a task.

E

EA – Enterprise Architecture

e.g. - for example; used to provide examples and is not an exhaustive or all inclusive list.

ESP – Enterprise Standards Profile

F

FIPS – Federal Information Processing Standards

FIPS-validated Cryptography - A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-3 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP). See NSA-approved cryptography.

Fire Call Account – Local site accounts for emergency or special issues used by Enterprise Operations (EOPs) or other approved organizations.

FISMA – Federal Information Security Management Act

G

GMT - Greenwich Mean Time

Exhibit 10.8.15-2 (Cont. 2) (05-12-2025)**Terms and Acronyms****H**

Host – Any computer that has full two-way access to other computers on the Internet.

Host Server – The physical machine that uses a hypervisor to manage the virtual machine(s).

HTTP - Hypertext Transfer Protocol

HVA - High value asset, as defined by CISA is information or an information system that is so critical to an organization that the loss or corruption of this information or loss of access to the system would have serious impact to the organization's ability to perform its mission or conduct business. These assets, systems, and datasets may contain sensitive controls, instructions or data used in critical operations, or they may house unique collections of data.

Hypervisor – The virtualization component that manages the guest OS on a host and controls the flow of instructions between the guest OS and the physical hardware. Also described as software that allows a single host to run one or more guest operating systems. The hypervisor is basically a high-speed scheduler that issues out the physical resources such as CPU, disk space and RAM to the guest operating systems, (virtual machines). Can be referred to as a virtual machine manager.

I

i.e. - that is, provides exact clarification and typically meant to be an exhaustive list.

Information System Contingency Plan (ISCP) - Established procedures created and maintained by the IRS Information Technology organization and system owners for the assessment and recovery of a system following a system disruption. The ISCP provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system. The ISCP differs from DR plan primarily in that the information system contingency plan procedures are developed for recovery of the system regardless of site or location. An ISCP can be activated at the system's current location or at an alternate site. In contrast, a DR plan is primarily a site-specific plan developed with procedures to move operations of one or more information systems from a damaged or uninhabitable location to a temporary alternate location. Once the DR plan has successfully transferred an information system site would then use its respective ISCO to restore, recover, and test systems, and put them in operation.

Information Technology (IT) – IT is defined as any service, equipment or personnel that support any part of the lifecycle of those services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic:

- Aquisition
- Storage
- Analysis
- Evaluation
- Manipulation
- Management
- Movement
- Control
- Display
- Switching
- Interchange
- Transmission
- Reception of data or information by the agency

Exhibit 10.8.15-2 (Cont. 3) (05-12-2025)

Terms and Acronyms

1. For purposes of this definition, equipment is used by an agency if the equipment is used by the agency directly or issued by a contractor under a contract with the agency that require –
 - a. Its use; or
 - b. To a significant extent, its use in the performance of a service or the furnishing of a product
2. The term “*information technology*” includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services and cloud computing), and related resources.
 - a. Is acquired by a contractor incidental to a contract, or
 - b. Contains embedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment, such as electronic thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, is not information technology.

Information Technology Contingency Plan (ITCP) - Support plans designed to ensure continuity of general support systems and major systems following a disruption.

Internet Protocol (IP) -The principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries.

Internet Protocol Security (IPSec) - A protocol suite for securing Internet Protocol communications by authenticating and encrypting each IP packet of a communication session.

IRM – Internal Revenue Manual

ISSO – See SSO

L

LAN- Local Area Network

N

NARA - National Archives and Records Administration. See IRM 1.15.6 *Managing Electronic Records*, for guidance on implementation of electronic records, management in systems design, development, production, use of storage of official records, and data files, as established by NARA and listed in the Code of Federal Regulations (CFR).

NIST – National Institute of Standards and Technology

NSA – National Security Agency

O

OMB – Office of Management and Budget

OS – Operating System

P

PDS – Protected Distribution System

Exhibit 10.8.15-2 (Cont. 4) (05-12-2025)**Terms and Acronyms**

Permissions – The access controls of a file or directory in the form of read, write, and execute for each of the three groups; file owner, same group member, and everyone else.

PKI – Public Key Infrastructure

R

Risk-Based Decision (RBD) – Decision made by individuals responsible for ensuring security by utilizing a wide variety of information, analysis, assessment, and processes. The type of information taken into account when making a risk-based decision may change based on life cycle phase and decision is made taking entire posture of the system into account. Some examples of information taken into account are formal and informal risk assessments, risk analysis, assessments, recommended risk mitigation strategies, and business impact. (This list is not intended to be all inclusive.)

S

Security Risk Management (SRM) - The management of security risks applies the principles of risk management to the management of security threats. It consists of identifying threats (or risk causes), assessing the effectiveness of existing controls to face those threats, determining the risks' consequence(s), prioritizing the risks by rating the likelihood and impact, classifying the type of risk, and selecting an appropriate risk option or risk response.

Security Technical Implementation Guide (STIG) - A methodology for standardized secure installation and maintenance of computer software and hardware. The term was coined by DISA which creates configuration documents in support of the United States Department of Defense (DoD). The implementation guidelines include recommended administrative processes and span the devices' lifecycle.

Sensitive But Unclassified (SBU) Information - Any information that requires protection due to the risk and magnitude of loss or harm to the IRS or the privacy to which individuals are entitled under 5 U.S.C. 552a (the Privacy Act), which could result from inadvertent or deliberate disclosure, alteration, or destruction.

SP – Special Publication

SRG – Security Requirements Guide

SSO - System Security Officer

Standard Operating Procedure (SOP) – A set of step-by-step instructions compiled by an organization to help workers carry out routine operations. SOPs aim to achieve efficiency, quality output and uniformity of performance, while reducing miscommunication and failure to comply with industry regulations.

System Administrator (SA) – A person who manages the technical aspects of a system. Refer to IRM 10.8.2, *Roles and Responsibilities*, for details.

T

Treasury Directive (TD) - Documents signed by the appropriate senior Treasury officials that: may further delegate authority from the most senior officials to other Treasury officials; and provide processes for implementing legal obligations and Departmental policy objectives.

U

UTC – Universal Time Coordinate

V

Exhibit 10.8.15-2 (Cont. 5) (05-12-2025)

Terms and Acronyms

Virtualization – The simulation of the software and/or hardware upon which other software runs by creating an abstracted layer from the actual hardware creating a unique instance of a physical system, but running independently in software or “virtual” state.

Exhibit 10.8.15-3 (05-12-2025)**Related Resources****IRS Publications**

- IRM 1.16.6, *Managing Electronic Records*
- IRM 2.149.1, *Information Technology (IT) Asset Management*
- IRM 2.150.2, *Configuration Management (CM)*
- IRM 10.8.1, *Information Technology (IT) Security, Security Policy*
- IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*
- IRM 10.8.21, *Information Technology (IT) Security, Database Security Policy*
- IRM 10.8.22, *Information Technology (IT) Security, Web Server Security Policy*
- IRM 10.8.50, *Information Technology (IT) Security, Enterprise Incident, Vulnerability, and Security Patch Management*
- IRM 10.8.60, *Information Technology (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance*
- IRM 10.8.62, *Information Technology (IT) Security, Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Process*
- IRM 10.9.1, *Classified National Security Information (CNSI)*

Department of the Treasury Publications

- TD P 85-01: Treasury Directive Publication 85-01 Version 3.1.3, *"Treasury Information Technology (IT) Security Program,"* issued February 28, 2022.

National Institute of Standards and Technology (NIST) Publications

- FIPS 140-2: Federal Information Processing Standards Publication 140-2, *"Security Requirements for Cryptographic Modules,"* issued May 25, 2001 (Change Notice 2, 12/3/2002).
- FIPS 140-3: Federal Information Processing Standards Publication 140-3, *"Security Requirements for Cryptographic Modules,"* issued March 22, 2019.
- FIPS 199: Federal Information Processing Standards Publication 199, *"Standards for Security Categorization of Federal Information and Information Systems,"* issued February 2004.
- FIPS 200: Federal Information Processing Standards Publication 200, *"Minimum Security Requirements for Federal Information and Information Systems,"* issued March 2006.
- SP 800-37 Rev 2: *"Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,"* issued December 2018.
- SP 800-53: NIST Special Publication 800-53 Revision 5.1.1, *"Security and Privacy Controls for Federal Information Systems and Organizations,"* issued November 7, 2023.

Defense Information Systems Agency (DISA) Publications

- General Purpose Operating System Security Requirements Guide (SRG) V3R2, January 30, 2025.

Public Law

- Federal: PL 113-283: Public Law 113-283, *"Federal Information Security Modernization Act of 2014,"* issued December 18, 2014