



# MANUAL TRANSMITTAL

Department of the Treasury  
Internal Revenue Service

10.8.55

AUGUST 25, 2025

## EFFECTIVE DATE

(08-25-2025)

## PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.8.55, **Information Technology (IT) Security, Network Security Policy**.

## MATERIAL CHANGES

- (1) Signature: Updated the name of the Chief Information Officer.
- (2) IRM 10.8.55.1, Program Scope and Objectives: Added reference to IRM 10.8.24, Cloud Computing Security Policy.
- (3) IRM 10.8.55.1, Program Scope and Objectives: Changed subsection title from Purpose of the Program to Program Purpose.
- (4) IRM 10.8.55.1.1, Background: Removed subsection 10.8.55.1.1.1. Scope and 10.8.55.1.1.2 Objectives.
- (5) IRM 10.8.55.1.3, IT Roles and Responsibilities: Added new subsection title.
- (6) IRM 10.8.55.1.4, Program Management and Review: Updated to align with Security Policy Boiler Plate.
- (7) IRM 10.8.55.1.5, Program Control: Updated to align with IRM 1.11.2 and Security Policy Boiler Plate.
- (8) IRM 10.8.55.1.6, Terms and Acronyms: Exhibit 10.8.55-2 updated with new terms and acronyms.
- (9) IRM 10.8.55.1.7, Related Resources: Exhibit 10.8.55-3 updated with new related resources.
- (10) IRM 10.8.55.3, IT Security Roles and Responsibilities: Added this subsection and moved the roles and responsibilities from IRM 10.8.55.1.3.
- (11) IRM 10.8.55.3.3, Network Security Management Standard: Updated the organizational change for EOps and UNS.
- (12) IRM 10.8.55.4.1.1, AC-02 Account Management: Updated to add the Enterprise Voice, Video, and Messaging (EVVM), and the Network Device Management Security Requirements Guides (SRG) language.
- (13) IRM 10.8.55.4.1.2, AC-03 Access Enforcement: Updated to add EVVM Endpoint, EVVM Session Management, Network Device Management, and the SDN Controller SRGs language.
- (14) IRM 10.8.55.4.1.3, AC-04 Information Flow Enforcement: Updated to add EVVM Endpoint, EVVM Policy, EVVM Session Management, Intrusion Detection and Prevention Systems, SDN Controller, and Virtual Private Network (VPN) SRGs language.
- (15) IRM 10.8.55.4.1.5, AC-07 Unsuccessful Logon Attempts: Updated to add EVVM Session Management SRG.
- (16) IRM 10.8.55.4.1.6, AC-08 System Use Notification: Updated to add EVVM Endpoint, EVVM Session Management, and Virtual Private Network (VPN) SRGs language.

- (17) IRM 10.8.55.4.1.7, AC-09 Previous Logon Notification: Added this new security requirement control subsection and EVVM Endpoint SRG language.
- (18) IRM 10.8.55.4.1.8, AC-10 Concurrent Session Control: EVVM Endpoint, EVVM Session Management, and Virtual Private Network (VPN) SRGs language.
- (19) IRM 10.8.55.4.1.10, AC-12 Session Termination: Updated to add EVVM Endpoint, EVVM Session Management, and Virtual Private Network (VPN) SRGs language.
- (20) IRM 10.8.55.4.1.11, AC-17 Remote Access: Added this new security requirement control subsection and EVVM Endpoint, EVVM Session Manager, SDN Controller, and Virtual Private Network SRGs language.
- (21) IRM 10.8.55.4.1.12, AC-23 Data Mining Protection: Added this new security requirement control subsection and Intrusion Detection and Prevention Systems SRG language.
- (22) IRM 10.8.55.4.3.2, AU-03 Content of Audit Records: Updated to add EVVM Endpoint, EVVM Session Management, Intrusion Detection and Prevention Systems, SDN Controller, and Virtual Private Network (VPN) SRGs language.
- (23) IRM 10.8.55.4.3.3, AU-04 Updated to add EVVM Endpoint, EVVM Session Management, Intrusion Detection and Prevention Systems, Network Device Management, and Virtual Private Network (VPN) SRGs language.
- (24) IRM 10.8.55.4.3.4, AU-05 Response to Audit Logging Process Failures: Updated the subsection title to align with NIST 800-53 Rev 5, added EVVM Session Management, Intrusion Detection and Prevention Systems, and Virtual Private Network (VPN) SRGs language.
- (25) IRM 10.8.55.4.3.5, AU-06 Audit Record Review, Analysis, and Reporting: Added this new security requirement control subsection and Intrusion Detection and Prevention Systems SRG language.
- (26) IRM 10.8.55.4.3.7, AU-09 Protection of Audit Information: Updated to add EVVM Session Management, Intrusion Detection and Prevention Systems, and Virtual Private Network (VPN) SRGs language.
- (27) IRM 10.8.55.4.3.9, AU-12 Audit Record Generation: Updated to add EVVM Endpoint, EVVM Policy, EVVM Session Management, Intrusion Detection and Prevention Systems, and Virtual Private Network (VPN) SRGs language.
- (28) IRM 10.8.55.4.5.1, CM-05 Access Restrictions for Change: Updated to add SDN Controller SRG language.
- (29) IRM 10.8.55.4.5.2, CM-06 Configuration Settings: Updated to add EVVM Endpoint, EVVM Session Management, Intrusion Detection and Prevention Systems, SDN Controller, and Virtual Private Network (VPN) SRGs language.
- (30) IRM 10.8.55.4.5.3, CM-07 Least Functionality: Updated to add EVVM Endpoint, EVVM Session Management, Intrusion Detection and Prevention Systems, SDN Controller, and Virtual Private Network (VPN) SRGs language.
- (31) IRM 10.8.55.4.5.4, CM -11 User-Installed Software: Updated to add SDN Controller SRG language.
- (32) IRM 10.8.55.4.5.5, CM -14 Signed Components: Updated to add Network Device Management SRG language.
- (33) IRM 10.8.55.4.6, CP - Contingency Planning: Updated to align with the Security Policy boilerplate.

- 
- (34) IRM 10.8.55.4.6.1 CP-07 Alternate Processing Site: Added this new security requirement control subsection and EVVM Policy SRG language.
  - (35) IRM 10.8.55.4.6.1 CP-09 System Backup: Updated to add Network Device Management SRG language.
  - (36) IRM 10.8.55.4.7.1, IA-02 Identification and Authentication (Organizational Users): Updated to add EVVM Endpoint, EVVM Session Management, Network Device Management, and Virtual Private Network (VPN) SRGs language.
  - (37) IRM 10.8.55.4.7.2, IA-03 Device Identification and Authentication: Updated to add EVVM Session Management and Virtual Private Network (VPN) SRGs language.
  - (38) IRM 10.8.55.4.7.3, IA-05 Authenticator Management: Updated to add EVVM Endpoint, EVVM Session Management, Network Device Management, and Virtual Private Network (VPN) SRGs language.
  - (39) IRM 10.8.55.4.7.5, IA-07 Cryptographic Module Authentication: Updated to add SDN Controller and Virtual Private Network (VPN) SRGs language.
  - (40) IRM 10.8.55.5.7.6, IA-08 Identification and Authorization (Non-Organizational Users): Added this new security requirement control subsection and Virtual Private Network (VPN) SRG language.
  - (41) IRM 10.8.55.5.7.7, IA-11 Re-Authentication: Added this new security requirement control subsection; and added EVVM Session Management and Virtual Private Network (VPN) SRGs language.
  - (42) IRM 10.8.55.5.9.1, MA-03 Maintenance Tools: Added this new security requirement control subsection and Network Device Management SRG language.
  - (43) IRM 10.8.55.5.9.2, MA-04 Nonlocal Maintenance: Updated to add Network Device Management SRG language.
  - (44) IRM 10.8.55.4.13, PM - Program Management: Added this new security requirement control subsection.
  - (45) IRM 10.8.55.4.13.1, PM-1 Information Security Program Plan: Added this new security requirement control subsection and EVVM Policy SRG language.
  - (46) IRM 10.8.55.4.18.2, SC-02 Separation of System and User Functionality: Added this new security requirement control subsection and SDN Controller SRG language.
  - (47) IRM 10.8.55.4.18.3, SC-03 Security Function Isolation: Added this new security requirement control subsection and SDN Controller SRG language.
  - (48) IRM 10.8.55.4.18.4, SC-05 Denial-of-Service Protection: Updated to add EVVM Session Management, Intrusion Detection and Prevention Systems, Layer 2 Switch, Router, and SDN Controller SRGs language.
  - (49) IRM 10.8.55.4.18.5, SC-07 Boundary Protection: Updated to add Intrusion Detection and Prevention Systems, Layer 2 Switch, Router, SDN Controller, and Virtual Private Network (VPN) SRGs language.
  - (50) IRM 10.8.55.4.18.6, SC-08 Transmission Confidentiality and Integrity: Added this new security requirement control subsection and EVVM Endpoint, EVVM Session Manager, and Virtual Private Network SRGs language.
  - (51) IRM 10.8.55.4.18.7, SC-10 Network Disconnect: Updated to add EVVM Endpoint, EVVM Session Management, and Virtual Private Network (VPN) SRGs language.

- (52) IRM 10.8.55.4.18.8, SC-13 Cryptographic Protection: Updated to add EVVM Endpoint, EVVM Session Management, and Virtual Private Network (VPN) SRGs language.
- (53) IRM 10.8.55.4.18.9, SC-15 Collaborative Computing Devices and Applications: Added this new security requirement control subsection and EVVM Endpoint SRG language.
- (54) IRM 10.8.55.4.18.10, SC-17 Public Key Infrastructure Certificates: Added this new security requirement control subsection and Network Device Management SRG language.
- (55) IRM 10.8.55.4.18.11, SC-18 Mobile Code: Added this new security requirement control subsection; and added EVVM Endpoint, EVVM Session Management, Network Device Management, Router, and Virtual Private Network SRGs language.
- (56) IRM 10.8.55.4.18.12, SC-23 Session Authenticity: Updated to add EVVM Endpoint, EVVM Session Management, Router, and Virtual Private Network (VPN) SRGs language.
- (57) IRM 10.8.55.4.18.13, SC-24 Fail in Known State: Updated to add EVVM Endpoint, EVVM Session Management, Intrusion Detection and Prevention Systems, SDN Controller, and Virtual Private Network (VPN) SRGs language.
- (58) IRM 10.8.55.4.18.14, SC-28 Protection of Information at Rest: Updated to add Network Device Management SRG language.
- (59) IRM 10.8.55.4.18.15, SC-45 System Time Synchronization: Added this new security requirement control subsection and Network Device Management SRG language.
- (60) IRM 10.8.55.4.18.16, SC-47 Alternate Communications Paths: Added this new security requirement control subsection; and added Intrusion Detection and Prevention Systems, Layer 2 Switch, Router, SDN Controller, and Virtual Private Network (VPN) SRGs language.
- (61) IRM 10.8.55.4.19.1, SI-02 Flaw Remediation: Updated to add Network Device Management SRG language.
- (62) IRM 10.8.55.4.19.2, SI-03 Malicious Code Protection: Added this new security requirement control subsection and Intrusion Detection and Prevention Systems SRG language.
- (63) IRM 10.8.55.4.19.3, SI-04 System Monitoring: Added this new security requirement control subsection and Intrusion Detection and Prevention Systems SRG language.
- (64) IRM 10.8.55.4.19.4, SI-05 Security Alerts, Advisories, and Directives: Added this new security requirement control subsection and SDN Controller SRG language.
- (65) IRM 10.8.55.4.19.5, SI-10 Information Input Validation: Added this new security requirement control subsection and Intrusion Detection and Prevention Systems SRG language.
- (66) IRM 10.8.55.4.19.6, SI-11 Error Handling: Added this new security requirement control subsection; and EVVM Session Manager, Intrusion Detection and Prevention Systems, and SDN Controller SRGs language.
- (67) Exhibit 10-8-55-1, Security Requirements Checklists: Updated with the language removed from 10.8.55.1.1.1.
- (68) Throughout: Made editorial changes to clarify, reorganize and remove duplicate content. Incorporated plain language and updated grammar, titles, website addresses and references.

#### **EFFECT ON OTHER DOCUMENTS**

IRM 10.8.55 dated November 03, 2023 is superseded. Additionally, this IRM supplements IRM 10.8.1, **Security Policy**, IRM 10.8.24, **Cloud Computing Security Policy**, and IRM 10.8.54, **Minimum Firewall Administration Requirements**.

#### **AUDIENCE**

IRM 10.8.55 must be distributed to all personnel responsible for ensuring that adequate security is provided for IRS information and information systems. This policy applies to all employees, contractors, and vendors of the IRS.

Kaschit Pandya  
Acting, Chief Information Officer



# Network Security Policy

#### 10.8.55.1 Program Scope and Objectives

#### 10.8.55.1.2 Authority

#### 10.8.55.1.4 Program Management and Review

#### 10.8.55.1.6 Terms and Acronyms

#### 10.8.55.2 Risk Acceptance and Risk-Based Decisions

[illegible]

[illegible]



# # # # # # # # # #

## #

- Cat. No. 66020C (08-25-2025)  
Any line marked with a #  
is for **Official Use Only**



10.8.55.1  
(08-25-2025)  
**Program Scope and  
Objectives**

- (1) **Overview:** This IRM lays the foundation to implement and manage security controls and guidance for the use of network devices within the Internal Revenue Service (IRS).
  - a. This IRM is subordinate to IRM 10.8.1, **Security Policy**, and augments the existing requirements identified within IRM 10.8.1, **Security Policy**, as they relate to IRS network security for on-premise systems, including on-premise 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, **Cloud Computing Security Policy**, as they relate to IRS network devices for off-premise cloud deployments.
- (2) **Program Purpose:** Develop and publish security policies to protect the IRS IT infrastructure against potential security threats, risks and vulnerabilities to ensure compliance with federal mandates and legislation.
- (3) **Audience:** The provisions in this IRM 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 information systems that store, process, or transmit IRS information or connect to an IRS network or system.
- (4) **Policy Owner:** Chief Information Officer (CIO)
- (5) **Program Owner:** Cyber security, Cyber security Threat Response and Remediation
- (6) **Program Goals:** To protect the confidentiality, integrity, and availability of IRS information and information systems.

10.8.55.1.1  
(08-25-2025)  
**Background**

- (1) This IRM establishes a comprehensive policy to implement the minimum security controls to safeguard network devices within the IRS organization.
- (2) IRM 10.8.55 is part of the IRM Part 10.8 series for IRS IT Cyber security.

10.8.55.1.2  
(08-25-2025)  
**Authority**

- (1) All IRS information 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), National Institute of Standards and Technology (NIST), Cyber security and Infrastructure Security Agency (CISA), National Archives and Records Administration (NARA), the Department of the Treasury, and IRS guidelines as they apply.

10.8.55.1.3  
(08-25-2025)  
**Roles and  
Responsibilities**

- (1) The IRS must implement security roles in accordance with federal laws 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) The supplemental roles and responsibilities specific to the implementation of network devices located in IRM 10.8.55.3, IT Roles and Responsibilities subsection of this IRM.

10.8.55.1.4  
(08-25-2025)

**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 requirements checklists. Stakeholders are notified when revisions to the security policies and security requirements 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 practice methodologies (such as Capability Maturity Model Integration (CMMI), Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve the IRS IT process and service efficiency and effectiveness.

10.8.55.1.5  
(08-25-2025)

**Program Controls**

- (1) Each IRM in the 10.8 series is assigned an author who reviews the IRM annually 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 requirements 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) 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 network devices.
- (5) In the event there is a discrepancy between this IRM and IRM 10.8.1, IRM 10.8.1 has precedence, unless the security controls/requirements in this IRM are more restrictive.

10.8.55.1.6  
(08-25-2025)

**Terms and Acronyms**

- (1) Refer to Exhibit 10.8.55-2, Terms and Acronyms, for a list of terms, acronyms, and definitions.

10.8.55.1.7  
(08-25-2025)

**Related Resources**

- (1) In addition to federal guidance cited throughout this IRM, this IRM incorporates IRS-defined policy, regulatory and mandated guidance, and policy from other sources. Refer to Exhibit 10.8.55-3, Related Resources, for a list of related resources and references.

10.8.55.2  
(08-25-2025)

**Risk Acceptance and  
Risk-Based Decisions**

- (1) Any exception to this IRM requires the authorizing official (AO) to make a risk acceptance decision.
- (2) Users must submit risk-based decision (RBD) requests in accordance with Cybersecurity's Security Risk Management (SRM) Risk Acceptance Process within the Risk-Based Decision Standard Operating Procedures (SOP).

- (3) Refer to IRM 10.8.1, **Security Policy** for additional guidance on risk acceptance and RBD.

#  
#

#  
#  
#  
#

#  
#  
#  
#  
#  
#  
#

#  
#  
#

#  
#  
#  
#  
#  
#

10.8.55.4  
(08-25-2025)

**IT Security Controls**

- (1) The security controls within this IRM supplement the requirements found in IRM 10.8.1, **Security Policy** or IRM 10.8.24, **Cloud Computing Security Policy** (as applicable).
  - a. Refer to IRM 10.8.1, **Security Policy** or IRM 10.8.24, **Cloud Computing Security Policy** (as applicable) for security control families not addressed within this IRM.
- (2) It is acceptable to configure settings to be more restrictive than those defined in this IRM.

- #####

[illegible]

#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#



[illegible]

#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#

[illegible]

[illegible]

#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
  
  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#

[illegible]

#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
  
  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#

#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#



#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#

[illegible]

#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#

#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#

[illegible]

[illegible]

#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
  
  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#

[illegible]



[illegible]

#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#

#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
  
#  
#  
  
#  
#

[illegible]

#  
#  
#  
  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#

#  
#  
#  
#  
  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#

##  
##  
##  
  
##  
##  
  
##  
##  
  
##  
##  
##  
##  
  
##  
##  
  
##  
##  
##  
  
##  
##  
##  
  
##  
##  
##  
  
##  
##  
##  
  
##  
##  
##

[illegible]



[illegible]

[illegible]

#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#

#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#

#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#

#####

#  
#  
#  
  
#  
#  
#  
  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#

#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
#  
  
#  
#  
  
#  
#



#  
#  
#

#  
#  
#  
#

#  
#  
#

#  
#  
#  
#

#  
#  
#

#  
#  
#  
#

#  
#  
#

#  
#  
#  
#

#  
#  
#

#  
#  
#

#  
#  
#  
#

#  
#  
#

#  
#  
#

#  
#  
#  
#

[illegible]

**#**

#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#

##  
##  
##  
  
##  
##  
##  
  
##  
##  
##  
  
##  
##  
  
##  
##  
##  
  
##  
##  
  
##  
##  
##  
  
##  
##  
##  
  
##  
##  
##  
  
##  
##  
##

#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#

##  
##  
##  
  
##  
##  
##  
##  
##  
##  
  
##  
##  
##  
##  
##  
##  
  
##  
##  
##  
  
##  
##  
##  
  
##  
##  
##  
  
##  
##  
##  
  
##  
##  
##

#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
  
#  
#  
  
#  
#



[illegible]

##  
##  
##  
  
##  
##  
  
##  
##  
##  
##  
##  
##  
##  
##  
  
##  
##  
##  
  
##  
##  
##  
##  
  
##  
##  
##  
##  
  
##  
##  
##  
##

#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#

##  
##  
##  
##  
##  
##  
##  
  
##  
##  
##  
##  
  
##  
##  
##  
##  
##  
##  
##  
  
##  
##  
##  
##  
  
##  
##  
##  
##  
##  
##  
##  
  
##  
##  
##  
##

[illegible]

#  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#

#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
  
#

#



[illegible]

#  
#  
#  
  
#  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#  
#  
  
#  
#  
#  
  
#  
#  
#

#  
#  
#  
#

**This Page Intentionally Left Blank**

[illegible]

[illegible]

**Exhibit 10.8.55-2 (08-25-2025)****Terms and Acronyms****A**

**AC** - Access Control (NIST security and privacy control family title)

**Access Control** - The process of granting or denying specific requests:

1) For obtaining and using information and related information processing services.

2) To enter specific physical facilities (e.g., federal buildings, military establishments, and border crossing entrances).

**AES** - Advanced Encryption Standard

**ALI** - Automatic Location Identification

**ANI** - Automatic Number Identification

**API** - Application Program Interface

**ARP** - Address Resolution Protocol

**AR** - Aggregation Router

**AS** - Autonomous System

**Asset** - A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

**ASM** - Any Source Multicast

**AS-SIP** - Assured Services Session Initiation Protocol

**AT** - Awareness and Training (NIST security and privacy control family title)

**AU** - Audit and Accountability (NIST security and privacy control family title)

**Audit** - An independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and procedures, and to recommend necessary changes in controls, policies, or procedures.

**Audit Trail** - A chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of each event in a transaction from inception to output of final results.

**Authentication** - The act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information. Typically, a measure designed to protect against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator. The process of identifying an individual is usually based on a username and password, but can also be done through other means, such as tokens, access cards, and biometrics. Authentication ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

**Authenticator** - The means used to confirm the identity of a user, processor, or device (e.g., user password, token, PKI certificate, biometric, or key card).

**Exhibit 10.8.55-2 (Cont. 1) (08-25-2025)****Terms and Acronyms**

**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 aAuthority.

**Authorized User** Any appropriately cleared individual with a requirement to access an IRS information system in order to perform or assist in a lawful and authorized governmental function.

**A/V** - Audio/Visual

**Availability** - The ability to access information system resources in a timely manner as required by an authorized user; one of the fundamental components of information security.

**Awareness** - Activities which seek to focus attention on information security or set of issues. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. Awareness relies on reaching broad audiences with attractive packaging techniques.

**B**

**BGP** - Border Gateway Protocol

**Bogon/Martian** - A bogon route or martian address is a type of packet that should never be routed inbound through the perimeter device. Bogon routes and martian addresses are commonly found as the source addresses of DDoS attacks. By not having a policy implemented to keep these addresses up to date, the network will run the risk of allowing illegitimate traffic into the network or even blocking legitimate traffic. Also, if there are rulesets with "any" as the source address then bogons/martians must be applied.

**Bridge Protocol Data Unit (BPDU)** – Frames that contain information about the spanning tree protocol. A switch sends BPDUs using a unique source MAC address from its origin port to a multicast address with destination MAC.

**BU** - Business Unit

**C**

**C2** - Command and control

**CA** - Assessment, Authorization, and Monitoring (NIST security and privacy control family title)

**CAC** - Common Access Card

**CAS** - Channel Associated Signaling

**CCMP** - Counter Mode with Cipher Block Chaining Message Authentication Protocol

**CD** - Compact Disc

**CE** - Customer Edge

**CER** - Customer Edge Router

**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 certification.



**Exhibit 10.8.55-2 (Cont. 2) (08-25-2025)****Terms and Acronyms**

**Channel Service Unit/Data Service Unit (CSU/DSU)** - A hardware device about the size of an external modem that converts a digital data frame from the communications technology used on a LAN into a frame appropriate to a WAN and vice versa.

**CIA** - Confidentiality, Integrity, and Availability

**CIO** - Chief Information Officer

**CIS** - Center for Internet Security

**CISA** - Cyber security and Infrastructure Security Agency

**CISO** - Chief Information Security Officer

**Client Agent** - Configures how often client computers retrieve the policy that gives them their basic configuration settings. For example, after you configure the other client agent settings, Configuration Manager puts those settings into policy and sends them to the management point, and client computers poll for them on the schedule that you configure. This agent also controls settings that are common to several Configuration Manager features, for example, how often users are prompted with reminders about client operations and what customized organization names users see with the reminders

**COOP** - Continuity of Operations

**CM** - Configuration Management (NIST security and privacy control family title)

**CMMI** - Capability Maturity Model Integration

**CNSI** - Classified National Security Information

**CNSSAM** - Committee on National Security Systems Advisory Memorandum

**Configuration Control** - Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against unauthorized or improper modifications prior to, during, and after system implementation.

**Continuous Monitoring** - Per NIST SP 800-137, continuous monitoring is maintaining an ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. The objective is to conduct ongoing monitoring of the security of an organization's networks, information, and systems, and respond by accepting, avoiding/rejecting, transferring/sharing, or mitigating risk as situations change.

**CP** - Contingency Planning (NIST security and privacy control family title)

**CRL** - Certificate Revocation List

**Cryptography** - The discipline that embodies the principles, means, and methods for the transformation of data in order to hide semantic content, prevent unauthorized use, or prevent undetected modification.

**CSfC** - Commercial Solution for Classified

**CSIRC** - Computer Security Incident Response Center

**CSW** - Critical Software

**CSU** - Channel Service Unit

**CTI** - Computer Telephony Integration

**Exhibit 10.8.55-2 (Cont. 3) (08-25-2025)****Terms and Acronyms****D**

**DAI** - Dynamic ARP Inspection

**DDoS** - Distributed Denial-of-Service

**Denial-of-Service (DoS)** - Action(s) that strive to make a computer resource unavailable to authorized users, generally consisting of the concerted efforts of a person or persons to prevent an information resource from functioning efficiently or at all, temporarily or indefinitely.

**Deep Packet Inspection** - An inspection engine that analyzes data at the application layer, typically layers 5 through 7 of the open systems interconnection (OSI) model.

**Demilitarized Zone (DMZ)** - An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied. A host or network segment inserted as a "neutral zone" between an organization's private network and the internet. perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

**Designated Router (DR)** – Router selected to receive other router's link-state advertisements. Each multi-access network has a DR, which performs two main functions; originate network link advertisements on behalf of the network and establish adjacencies with all routing devices on the network, thus participating in the synchronizing of the link-state databases.

**DH** - Diffie-Hellman

**DISA** - Defense Information Systems Agency

**DNS** - Domain Name System

**DO** - Departmental Offices

**DR** - Designated Router

**DRBG** - Deterministic Random Bit Generators

**DSU** - Data Service Unit

**Dynamic Host Configuration Protocol (DHCP)** - A protocol used by network devices (clients) to obtain various parameters necessary for the clients to operate in an Internet Protocol (IP) network. By using this protocol, system administration workload greatly decreases, and devices can be added to the network with minimal or no manual configurations.

**DVD** - Digital Video Disc

**E**

**EA** - Enterprise Architecture

**EAP** - Extensible Authentication Protocol

**Encryption** - The reversible transformation of data from the original (the plaintext) to a difficult-to-interpret format (the ciphertext) as a mechanism for protecting its confidentiality, integrity and sometimes its authenticity. Encryption uses an encryption algorithm and one or more encryption keys.

**Exhibit 10.8.55-2 (Cont. 4) (08-25-2025)****Terms and Acronyms**

**EO** - Executive Order

**EOps** - Enterprise Operations

**ESC** - Enterprise Session Controller

**ESP** - Enterprise Standards Profile

**EVVM** - Enterprise Voice, Video, and Messaging

**F**

**Federal Information Processing Standard (FIPS)** - A standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability.

**Federal Information Security Modernization Act (FISMA)** - Title III of the E-Government Act requiring each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Annual security reviews of programs and systems are to be conducted and the results reported to the Office of Management and Budget (OMB).

**FES** - Fire and Emergency Services

**FOD** - Functional Operating Divisions

**FTP** - File Transfer Protocol

**G**

**GMT** - Greenwich Mean Time

**Group Master Key (GMK)** - An auxiliary key that may be used to derive a group temporal key.

**GSP** - Guideline, Standard and Procedure

**GTSM** - Generalized TTL (Time-to-Live) Security Mechanism

**H**

**HIGH Impact System** - An information system in which at least one security objective (e.g., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of HIGH.

**HMAC-SHA-1** - Keyed-Hash Message Authentication Code Secure Hash Algorithm 1

**HTTP** - Hypertext Transfer Protocol

**HTTPS** - Hypertext Transfer Protocol Secure

**HVA** - High Value Asset

**I**

**IA** - Identification and Authentication (NIST security and privacy control family title)

**Exhibit 10.8.55-2 (Cont. 5) (08-25-2025)****Terms and Acronyms**

**iBGP** - Internal Border Gateway Protocol

**ICMP** - Internet Control Message Protocol

**ID** - Identification

**IEEE** - Institute of Electrical and Electronics Engineers

**IEEE 802.11** - A family of IEEE standards that extend the common wired Ethernet local network standard into the wireless domain using the 5 GHz and 2.4 GHz public spectrum bands. It specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. It is commonly referred to as “Wi-Fi” because the “Wi-Fi Alliance” provides certification for 802.11 products.

**IG** - Interim Guidance

**IKE** - Internet Key Exchange

**Information at Rest** - Data in computer storage (e.g., on hard disk drives, CDs/DVDs, floppy disks, thumb drives, personal digital assistants (PDAs), cellphones, other removable storage media, etc.) while excluding data that is traversing in a network (data in transit) or temporarily residing in computer memory to be read or updated (data in use).

**Information Security** - The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide CIA.

**Information System** - A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

**Interior Gateway Protocol (IGP)** - A type of protocol used in exchanging routing information between gateways (commonly routers) within an autonomous system (for example, a system of corporate local area networks). This routing information can then be used to router network-layer protocols like IP.

**Intermediate Distribution Frame (IDF)** - A distribution frame that cross-connects the user cable media to individual line circuits and may serve as a distribution point for multipair cables from the main distribution frame or combined distribution frame to individual cables connected to equipment in areas remote from these frames.

**Internet Group Management Protocol (IGMP)** - A communication protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships.

**Intrusion Detection System (IDS)** - Software and/or hardware designed to detect unwanted attempts to access, manipulate, and/or disable computer systems, mainly through a network, such as the Internet.

**Intrusion Detection and Prevention System (IDPS)** - Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

**IP** - Internet Protocol

**Intrusion Prevention System (IPS)** - System(s) which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

**IPSec** - Internet Protocol Security

**IPv4/IPv6** - Internet Protocol Version 4/6

**Exhibit 10.8.55-2 (Cont. 6) (08-25-2025)****Terms and Acronyms**

**IR** - Incident Response (NIST security control family title)

**IRM** - Internal Revenue Manual

**IRS** - Internal Revenue Service

**ISSO** - Information System Security Officer

**ISSM** - Information System Security Manager

**IT** - Information Technology

**ITIL** - Information Technology Infrastructure Library

**ITSP** - Internet Telephony Service Provider

**K**

**KDF** - Key Derivation Function

**Key Management** - The activities involving the handling of cryptographic keys and other related security parameters during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.

**Keyed-Hash Message Authentication Code (HMAC)** - A specific type of message authentication code involving a cryptographic hash function and a secret cryptographic key. It may be used to simultaneously verify both the data integrity and the authentication of a message.

**L**

**L2F** - Layer 2 forwarding

**L2TP** - Layer 2 Tunneling Protocol

**L2VPN** - Layer 2 Virtual Private Network

**L3VPN** - Layer 3 Virtual Private Network

**Label Distribution Protocol (LDP)** - A protocol in which routers capable of MPLS exchange label mapping information. Two routers with an established session are called LDP peers and the exchange of information is bi-directional.

**LAN** - Local Area Network

**LDAP** - Lightweight Directory Access Protocol

**Least Privilege** - The security principle that requires each subject to be granted the most restrictive set of privileges necessary to carry out their assigned duties and functions.

**LLDP** - Link Layer Discovery Protocols

**LSC** - Local Session Controller

**LSS** - Lean Six Sigma (LSS))

**M**

**MA** - Maintenance (NIST security control family title)

**Exhibit 10.8.55-2 (Cont. 7) (08-25-2025)****Terms and Acronyms**

**MAB** - MAC Authentication Bypass

**MAC Address** - Media Access Control Address

**MFSS** - Multi-function Soft Switch

**MG** - Media Gateway

**MP** - Media Protection (NIST security control family title)

**MSDP** - Multicast Source Discovery Protocol

**Multicast Listener Discovery (MLD)** - Used by IPv6 routers for discovering multicast listeners on a directly attached link, much like IGMP is used in IPv4.

**Multi-factor Authentication (MFA)** - Requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multi-factor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government PIV card and the DoD CAC.

**Multi-Protocol Labeled Switching (MPLS)** - A type of data-carrying technique for high-performance telecommunications network.

**N**

**NARA** - National Archives and Records Administration. See **Document 12829**, General Records Schedule (GRS) 3.2, Information Systems Security Records, for the National Archives and Records Administration (NARA)-approved retention and disposition requirements.

**NDM** - Network Device Management

**Network Access** - Access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

**Network Address Translation – Protocol Translation (NAT-PT)** - An IPv6-to-IPv4 translation mechanism, as defined in RFC 2765 and RFC 2766, which allows IPv6-only devices to communicate with IPv4-only devices and vice versa.

**Network Elements** - Any multiplexers, routers, CSU/DSUs, channel compression devices, and/or trunk encryption that is in the route or path that connects IRS switches, non-IRS users, and/or IP devices.

**NIST** - National Institute of Standards and Technology

**NMCC** - UNS Network Management Control Center

**NMS** - Network Management System

**NOC** - Network Operations Center

**Non-Repudiation** - Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

**NSA** - National Security Agency

**NSAP** - Network Service Access Point

**Exhibit 10.8.55-2 (Cont. 8) (08-25-2025)****Terms and Acronyms**

**NSS** - National Security System

**NTP** - Network Time Protocol

**O**

**OCSP** - Online Certificate Status Protocol

**OFDM** - Orthogonal Frequency Division Multiplexing

**OIG** - Office of Inspector General

**OMB** - Office of Management and Budget

**Operating System (OS)** - A collection of software that manages computer hardware resources and provides common service for computer programs.

**OSI** - Open Systems Interconnection

**Out of Band Management Network (OOB/OOBM)** - This is the dedicated management network. It utilizes encrypted connections (Transport Layer Security [TLS] and Internet Protocol Security [IPSec]) between the user and the hosting site to provide management capability for servers, applications and network devices. It also provides transport of monitoring and reporting devices.

**P**

**Pairwise Master Key (PMK)** - A key established between the wireless station and the access point. This key is typically generated using 802.1X, which is authentication of the user to a RADIUS or other authentication server using Extensible Authentication Protocol. Both the station and RADIUS server derive identical keys and the RADIUS server returns that key to the access point.

**Path Maximum Transmission Unit (PMTU) Discovery** - A standardized technique in computer networking for determining the MTU size on the network path between two IP hosts, usually with the goal of avoiding IP fragmentation. Originally intended for routers in IPv4, in IPv6 this function has been explicitly delegated to the end points of a communication session. See RFC 119 for additional guidance on PMTU Discovery.

**PC** - Personal Computer

**PE** - Physical and Environmental Protection (NIST security and privacy control family title)

**PDA** - Personal Digital Assistant

**PFS** - Perfect Forward Secrecy

**PII** - Personally Identifiable Information

**PIM** - Protocol Independent Multicast

**PIN** - Personal identification number

**PIV** - Personal Identity Verification

**PKI** - Public Key Infrastructure

**PL** - Planning (NIST security and privacy control family title)



**Exhibit 10.8.55-2 (Cont. 9) (08-25-2025)****Terms and Acronyms**

**Plan of Action and Milestones (POA&M)** - A key document of an information system's security authorization package describing the specific measures that are planned: (i) to correct weaknesses or deficiencies noted in the security controls during the security control assessment; and (ii) to address known vulnerabilities in the information system. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

**PM** - Program Management (NIST security and privacy control family title)

**POTS** - Plain Old Telephone Service

**PPTP** - Point-to-Point Tunneling Protocol

**PPSM** - Ports, Protocols, and Services Management

**PRI** - Primary Rate Interface

**PS** - Personnel Security (NIST security control family title)

**PT** - PII Processing and Transparency (NIST security control family title)

**Public Key Infrastructure (PKI)** - A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

**PTZ** - Pan, Tilt and Zoom

**Q**

**Quality-of-Service (QoS)** - The description or measurement of the overall performance of a service, such as telephony or computer networking service, particularly the performance seen by the users of the network. Cisco defines as the set of techniques to manage network resources.

**R**

**RA** - Risk Assessment (NIST security and privacy control family title)

**Rapid Spanning Tree Protocol (RSTP)** - A network protocol that builds a loop-free logical topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. STP also allows a network design to include backup links providing fault tolerance if an active link fails.

**RD** - Route Distinguisher

**Remediation** - The act of correcting a vulnerability or eliminating a threat through activities such as installing a patch, adjusting configuration settings, or uninstalling a software application.

**Remote Access** - Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

**Remote Access Server (RAS)** - A server, normally equipped with one or more modems, which allows remote users to dial in and establish temporary connections to a network.

**Remote Authentication Dial-In User Service (RADIUS)** - A client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.

**RFID** - Radio Frequency Identification



**Exhibit 10.8.55-2 (Cont. 10) (08-25-2025)****Terms and Acronyms**

**Risk Acceptance Decision** - A decision in which the Authorizing Official determine if they are going to accept a risk.

**Risk Assessment** - The process of determining risks; that is, determining the extent to which an entity is threatened by potential, adverse circumstances or events. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF). Risk assessment for information system-related security risks includes assessment of the susceptibility to adverse impacts through information (e.g., consideration of dependence on information, vulnerabilities in mission and business processes, and effectiveness of risk mitigations) and assessment of the threat environment with regard to causing such impacts. Synonymous with risk analysis.

**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). To document risk-based determinations, IT Cyber security has created an SOP and associated Form 14201.

**Robust Security Network (RSN)** - A protocol for establishing secure communications over an 802.11 wireless network.

**RP** - Rendezvous Point

**RSN** - Robust Security Network

**RSVP** - Resource Reservation Protocol

**RSVP-TE** - Resource Reservation Protocol – Traffic Engineering

**RT** - Route Target

**RTCP** - Real-Time Transport Control Protocol

**RTP** - Real-Time Transport Protocol

**RTR** - Router

**S**

**SA** - System Administrator; System and Services Acquisition (NIST security and privacy control family title)

**SC** - System and Communications Protection (NIST security and privacy control family title)

**SDN** - Software-Defined Networking

**Security Authorization** - The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation, based on the implementation of an agreed-upon set of security controls.

**Security Authorization Boundary** - All components of an information system to be authorized for operation by an AO and excludes separately authorized systems, to which the information system is connected.

**Security Requirements Guide (SRG)** - General statements and recommendations on how to secure a type of technology, without calling out a specific flavor or vendor.

**Exhibit 10.8.55-2 (Cont. 11) (08-25-2025)****Terms and Acronyms**

**Security Technical Implementation Guide (STIG)** - A methodology for standardized secure installation and maintenance of computer software and hardware.

**SHA-1** - Secure Hash Algorithm 1

**SIP** - Session Initiation Protocol

**SG** - Source-Group

**SI** - System and Information Integrity (NIST security and privacy control family title)

**SSL** - Secure Socket Layer

**SNMP** - Simple Network Management Protocol

**SP** - Special Publication

**Spanning Tree Protocol (STP)** – A network protocol that builds a loop-free logical topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. STP also allows a network design to include backup links providing fault tolerance if an active link fails.

**SPT** - Shortest-Path Tree (threshold)

**SQL** - Structured Query Language

**SR** - Supply Chain Risk Management (NIST security and privacy control family title)

**SRM** - Security Risk Management

**SRTCP** - Secure Real-Time Transport Protocol Control Protocol

**SS** - Soft switch

**Standard Operating Procedure (SOP)** - Established or prescribed methods to be followed routinely for the performance of designated operations or in designated situations.

**T**

**TCP/IP** - Transmission Control Protocol/Internet Protocol

**TCP/UDP** - Transmission Control Protocol/User Datagram Protocol

**Technical Controls** - The security controls (e.g., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

**Terminal Access Controller Access Control System (TACACS)** - An authentication protocol common to UNIX networks that allows a remote access server to forward a user's login password to an authentication server to determine whether access can be allowed to a given system.

**TIGTA** - Treasury Inspector General for Tax Administration

**TLS** - Transport Layer Security

**Exhibit 10.8.55-2 (Cont. 12) (08-25-2025)****Terms and Acronyms**

**Treasury Directive Publication (TD P)** - Documents that provide IT security requirements and supporting guidance that apply to the Department of the Treasury bureaus, Departmental Offices (DO), Office of the Inspector General (OIG), and the Treasury Inspector General for Tax Administration (TIGTA), hereafter referred to collectively as bureaus.

**TS-SCI** - Top secret – sensitive compartmented information

**TTL** - Time-to-Live

**U**

**UC** - Unified Capability/Unified Capabilities

**UDLD** - Unidirectional Link Detection

**UNS** - User and Network Services

**UNIX** - Uniplexed Information Computing System

**URL** - Uniform Resource Locator

**uRPF** - Unicast Reverse Path Forwarding

**US-CERT** - United States Computer Emergency Readiness Team

**User Account** - An operating system data object containing information identifying a user to an operating system. A user account, for example typically contains a user's name and password, the user account's group memberships, and the user's rights and permissions for accessing an information system and its resources.

**UTC** - Coordinated Universal Time

**UUFB** - Unknown Unicast Flood Blocking

**V**

**VC** - Virtual Circuit

**VFI** - Virtual Forwarding Instance

**VLAN** - Virtual Local Area Network

**VLAN Trunk Protocol (VPT)** - A Cisco proprietary protocol that propagates the definition of VLANs on the whole local area network.

**Voice over Internet Protocol (VoIP)** - A methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks.

**VPLS** - Virtual Private LAN Services

**VPN** - Virtual Private Network

**VPWS** - Virtual Private Wire Service

**VRF** - Virtual Routing and Forwarding

**VTC** - Video Teleconferencing

**Exhibit 10.8.55-2 (Cont. 13) (08-25-2025)****Terms and Acronyms**

**Vulnerability** - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

**Vulnerability Assessment (VA)** - Formal description and evaluation of the vulnerabilities in an information system.

**Vulnerability Scanning** - The process of proactively identifying vulnerabilities of an information system in order to determine if and where a system can be exploited and/or threatened. Employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

**VVoIP** - Voice/Video over Internet Protocol

**W**

**Waiver** - A process utilized by IRS's Enterprise Architecture (EA) organization. System owners can request a waiver for system(s) that cannot meet the infrastructure configuration management requirements established by the EA.

**Wide Area Network (WAN)** - A network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, or national boundaries) using private or public network transports.

**WIDS** - Wireless Intrusion Detection System

**Wi-Fi Protected Access (WPA)** - A security protocol and security certification program developed by the Wi-Fi Alliance to secure wireless computer networks.

**WIPS** - Wireless Intrusion Protection System

**Wireless Local Area Network (WLAN)** - Links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), and usually provides a connection through an access point to the wider internet.

**WPA2** - Wi-Fi Protected Access II

**Exhibit 10.8.55-3 (08-25-2025)****Related Resources****IRS Publications**

- IRM 10.8.1, **Information Technology (IT) Security, Security Policy**, issued December 12, 2023
- IRM 10.8.2, **Information Technology (IT) Security, IT Security Roles and Responsibilities**, issued November 07, 2023
- IRM 10.8.24, **Information Technology (IT) Security, Cloud Computing Security Policy**, issued February 02, 2024
- IRM 10.8.26, **Information Technology (IT) Security, Wireless and Mobile Device Security Policy**, issued November 06, 2023
- IRM 10.8.50, **Information Technology (IT) Security, Enterprise Incident, Vulnerability, and Security Patch Management**, issued March 11, 2024
- IRM 10.8.54, **Information Technology (IT) Security, Minimum Firewall Administration Requirements**, issued July 22, 2024
- IRM 10.9.1, **Classified National Security Information (CNSI)**, November 06, 2023

**Department of the Treasury Publications**

- TD P 85-01, **Treasury Information Technology (IT) Security Program v3.1.3**, issued February 28, 2022

**National Institute of Standards and Technology (NIST) Publications**

- FIPS 140-2: **Security Requirements for Cryptographic Modules**, issued May 25, 2001 (Change Notice 2, 12/3/2002)
- FIPS 140-3: **Security Requirements for Cryptographic Modules**, issued March 22, 2019
- FIPS 198-1: **The Keyed-Hash Message Authentication Code (HMAC)**, issued July 16, 2008
- FIPS 199: **Standards for Security Categorization of Federal Information and Information Systems**, issued February 01, 2004
- FIPS 200: **Minimum Security Requirements for Federal Information and Information Systems**, issued March 01, 2006
- SP 800-37 Revision 2: **Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy**, issued December 20, 2018
- SP 800-53 Revision 5: **Security and Privacy Controls for Information Systems and Organizations**, issued December 10, 2020 (includes updates as of November 07, 2023)
- SP 800-53A Rev 5: **Assessing Security and Privacy Controls in Information Systems and Organizations**, issued January 25, 2022 (includes updates as of November 07, 2023)
- SP 800-57 Rev 5: **Recommended for Key Management – Part 1 General**, issued May 04, 2020
- SP 800-70 Rev 4 : **National Checklist Program for IT Products: Guidelines for Checklist Users and Developers**, issued February 15, 2018
- SP 800-97: **Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i**, issued February 07, 2007
- SP 800-98: **Guidelines for Securing Radio Frequency Identification (RFID) Systems**, issued April 06, 2007
- SP 800-131A Revision 2: **Transitioning the Use of Cryptographic Algorithms and Key Lengths**, issued March 21, 2019
- SP 800-153: **Guidelines for Securing Wireless Local Area Networks (WLANs)**, issued February 21, 2012
- SP 800-175B Revision 1: **Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms**, issued March 31, 2020

**Exhibit 10.8.55-3 (Cont. 1) (08-25-2025)****Related Resources****Defense Information Systems Agency (DISA) Publications**

- Enterprise Voice, Video, and Messaging Endpoint SRG V1R1, issued March 15, 2024
- Enterprise Voice, Video, and Messaging Policy SRG V1R1, issued March 15, 2024
- Enterprise Voice, Video, and Messaging Session Management SRG V1R1, issued March 15, 2024
- Intrusion Detection and Prevention Systems SRG V3R2 issued January 30, 2025
- Layer 2 Switch SRG V3R2, issued April 02, 2025
- Network Device Management SRG V5R3, issued April 02, 2025
- Router SRG V5R1, issued July 24, 2024
- SDN Controller SRG V2R1, issued July 24, 2024
- Virtual Private Network (VPN) SRG V3R3, issued 30 January 2025
- DISA STIGs and SRGs are available at: *STIG Document Library - DoD Cyber Exchange*