



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.1

APRIL 30, 2025

EFFECTIVE DATE

(04-30-2025)

PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.8.1, *Information Technology (IT) Security, Security Policy*.

MATERIAL CHANGES

- (1) 10.8.1.4.16.1.3 (3), Personally Identifiable Information (PII): Updated to comply with January 2025 Executive Orders and OPM guidance.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 10.8.1 dated January 28, 2025.

AUDIENCE

The provisions in this manual apply to:

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

Rajiv Uppal
Chief Information Officer

10.8.1
Security Policy

Table of Contents

- 10.8.1.1 Program Scope and Objectives
 - 10.8.1.1.1 Background
 - 10.8.1.1.2 Authority
 - 10.8.1.1.3 Roles and Responsibilities
 - 10.8.1.1.4 Program Management and Review
 - 10.8.1.1.5 Program Controls
 - 10.8.1.1.6 Terms and Acronyms
 - 10.8.1.1.7 Related Resources
- 10.8.1.2 Risk Acceptance and Risk-Based Decisions (RBDs)
 - 10.8.1.2.1 Risk Acceptance Request
 - 10.8.1.2.2 Exceptions to Treasury Requirements
- 10.8.1.3 General Policy
 - 10.8.1.3.1 Zero Trust and Zero Trust Architecture
 - 10.8.1.3.2 Critical Software
- 10.8.1.4 Security and Privacy Controls, Enhancements, and Supplemental Guidance
 - 10.8.1.4.1 AC-01 Access Control Policy and Procedures
 - 10.8.1.4.1.1 AC-02 Account Management
 - 10.8.1.4.1.1.1 Business Role Account Inactivity
 - 10.8.1.4.1.1.2 Fire Call Account
 - 10.8.1.4.1.1.3 Service Account Requirements
 - 10.8.1.4.1.1.4 Non-Person Entity (NPE) Account Requirements
 - 10.8.1.4.1.1.5 Access to Sensitive Information
 - 10.8.1.4.1.1.6 Access Authorization
 - 10.8.1.4.1.2 AC-03 Access Enforcement
 - 10.8.1.4.1.3 AC-04 Information Flow Enforcement
 - 10.8.1.4.1.4 AC-05 Separation of Duties
 - 10.8.1.4.1.5 AC-06 Least Privilege (InTC)
 - 10.8.1.4.1.6 AC-07 Unsuccessful Logon Attempts
 - 10.8.1.4.1.7 AC-08 System-Use Notifications
 - 10.8.1.4.1.8 AC-09 Previous Logon (Access) Notification
 - 10.8.1.4.1.9 AC-10 Concurrent Session Control
 - 10.8.1.4.1.10 AC-11 Device Lock
 - 10.8.1.4.1.11 AC-12 Session Termination
 - 10.8.1.4.1.12 AC-13 (Withdrawn)
 - 10.8.1.4.1.13 AC-14 Permitted Actions without Identification or Authentication

- 10.8.1.4.1.14 AC-15 (Withdrawn)
- 10.8.1.4.1.15 AC-16 Security and Privacy Attributes
- 10.8.1.4.1.16 AC-17 Remote Access
- 10.8.1.4.1.17 AC-18 Wireless Access
- 10.8.1.4.1.18 AC-19 Access Control for Mobile Devices
 - 10.8.1.4.1.18.1 Telecommunication Devices
 - 10.8.1.4.1.18.2 Video and Photographic Technologies
- 10.8.1.4.1.19 AC-20 Use of External Systems
 - 10.8.1.4.1.19.1 Personally-Owned and Other Non-Government Furnished Equipment
- 10.8.1.4.1.20 AC-21 Information Sharing
- 10.8.1.4.1.21 AC-22 Publicly Accessible Content
- 10.8.1.4.1.22 AC-23 Data Mining Protection
- 10.8.1.4.1.23 AC-24 Access Control Decisions
- 10.8.1.4.1.24 AC-25 Reference Monitor
- 10.8.1.4.2 AT-01 Awareness and Training Policy and Procedures
 - 10.8.1.4.2.1 AT-02 Literacy Training and Awareness (InTC)
 - 10.8.1.4.2.2 AT-03 Role-Based Training
 - 10.8.1.4.2.3 AT-04 Training Records
 - 10.8.1.4.2.4 AT-05 (Withdrawn)
 - 10.8.1.4.2.5 AT-06 Training Feedback
- 10.8.1.4.3 AU-01 Audit and Accountability Policy and Procedures
 - 10.8.1.4.3.1 AU-02 Event Logging
 - 10.8.1.4.3.2 AU-03 Content of Audit Records
 - 10.8.1.4.3.3 AU-04 Audit Log Storage Capacity
 - 10.8.1.4.3.4 AU-05 Response to Audit Logging Process Failures
 - 10.8.1.4.3.5 AU-06 Audit Record Review, Analysis, and Reporting (InTC)
 - 10.8.1.4.3.6 AU-07 Audit Record Reduction and Report Generation (InTC)
 - 10.8.1.4.3.7 AU-08 Time Stamps
 - 10.8.1.4.3.8 AU-09 Protection of Audit Information
 - 10.8.1.4.3.9 AU-10 Non-Repudiation (InTC)
 - 10.8.1.4.3.10 AU-11 Audit Record Retention
 - 10.8.1.4.3.11 AU-12 Audit Record Generation (InTC)
 - 10.8.1.4.3.12 AU-13 Monitoring for Information Disclosure (InTC)
 - 10.8.1.4.3.13 AU-14 Session Audit
 - 10.8.1.4.3.14 AU-15 (Withdrawn)
 - 10.8.1.4.3.15 AU-16 Cross-Organizational Audit Logging
- 10.8.1.4.4 CA-01 Assessment, Authorization, and Monitoring Policy and Procedures
 - 10.8.1.4.4.1 CA-02 Control Assessments
 - 10.8.1.4.4.2 CA-03 Information Exchange

- 10.8.1.4.4.2.1 Interconnection Security Agreements
- 10.8.1.4.4.3 CA-04 (Withdrawn)
- 10.8.1.4.4.4 CA-05 Plan of Action and Milestones (POA&M)
- 10.8.1.4.4.5 CA-06 Authorization
 - 10.8.1.4.4.5.1 FISMA Reporting Requirements
- 10.8.1.4.4.6 CA-07 Continuous Monitoring (InTC)
 - 10.8.1.4.4.6.1 Compliance Monitoring
- 10.8.1.4.4.7 CA-08 Penetration Testing
- 10.8.1.4.4.8 CA-09 Internal System Connections
- 10.8.1.4.5 CM-01 Configuration Management Policy and Procedures
 - 10.8.1.4.5.1 CM-02 Baseline Configuration
 - 10.8.1.4.5.2 CM-03 Configuration Change Control
 - 10.8.1.4.5.3 CM-04 Impact Analysis
 - 10.8.1.4.5.4 CM-05 Access Restrictions for Change
 - 10.8.1.4.5.5 CM-06 Configuration Settings
 - 10.8.1.4.5.6 CM-07 Least Functionality
 - 10.8.1.4.5.7 CM-08 System Component Inventory
 - 10.8.1.4.5.8 CM-09 Configuration Management Plan
 - 10.8.1.4.5.9 CM-10 Software Usage Restrictions
 - 10.8.1.4.5.10 CM-11 User-Installed Software
 - 10.8.1.4.5.11 CM-12 Information Location
 - 10.8.1.4.5.12 CM-13 Data Action Mapping
 - 10.8.1.4.5.13 CM-14 Signed Components
- 10.8.1.4.6 CP-01 Contingency Planning Policy and Procedures
 - 10.8.1.4.6.1 CP-02 Contingency Plan
 - 10.8.1.4.6.1.1 Emergency Response Capability
 - 10.8.1.4.6.2 CP-03 Contingency Training
 - 10.8.1.4.6.3 CP-04 Contingency Plan Testing
 - 10.8.1.4.6.4 CP-05 (Withdrawn)
 - 10.8.1.4.6.5 CP-06 Alternate Storage Site
 - 10.8.1.4.6.6 CP-07 Alternate Processing Site
 - 10.8.1.4.6.7 CP-08 Telecommunications Services
 - 10.8.1.4.6.8 CP-09 System Backup
 - 10.8.1.4.6.9 CP-10 System Recovery and Reconstitution
 - 10.8.1.4.6.10 CP-11 Alternate Communications Protocols
 - 10.8.1.4.6.11 CP-12 Safe Mode
 - 10.8.1.4.6.12 CP-13 Alternative Security Mechanisms
- 10.8.1.4.7 IA-01 Identification and Authentication Policy and Procedures
 - 10.8.1.4.7.1 IA-02 Identification and Authentication (Organizational Users)

- 10.8.1.4.7.2 IA-03 Device Identification and Authentication
- 10.8.1.4.7.3 IA-04 Identifier Management (InTC)
- 10.8.1.4.7.4 IA-05 Authenticator Management
 - 10.8.1.4.7.4.1 Application and Operating System (OS) Password Policies for Non-MFA Systems
- 10.8.1.4.7.5 IA-06 Authenticator Feedback
- 10.8.1.4.7.6 IA-07 Cryptographic Module Authentication
- 10.8.1.4.7.7 IA-08 Identification and Authentication (Non-Organizational Users)
- 10.8.1.4.7.8 IA-09 Service Identification and Authentication
- 10.8.1.4.7.9 IA-10 Adaptive Authentication
- 10.8.1.4.7.10 IA-11 Re-authentication
- 10.8.1.4.7.11 IA-12 Identity Proofing
- 10.8.1.4.7.12 IA-13 Identity Providers and Authorization Servers
- 10.8.1.4.8 IR-01 Incident Response Policy and Procedures
 - 10.8.1.4.8.1 IR-02 Incident Response Training
 - 10.8.1.4.8.2 IR-03 Incident Response Testing
 - 10.8.1.4.8.3 IR-04 Incident Handling (InTC)
 - 10.8.1.4.8.4 IR-05 Incident Monitoring
 - 10.8.1.4.8.5 IR-06 Incident Reporting
 - 10.8.1.4.8.6 IR-07 Incident Response Assistance
 - 10.8.1.4.8.7 IR-08 Incident Response Plan
 - 10.8.1.4.8.8 IR-09 Information Spillage Response
- 10.8.1.4.9 MA-01 Maintenance Policy and Procedures
 - 10.8.1.4.9.1 MA-02 Controlled Maintenance
 - 10.8.1.4.9.2 MA-03 Maintenance Tools
 - 10.8.1.4.9.3 MA-04 Non-Local Maintenance
 - 10.8.1.4.9.4 MA-05 Maintenance Personnel
 - 10.8.1.4.9.5 MA-06 Timely Maintenance
 - 10.8.1.4.9.6 MA-07 Field Maintenance
- 10.8.1.4.10 MP-01 Media Protection Policy and Procedures
 - 10.8.1.4.10.1 MP-02 Media Access
 - 10.8.1.4.10.2 MP-03 Media Marking
 - 10.8.1.4.10.3 MP-04 Media Storage
 - 10.8.1.4.10.3.1 Portable Electronic Devices (PEDs) as Storage Media
 - 10.8.1.4.10.4 MP-05 Media Transport
 - 10.8.1.4.10.5 MP-06 Media Sanitization
 - 10.8.1.4.10.6 MP-07 Media Use (InTC)
 - 10.8.1.4.10.6.1 Portable Electronic Devices (PEDs)
 - 10.8.1.4.10.7 MP-08 Media Downgrading
- 10.8.1.4.11 PE-01 Physical and Environmental Protection Policy and Procedures

-
- 10.8.1.4.11.1 PE-02 Physical Access Authentication (InTC)
 - 10.8.1.4.11.2 PE-03 Physical Access Control
 - 10.8.1.4.11.3 PE-04 Access Control for Transmission
 - 10.8.1.4.11.4 PE-05 Access Control for Output Devices
 - 10.8.1.4.11.5 PE-06 Monitoring Physical Access
 - 10.8.1.4.11.6 PE-07 (Withdrawn)
 - 10.8.1.4.11.7 PE-08 Visitor Access Records
 - 10.8.1.4.11.8 PE-09 Power Equipment and Cabling
 - 10.8.1.4.11.9 PE-10 Emergency Shutoff
 - 10.8.1.4.11.10 PE-11 Emergency Power
 - 10.8.1.4.11.11 PE-12 Emergency Lighting
 - 10.8.1.4.11.12 PE-13 Fire Protection
 - 10.8.1.4.11.13 PE-14 Environmental Controls
 - 10.8.1.4.11.14 PE-15 Water Damage Protection
 - 10.8.1.4.11.15 PE-16 Delivery and Removal
 - 10.8.1.4.11.16 PE-17 Alternate Work Site
 - 10.8.1.4.11.17 PE-18 Location of System Components
 - 10.8.1.4.11.18 PE-19 Information Leakage
 - 10.8.1.4.11.19 PE-20 Asset Monitoring and Tracking
 - 10.8.1.4.11.20 PE-21 Electromagnetic Pulse Protection
 - 10.8.1.4.11.21 PE-22 Component Marking
 - 10.8.1.4.11.22 PE-23 Facility Location
 - 10.8.1.4.12 PL-01 Planning Policy and Procedures
 - 10.8.1.4.12.1 PL-02 System Security and Privacy Plans
 - 10.8.1.4.12.2 PL-03 (Withdrawn)
 - 10.8.1.4.12.3 PL-04 Rules of Behavior
 - 10.8.1.4.12.4 PL-05 (Withdrawn)
 - 10.8.1.4.12.5 PL-06 (Withdrawn)
 - 10.8.1.4.12.6 PL-07 Security Concept of Operations
 - 10.8.1.4.12.7 PL-08 Security and Privacy Architecture
 - 10.8.1.4.12.8 PL-09 Central Management
 - 10.8.1.4.12.9 PL-10 Baseline Selection
 - 10.8.1.4.12.10 PL-11 Baseline Tailoring
 - 10.8.1.4.13 Program Management Controls
 - 10.8.1.4.13.1 PM-01 Information Security Program Plan (InTC)
 - 10.8.1.4.13.2 PM-02 Information Security Program Leadership Role
 - 10.8.1.4.13.3 PM-03 Information Security and Privacy Resources
 - 10.8.1.4.13.4 PM-04 Plan of Action and Milestones (POA&M) Process
 - 10.8.1.4.13.5 PM-05 System Inventory

- 10.8.1.4.13.6 PM-06 Measures of Performance
- 10.8.1.4.13.7 PM-07 Enterprise Architecture
- 10.8.1.4.13.8 PM-08 Critical Infrastructure Plan
 - 10.8.1.4.13.8.1 Treasury Critical Infrastructure Protection (CIP) Plan Overview
- 10.8.1.4.13.9 PM-09 Risk Management Strategy
- 10.8.1.4.13.10 PM-10 Authorization Process
- 10.8.1.4.13.11 PM-11 Mission and Business Process Definition
- 10.8.1.4.13.12 PM-12 Insider Threat Program (InTC)
 - 10.8.1.4.13.12.1 IRS Insider Threat Capability (InTC)
- 10.8.1.4.13.13 PM-13 Security and Privacy Workforce
- 10.8.1.4.13.14 PM-14 Testing, Training, and Monitoring (InTC)
- 10.8.1.4.13.15 PM-15 Security and Privacy Groups and Associations
- 10.8.1.4.13.16 PM-16 Threat Awareness Program (InTC)
- 10.8.1.4.13.17 PM-17 Protecting Controlled Unclassified Information on External Systems
- 10.8.1.4.13.18 PM-18 Privacy Program Plan
- 10.8.1.4.13.19 PM-19 Privacy Program Leadership Role
- 10.8.1.4.13.20 PM-20 Dissemination of Privacy Program Information
- 10.8.1.4.13.21 PM-21 Accounting of Disclosures
- 10.8.1.4.13.22 PM-22 Personally Identifiable Information Quality Management
- 10.8.1.4.13.23 PM-23 Data Governance Body
- 10.8.1.4.13.24 PM-24 Data Integrity Board
- 10.8.1.4.13.25 PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research
- 10.8.1.4.13.26 PM-26 Complaint Management
- 10.8.1.4.13.27 PM-27 Privacy Reporting
- 10.8.1.4.13.28 PM-28 Risk Framing
- 10.8.1.4.13.29 PM-29 Risk Management Program Leadership Roles
- 10.8.1.4.13.30 PM-30 Supply Chain Risk Management Strategy
- 10.8.1.4.13.31 PM-31 Continuous Monitoring Strategy
- 10.8.1.4.13.32 PM-32 Purposing
- 10.8.1.4.14 PS-01 Personnel Security Policy and Procedures
 - 10.8.1.4.14.1 PS-02 Position Risk Designation
 - 10.8.1.4.14.2 PS-03 Personnel Screening (InTC)
 - 10.8.1.4.14.3 PS-04 Personnel Termination (InTC)
 - 10.8.1.4.14.4 PS-05 Personnel Transfer (InTC)
 - 10.8.1.4.14.5 PS-06 Access Agreements
 - 10.8.1.4.14.6 PS-07 External Personnel Security
 - 10.8.1.4.14.7 PS-08 Personnel Sanctions (InTC)
 - 10.8.1.4.14.8 PS-09 Position Descriptions

- 10.8.1.4.15 PT - Personally Identifiable Information Processing and Transparency
- 10.8.1.4.16 RA-01 Risk Assessment Policy and Procedures
 - 10.8.1.4.16.1 RA-02 Security Categorization
 - 10.8.1.4.16.1.1 Sensitive But Unclassified (SBU) Information
 - 10.8.1.4.16.1.2 Controlled Unclassified Information (CUI)
 - 10.8.1.4.16.1.3 Personally Identifiable Information (PII)
 - 10.8.1.4.16.2 RA-03 Risk Assessment
 - 10.8.1.4.16.3 RA-04 (Withdrawn)
 - 10.8.1.4.16.4 RA-05 Vulnerability Monitoring and Scanning
 - 10.8.1.4.16.4.1 Vulnerability Prioritization
 - 10.8.1.4.16.4.2 Vulnerability Remediation
 - 10.8.1.4.16.5 RA-06 Technical Surveillance Countermeasures Survey
 - 10.8.1.4.16.6 RA-07 Risk Response
 - 10.8.1.4.16.7 RA-08 Privacy Impact Assessments
 - 10.8.1.4.16.8 RA-09 Criticality Analysis
 - 10.8.1.4.16.9 RA-10 Threat Hunting
- 10.8.1.4.17 SA-01 System and Services Acquisition Policy and Procedures
 - 10.8.1.4.17.1 SA-02 Allocation of Resources
 - 10.8.1.4.17.2 SA-03 System Development Life Cycle (SDLC)
 - 10.8.1.4.17.3 SA-04 Acquisition Process
 - 10.8.1.4.17.4 SA-05 System Documentation
 - 10.8.1.4.17.5 SA-06 (Withdrawn)
 - 10.8.1.4.17.6 SA-07 (Withdrawn)
 - 10.8.1.4.17.7 SA-08 Security and Privacy Engineering Principles
 - 10.8.1.4.17.8 SA-09 External System Services
 - 10.8.1.4.17.9 SA-10 Developer Configuration Management
 - 10.8.1.4.17.10 SA-11 Developer Testing and Evaluation
 - 10.8.1.4.17.11 SA-12 (Withdrawn)
 - 10.8.1.4.17.12 SA-13 (Withdrawn)
 - 10.8.1.4.17.13 SA-14 (Withdrawn)
 - 10.8.1.4.17.14 SA-15 Development Process, Standards, and Tools
 - 10.8.1.4.17.15 SA-16 Developer-Provided Training
 - 10.8.1.4.17.16 SA-17 Develop Security and Privacy Architecture and Design
 - 10.8.1.4.17.17 SA-18 (Withdrawn)
 - 10.8.1.4.17.18 SA-19 (Withdrawn)
 - 10.8.1.4.17.19 SA-20 Customized Development of Critical Components
 - 10.8.1.4.17.20 SA-21 Developer Screening
 - 10.8.1.4.17.21 SA-22 Unsupported System Components
 - 10.8.1.4.17.22 SA-23 Specialization

-
- 10.8.1.4.18 SC-01 System and Communications Protection Policy and Procedures
 - 10.8.1.4.18.1 SC-02 Separation of System and User Functionality
 - 10.8.1.4.18.2 SC-03 Security Function Isolation
 - 10.8.1.4.18.3 SC-04 Information in Shared System Resources
 - 10.8.1.4.18.4 SC-05 Denial of Service Protection
 - 10.8.1.4.18.5 SC-06 Resource Availability
 - 10.8.1.4.18.6 SC-07 Boundary Protection (InTC)
 - 10.8.1.4.18.6.1 Internet Security
 - 10.8.1.4.18.6.2 Network Protection and Design
 - 10.8.1.4.18.7 SC-08 Transmission Confidentiality and Integrity
 - 10.8.1.4.18.8 SC-09 (Withdrawn)
 - 10.8.1.4.18.9 SC-10 Network Disconnect
 - 10.8.1.4.18.10 SC-11 Trusted Path
 - 10.8.1.4.18.11 SC-12 Cryptographic Key Establishment and Management
 - 10.8.1.4.18.12 SC-13 Cryptographic Protection
 - 10.8.1.4.18.12.1 Public Key/Private Key
 - 10.8.1.4.18.13 SC-14 (Withdrawn)
 - 10.8.1.4.18.14 SC-15 Collaborative Computing Devices and Applications
 - 10.8.1.4.18.14.1 Collaborative Technology and Systems
 - 10.8.1.4.18.14.1.1 Internal Collaborative Technology and Systems (e.g., SharePoint, Centra)
 - 10.8.1.4.18.14.1.2 External Collaborative Technology and Systems
 - 10.8.1.4.18.15 SC-16 Transmission of Security and Privacy Attributes
 - 10.8.1.4.18.16 SC-17 Public Key Infrastructure (PKI) Certificates
 - 10.8.1.4.18.17 SC-18 Mobile Code
 - 10.8.1.4.18.18 SC-19 (Withdrawn)
 - 10.8.1.4.18.19 SC-20 Secure Name/Address Resolution Service (Authoritative Source)
 - 10.8.1.4.18.20 SC-21 Secure Name/Address Resolution Service (Recursive or Caching Resolver)
 - 10.8.1.4.18.21 SC-22 Architecture and Provisioning for Name/Address Resolution Service
 - 10.8.1.4.18.22 SC-23 Session Authenticity
 - 10.8.1.4.18.23 SC-24 Fail in Known State
 - 10.8.1.4.18.24 SC-25 Thin Nodes
 - 10.8.1.4.18.25 SC-26 Decoys
 - 10.8.1.4.18.26 SC-27 Platform-Independent Applications
 - 10.8.1.4.18.27 SC-28 Protection of Information at Rest
 - 10.8.1.4.18.28 SC-29 Heterogeneity
 - 10.8.1.4.18.29 SC-30 Concealment and Misdirection
 - 10.8.1.4.18.30 SC-31 Covert Channel Analysis
 - 10.8.1.4.18.31 SC-32 System Partitioning
 - 10.8.1.4.18.32 SC-33 (Withdrawn)

-
- 10.8.1.4.18.33 SC-34 Non-Modifiable Executable Programs
 - 10.8.1.4.18.34 SC-35 External Malicious Code Identification
 - 10.8.1.4.18.35 SC-36 Distributed Processing and Storage
 - 10.8.1.4.18.36 SC-37 Out-of-Band Channels
 - 10.8.1.4.18.37 SC-38 Operations Security (InTC)
 - 10.8.1.4.18.38 SC-39 Process Isolation
 - 10.8.1.4.18.39 SC-40 Wireless Link Protection
 - 10.8.1.4.18.40 SC-41 Port and I/O Device Access
 - 10.8.1.4.18.41 SC-42 Sensor Capability and Data
 - 10.8.1.4.18.42 SC-43 Usage Restrictions
 - 10.8.1.4.18.43 SC-44 Detonation Chambers
 - 10.8.1.4.18.44 SC-45 System Time Synchronization
 - 10.8.1.4.18.45 SC-46 Cross Domain Policy Enforcement
 - 10.8.1.4.18.46 SC-47 Alternate Communications Paths
 - 10.8.1.4.18.47 SC-48 Sensor Relocation
 - 10.8.1.4.18.48 SC-49 Hardware-Enforced Separation and Policy Enforcement
 - 10.8.1.4.18.49 SC-50 Software-Enforced Separation and Policy Enforcement
 - 10.8.1.4.18.50 SC-51 Hardware-Based Protection
 - 10.8.1.4.19 SI-01 System and Information Integrity Policy and Procedures
 - 10.8.1.4.19.1 SI-02 Flaw Remediation
 - 10.8.1.4.19.2 SI-03 Malicious Code Protection
 - 10.8.1.4.19.2.1 Electronic Mail (Email) Security
 - 10.8.1.4.19.2.1.1 Privately Owned Email Accounts
 - 10.8.1.4.19.3 SI-04 System Monitoring (InTC)
 - 10.8.1.4.19.4 SI-05 Security Alerts, Advisories, and Directives
 - 10.8.1.4.19.5 SI-06 Security and Privacy Function Verification
 - 10.8.1.4.19.6 SI-07 Software, Firmware, and Information Integrity
 - 10.8.1.4.19.7 SI-08 Spam Protection
 - 10.8.1.4.19.8 SI-09 (Withdrawn)
 - 10.8.1.4.19.9 SI-10 Information Input Validation
 - 10.8.1.4.19.10 SI-11 Error Handling
 - 10.8.1.4.19.11 SI-12 Information Management and Retention
 - 10.8.1.4.19.12 SI-13 Predictable Failure Prevention
 - 10.8.1.4.19.13 SI-14 Non-Persistence
 - 10.8.1.4.19.14 SI-15 Information Output Filtering
 - 10.8.1.4.19.15 SI-16 Memory Protection
 - 10.8.1.4.19.16 SI-17 Fail-Safe Procedures
 - 10.8.1.4.19.17 SI-18 Personally Identifiable Information Quality Operations
 - 10.8.1.4.19.18 SI-19 De-Identification

-
- 10.8.1.4.19.19 SI-20 Tainting
 - 10.8.1.4.19.20 SI-21 Information Refresh
 - 10.8.1.4.19.21 SI-22 Information Diversity
 - 10.8.1.4.19.22 SI-23 Information Fragmentation
 - 10.8.1.4.20 SR-01 Supply Chain Risk Management Policy and Procedures
 - 10.8.1.4.20.1 SR-02 Supply Chain Risk Management Plan
 - 10.8.1.4.20.2 SR-03 Supply Chain Controls and Processes
 - 10.8.1.4.20.3 SR-04 Provenance
 - 10.8.1.4.20.4 SR-05 Acquisition Strategies, Tools, and Methods
 - 10.8.1.4.20.5 SR-06 Supplier Assessments and Reviews
 - 10.8.1.4.20.6 SR-07 Supply Chain Operations Security
 - 10.8.1.4.20.7 SR-08 Notification Agreements
 - 10.8.1.4.20.8 SR-09 Tamper Resistance and Detection
 - 10.8.1.4.20.9 SR-10 Inspection of Systems or Components
 - 10.8.1.4.20.10 SR-11 Component Authenticity
 - 10.8.1.4.20.11 SR-12 Component Disposal

Exhibits

- 10.8.1-1 Terms and Acronyms
- 10.8.1-2 Related Resources

10.8.1.1
(01-28-2025)
Program Scope and Objectives

- (1) **Overview:** This IRM lays the foundation to implement and manage security for systems within the IRS. It provides guidance on all aspects of security for the protection of information technology (IT) resources.
 - a. This guidance establishes the IT security framework for the development of security control specific implementations defined in subordinate IRMs, IRS publications (e.g., IRS Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*; IRS Pub 4812, *Contractor Security & Privacy Controls -- Handling and Protecting Information or Information Systems*), and subordinate procedural guidance (e.g., standard operating Procedures (SOPs), desk procedures).
 - b. This IRM provides the minimal security requirements for IRS IT systems based on data classification. Subordinate IRM sections of the 10.8, *Information Technology (IT) Security* series provide platform and technology specific security requirements and may have vendor specific hardening security requirements checklists associated with them. In the event there is a conflict between IRM 10.8.1, *Information Technology (IT) Security, Security Policy*, and subordinate IRM sections (and their checklists), the more restrictive setting must be implemented and documented.
 - c. Subordinate procedural guidance (e.g., SOPs) must be used to provide detailed guidance for implementing and complying with the requirements within this IRM.
 - d. Binding operational directives (BODs) and emergency directives (EDs) issued by Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS) are effective immediately and are incorporated into IRS Security Policies. If there is a conflict with or variance between the CISA guidance and IRS security guidance, the more restrictive guidance takes precedence.
- (2) **Program Purpose:** Develop and publish security policies to protect the IRS against potential security threats, risks, and vulnerabilities to ensure compliance with federal mandates and legislation.
- (3) **Audience:** The provisions within this policy apply to:
 - a. All offices and business, operating, and functional units within the IRS.
 - b. IRS personnel and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, which use or operate systems that store, process, or transmit IRS information or connect to an IRS network or system.
- (4) **Policy Owner:** Chief Information Officer (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.

10.8.1.1.1
(12-12-2023)
Background

- (1) *Federal Information Processing Standards (FIPS) Publication 200, Minimum Security Requirements for Federal Information and Information Systems* mandates the use of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 as baseline for the creation of agency IT security policy.

10.8.1.1.2
(12-13-2022)

Authority

- (2) IRM 10.8.1 is part of the IRM Part 10, *Security, Privacy, Assurance, and Artificial Intelligence* series for IRS IT Cybersecurity.
- (1) This IRM covers IT controls from *NIST SP 800-53 Rev 5, Security and Privacy Controls for Information Systems and Organizations*, Department of the Treasury policy, IRS-defined policy, regulatory and mandated guidance, and other sources (refer to IRM 10.8.1.1.7 Related Resources subsection within this IRM).
- (2) Per *FIPS 200*:
 - a. Policies and procedures play an important role in the effective implementation of enterprise-wide information security programs within the Federal Government and the success of the resulting security measures employed to protect federal information and information systems. Thus, organizations must develop and promulgate formal, documented policies and procedures governing the minimum security requirements set forth in this standard and must ensure their effective implementation.
 - b. SPs are developed and issued by NIST as recommendations and guidance documents. For other than national security programs and systems, federal agencies must follow those NIST SPs mandated in a FIPS publication. *FIPS 200* mandates the use of SP 800-53, as amended. In addition, Office of Management and Budget (OMB) policies (including OMB Reporting Instructions for Federal Information Security Modernization Act of 2014 (FISMA) and Agency Privacy Management) state that for other than national security programs and systems, federal agencies must follow certain specific NIST SPs.
 - c. While federal agencies are required to follow certain specific NIST SPs in accordance with OMB policy, agencies have flexibility in how to apply the guidance. Federal agencies apply the security concepts and principles articulated in the NIST SPs in accordance with and in the context of the agency's missions, business functions, and environment of operation. Consequently, the application of NIST guidance by federal agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of adequate security for federal systems.
- (3) IRM 10.8.1 is issued under the authority of Treasury Directive Publication (TD P) 85-01, *Treasury Information Technology (IT) Security Program*.
- (4) In accordance with OMB's FISMA guidelines for non-national security programs and systems, agencies must follow NIST standards and guidance. Non-national security systems must provide adequate, risk-based protection in the control areas defined in *FIPS 200* by using the appropriate NIST SP 800-53 baseline security controls for the designated *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems* impact level, as augmented and scoped by the Department of the Treasury, bureau, and system owner (to the extent authorized).

10.8.1.1.3
(12-12-2023)

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.

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

10.8.1.1.4
(01-28-2025)
**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 manual 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, Department of the Treasury directives (TDs), NIST publications, National Archives and Records Administration (NARA) guidance, other regulatory guidance, and best practice methodologies.
 - d. Use best practice methodologies (such as Capability Maturity Model Integration (CMMI), Enterprise Life Cycle (ELC), Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve IRS IT process and service efficiency and effectiveness.

10.8.1.1.5
(01-28-2025)
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 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 requirements checklists that have recently been revised or are in the process of being revised.
- (3) This policy delineates the security management structure, assigns responsibilities, and lays the foundation necessary to measure progress and compliance. The requirements within this policy are organized to follow the order in which security and privacy controls are presented within *NIST SP 800-53 Rev 5*.
- a. In an effort to reference the origin of a requirement (NIST, Treasury, etc.), a requirement may have its origin referenced in parenthesis at the end of the requirement; such as (CA-01), (AC-03_T.001), or (IRS-defined).
 - b. Use of the term "system" in this policy is expanded to include Cloud technology, Web 2.0, and successor technologies, and is applicable to all non-national security systems. (TD P 85-01, 1.3)

- (4) This IRM applies to all IRS information and systems, which store, process, or transmit IRS data or connect to an IRS network or system. 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.
- (5) Cybersecurity documents and publishes controls (IRM 10.8 series) for the IRS IT environment/resources.
 - a. Authorizing officials (AOs) are required to develop and maintain additional operational documentation (e.g., action and implementation plans, SOPs), necessary for implementation of the security controls delineated in the IRM 10.8 series.
 - b. The AO is responsible for implementation of security policy. These responsibilities include the documentation and procedures for how the systems are managed, administered, and monitored.
- (6) This IRM establishes the minimum baseline security policy and requirements for all IRS IT assets in order to:
 - a. Protect the critical infrastructure and assets of the IRS against attacks that exploit IRS assets.
 - b. Prevent unauthorized access to IRS assets.
 - c. Enable IRS IT computing environments to meet the requirements of this policy and support the business needs of the organization.

Note: IRM 10.8.1 applies to on-premises systems, including on-premises cloud models. For off-premises cloud models, refer to IRM 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy*.

10.8.1.1.6
(12-12-2023)

Terms and Acronyms

- (1) For the purpose of this IRM, the following terms apply:
 - a. IRS personnel or users, which includes:
 - Employees
 - Consultants
 - Detailees
 - Temporary employees
 - Interns
 - IRS contractors
 - Non-person entity (NPE) also referred to as robotic process automation (RPA), Bots, artificial intelligence (AI) workers, digital assistants, etc.
 - b. Authorized or Unauthorized personnel applies to all IRS personnel being authorized or not authorized to perform a particular action.
 - c. "Developers" or "application developers" refers to "program developers/programmers" and "web developers" as defined in IRM 10.8.2.

Note: The requirement in part "c" does not refer to database administrators (DBAs), who may assist developers.

- (2) Refer to Exhibit 10.8.1-1, Terms and Acronyms for a list of terms, acronyms, and definitions.

10.8.1.1.7
(12-12-2023)

Related Resources

- (1) Refer to Exhibit 10.8.1-2, Related Resources for a list of related resources and references.

10.8.1.2
(01-28-2025)

**Risk Acceptance and
Risk-Based Decisions
(RBDs)**

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

Note: Users can access RBD documentation in the FISMA Doc Library on the *Enterprise FISMA Compliance (EFC)* site.

10.8.1.2.1
(01-28-2025)

**Risk Acceptance
Request**

- (1) Security vulnerabilities can be discovered at any point in a system's lifecycle and by many different means. The most common actions that lead to the discovery of vulnerabilities are system configuration scans, penetration tests, vulnerability scans, and FISMA Control Assessment processes.
- (2) Acceptable reasons for an RBD are:
 - a. Meeting the requirement is technically not possible;
 - b. Meeting the requirement is cost prohibitive; and
 - c. Meeting the requirement is operationally not feasible and would cause an undue burden to the system and/or seriously hinder its capability to accomplish its mission.
- (3) An RBD must be documented in the pertinent system's security documentation (e.g., system security plan (SSP)).
 - a. The AO's decision to accept the risk associated with an identified vulnerability and not remediate it is required to be tracked (e.g., Online RBD tool).
 - b. The AO's decision to remediate the risk associated with an identified vulnerability, but the remediation cannot be performed within the timelines defined in the Remediation Timelines table in IRM 10.8.1.4.16.4.2 Vulnerability Remediation, must be documented in a plan of action and milestones (POA&M).

Note: The AO's decision guidance above aligns with CA-05 Plan of Action and Milestones, PL-11 Baseline Tailoring, RA-07 Risk Response, and *NIST SP 800-18 Rev 1, Guide for Developing Security Plans for Federal Information Systems*.

- (4) IRS RBDs are not permanent.
- (5) Prior to an RBD expiring, steps must be taken to either renew the RBD or implement mitigation to address the weakness.
 - a. If an RBD is dependent on a policy adjustment, the RBD must remain in effect until either the policy has been adjusted or the RBD expires (whichever comes first).
 - b. When an RBD expires, the requestor must be notified of the expiration.
- (6) Refer to the Cybersecurity Risk Acceptance - Risk Based Decision website for guidance on the RBD process (e.g., SOP, requirements, Business Entitlement Access Request System (BEARS) access, Online RBD, roles).

10.8.1.2.2
(01-28-2025)

Exceptions to Treasury Requirements

- (1) Per TD P 85-01 Appendix A, IRS-wide exceptions to Treasury requirements must be managed differently than adding or removing controls from the system (i.e., tailoring).
 - a. Documentation of exception requests to Treasury requirements must include operational justification, risk acceptance, and risk mitigation measures. Such requests must be submitted to and approved by the IRS CIO, in consultation with the IRS chief information security officer (CISO). An approved exception must be signed by the individuals in these roles and held by the IRS, with a copy submitted to the Treasury CIO via the Treasury CISO for review.
 - b. This exception policy applies to the following:
 - i. Treasury parameters within NIST controls;
 - ii. Treasury controls; and
 - iii. Treasury policy located within TD P 85-01.

10.8.1.3
(01-28-2025)

General Policy

- (1) In accordance with FISMA, the IRS must develop, document, and implement a service-wide information security program supporting the operations and assets of this agency.
 - a. Requirements contained within this IRM must not be grandfathered.
 - b. Requirements contained within this IRM must not be based on past practices.
- (2) Systems approved for the processing of classified information must not be connected to any system not approved for classified operation. Systems approved for classified processing must not share peripherals with unclassified processing equipment except for switching devices approved by the National Security Agency (NSA). Approval for the use of switching devices must be included in the security authorization documentation. Systems approved for the processing of classified information must be installed in certified Security Areas in accordance with IRM 10.9.1.
- (3) The IRS Information Security Program must:
 - a. Ensure the objectives of applicable laws, policies, federal regulations, OMB guidance, TDs, NIST Publications, and other regulatory guidance are met by establishing and ensuring compliance with security requirements, procedures, and guidelines to properly implement security controls.

Note: In situations where regulatory guidance has been released outside of the annual update cycle for IRS requirement documents, the requirements within the regulatory guidance will be met through the issuance of interim guidance.
 - b. Ensure that systems used by the IRS provide appropriate protection for the confidentiality, integrity, and availability of IRS information, through the use of security controls.
 - c. Implement policies, standards, and procedures which are consistent with government-wide policies, standards, and procedures issued by OMB, Department of Commerce, General Services Administration (GSA), Office of Personnel Management (OPM), and Department of the Treasury. Different or more stringent requirements for securing National Security Information (NSI) must be incorporated into agency programs as required by appropriate national security directives.

- d. Provide for the protection of critical infrastructure by identifying critical assets and individual, proprietary, financial, tax, mission critical, or otherwise sensitive information in accordance with *Executive Order (EO) 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*.
- e. Review each interdependency analysis and provide updates at least every three years or whenever there has been a significant change to the critical asset or an impact to its environment.
- f. Ensure the ability to maintain processing during and following an emergency.
- g. Ensure the auditability of all systems.
- h. Ensure management is responsible for designating the sensitivity of information, providing for the implementation of security controls, and certifying adequacy of these controls.
- i. Ensure management accountability for resources entrusted to them in accomplishing IRS objectives.
- j. Ensure individual accountability for the data, information, and other IT resources to which individuals have access.

Note: Implementation of the security controls defined within this IRM address the IRS Information Security Program requirements explicitly or implicitly.

- (4) The IRS information security program must include:
 - a. Risk assessments that consider internal and external threats to the confidentiality, integrity, and availability of systems and data supporting critical operations and assets.
 - b. Policies and procedures for risk assessments associated with the operations and assets for programs and systems to effectively reduce information security risks to an acceptable level while ensuring compliance with prescribed policies and procedures.
 - c. Security awareness training to inform personnel of information security risks, procedures designed to reduce such risks, and their personal impact/responsibilities for both.
 - d. Management of assessments and evaluation of the effectiveness of information security policies and procedures.
 - e. A process for ensuring remedial action is defined for addressing deficiencies.
 - f. Procedures for detecting, reporting, and responding to incidents; mitigation of risks associated with such incidents before substantial damage occurs; notification/consultation with appropriate law enforcement officials and other offices/authorities.
 - g. Appropriate reporting to proper authorities of weaknesses and remedial actions.
- (5) The IRS must implement the provisions of FISMA to include the guidelines outlined in NIST publications, OMB guidance, and FIPS.
- (6) All IRS systems that generate, store, process, transfer, display, or communicate non-national security information must be protected at a level commensurate with the potential impact of a loss of confidentiality, integrity, or availability on IRS operations, assets, or individuals.

- (7) Systems in a development and testing environment must adhere to the security requirements within this IRM based on an assessment of risk and the system's assigned *FIPS 199* categorization level.
 - a. Refer to IRM 10.8.1.4.16.2 RA-03 Risk Assessment and IRM 10.8.1.4.16.1 Security Categorization subsections within this IRM for guidance on conducting an assessment of risk and defining security categorization levels.
- (8) Unless approved by the CIO, the use of emerging technologies that have not been evaluated by the federal government for their national security impacts is prohibited due to the associated security challenges, lack of security solutions and high implementation cost. (*EO 13960 Sec 2 (c), Sec 3 (b); 44 USC 3551 Purposes (6)*)

Note: IRS Enterprise Architecture (EA) Enterprise Standards Profile (ESP) is the authoritative repository for IRS approved products and standards.

- (9) This IRM and all security policy IRMs (10.8 series) must be evaluated a minimum of annually to ensure consistency with the IRS mission, functions, and associated laws, directives, regulations, and standards.

Note: Implementation of the security controls defined within this IRM address the IRS information security program requirements explicitly or implicitly.

10.8.1.3.1
(01-28-2025)
**Zero Trust and Zero
Trust Architecture**

- (1) The IRS must: (*EO 14028, Sec. 3(b)*) (L, M, H)
 - a. Update existing agency plans to prioritize resources for the adoption and use of cloud technology as outlined in relevant OMB guidance;
 - b. Develop a plan to implement zero trust architecture (ZTA), which must:
 - i. Incorporate, as appropriate, the migration steps that NIST has outlined in standards and guidance (e.g., *NIST SP 800-207, Zero Trust Architecture*);
 - ii. Describe any such steps that have already been completed;
 - iii. Identify activities that will have the most immediate security impact; and
 - iv. Include a schedule to implement them.
 - v. Include submission of implementation plan to OMB and CISA for fiscal year (FY) 2022 - FY 2024 for OMB concurrence and a budget estimate for FY 2024. (*OMB M-22-09 (III)*) (L, M, H)
 - c. Provide a report to the Director of OMB and the Assistant to the President and National Security Advisor (APNSA) discussing the plans required pursuant to sub-parts (1)a. and (1)b. above.

Note: The implementation of zero trust (ZT) and ZTA is pending further guidance from the Department of the Treasury.

- (2) As the IRS continues to use cloud technology, they must do so in a coordinated, deliberate way that allows the Federal Government to prevent, detect, assess, and remediate cyber incidents. To facilitate this approach, the migration to cloud technology must adopt ZTA, as practicable. (*EO 14028, Sec. 3(c)*) (L, M, H)
- (3) The IRS must: (*EO 14028, Sec. 3(d)*) (L, M, H)

- a. Adopt multi-factor authentication (MFA) and encryption for data at rest and in transit, to the maximum extent consistent with federal records laws and other applicable laws.
- (4) Privileged access management (PAM) solutions must not be used as a general purposed substitute for MFA or for routine single-sign-on access to legacy systems in place of needed modernization of those systems. (*OMB M-22-09 (III)(A)(2)*) (L, M, H)

Note: When ZTA is not available for implementation, PAM solutions may be an iterative step that provides ephemeral single-factor credentials for human access to a system.

- a. The IRS must integrate and enforce MFA across applications involving authenticated access to Federal systems by IRS staff, contractors, and partners.
- b. Refer to IRM 10.8.1.4.7.4 IA-05 Authenticator Management for exceptions.
- (5) The IRS must work with the DotGov program at CISA to “preload” IRS-owned .gov domains as hypertext transport protocol secure (HTTPS)-only in web browsers. (*OMB M-22-09 (III)(C)(3)*)

Note: Because *OMB M-22-09* also requires that agencies preload their .gov domains in web browsers, agencies are expected to satisfy the hypertext transport protocol (HTTP) strict transport security (HSTS) requirements of *OMB M-15-13* through preloading, rather than applying distinct HSTS policies to individual services.

- (6) The IRS must operate dedicated application security testing programs. (*OMB M-22-09 (III)(D)(1)*)
- (7) The IRS must utilize high-quality firms specializing in application security for independent third-party evaluation. (*OMB M-22-09 (III)(D)(2)*)

Note: CISA and GSA will work together to make the services of such firms available for rapid procurement.

- (8) The IRS must work toward employing immutable workloads when deploying services, especially in cloud-based infrastructure. (*OMB M-22-09 (III)(D)(6)*)
- (9) Refer to *NIST SP 800-207* for guidance on ZTA. (L, M, H)

10.8.1.3.2
(12-12-2023)
Critical Software

- (1) The IRS must comply with OMB and NIST guidance outlining security measures for the procurement of critical software, software supply chain security, and software verification. (*EO 14028, Sec. 4(i)(j)*).
- (2) Refer to the *NIST EO 14028, Improving the Nation’s Cybersecurity* website for guidance. (L, M, H)

10.8.1.4
(01-28-2025)
**Security and Privacy
Controls,
Enhancements, and
Supplemental Guidance**

- (1) The controls within this policy provide a range of safeguards and countermeasures for the IRS and IRS systems. (L, M, H)
 - a. There may, on occasion, be redundancy in requirements that appear in the security controls and control enhancements within this IRM and potentially other subordinate IRMs. This overlap in requirements is intended to reinforce the security requirements from the perspective of multiple controls and/or enhancements.
- (2) To define a control baseline for IRS systems, designators are assigned to each requirement, 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 is 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.

Note: For 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)". This indicator is in place of the *FIPS 199* designators previously defined. (TD P 85-01, Appendix A)
 - i. The following apply for controls designated as Program-level requirements:
 1. Deployed IRS-wide;
 2. Support information security programs;
 3. Not associated with security control baselines; and
 4. Independent of any system impact level.
- c. Control families and controls supporting the IRS' Insider Threat Capability are identified with "InTC" throughout this policy.
- d. Control families and controls that are to be included as part of the privacy control baseline are identified with a "(P)" indicator.
- e. Systems designated as cyber critical infrastructure assets must implement controls identified as critical infrastructure protection (CIP) overlay controls. (TD P 85-01, Appendix A)
 - 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.

ii. CIP overlay controls within this IRM will be designated with CIP at the end of the requirement.

Note: CIP Overlay Controls may be tailored as long as the following criteria is met:

1. The 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; and
 2. The associated documentation for this risk-based decision not to implement is submitted for review to the Department Cyber CIP Program Manager and the Departmental CISO for review and approval.
- f. Systems designated as a high value asset (HVA) must implement security controls identified as HVA overlay controls. (TD P 85-01, Appendix A)
- i. HVA overlay controls within this IRM will be designated with HVA at the end of the requirement.
- g. Controls allocated to the privacy baseline (P) and a *FIPS 199* categorization (e.g., L, M, H, O) or Treasury overlay (e.g., CIP, HVA) are joint controls.
- h. Software designated as Critical Software and platforms hosting Critical Software must implement security controls identified as critical software (CSW) overlay controls. (NIST Security Measures for EO-Critical Software Use)
- i. CSW overlay controls within this IRM will be designated with CSW at the end of the requirement.

Note: Security controls identified as CSW align with the security measures defined by *NIST - Security Measures for EO-Critical Software Use*.

Indicator	Applicability
L	Applies to systems categorized as <i>FIPS 199</i> Impact-level LOW
M	Applies to systems categorized as <i>FIPS 199</i> Impact-level MEDIUM
H	Applies to systems categorized as <i>FIPS 199</i> Impact-level HIGH
CIP	Treasury Overlay - Applies to systems identified as cyber critical infrastructure assets
HVA	Treasury 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
-----	---

- (3) For a list of organizational common controls (OCC), contact SRM.
- (4) It is acceptable to configure settings to be more restrictive than those defined within this IRM.
- (5) To configure less restrictive requirements requires a risk-based decision. Refer to IRM 10.8.1.2 Risk Acceptance and Risk-Based Decisions for additional guidance.

10.8.1.4.1
(09-28-2021)
**AC-01 Access Control
Policy and Procedures**

- (4) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1, *Privacy and Information Protection, Privacy Policy*. (L, M, H)

10.8.1.4.1.1
(01-28-2025)
**AC-02 Account
Management**

#####

[illegible]

#

#

10.8.1.4.1.1.1
(01-28-2025)
**Business Role Account
Inactivity**

10.8.1.4.1.1.2
(07-08-2015)
Fire Call Account

#

10.8.1.4.1.1.3
(01-28-2025)
**Service Account
Requirements**

- (1) Service accounts must comply with the security requirements and guidance within this IRM: (IRS-defined) (L, M, H)

#

- (3) Refer to IRM 10.8.15, *Information Technology (IT) Security, General Platform Operating System Security Policy*, and applicable operating system checklist(s) for additional guidance. (L, M, H)

10.8.1.4.1.1.4
(01-28-2025)
**Non-Person Entity (NPE)
Account Requirements**

- (1) The IRS must manage the digital identity lifecycle of NPEs, ensuring the digital identity is distinguishable, auditable, and consistently managed across the IRS. (*OMB M-19-17*) (L, M, H)

#

- (2) NPE accounts must comply with the security requirements and guidance within this IRM. (IRS-defined) (L, M, H)

Access to Sensitive Information

- (1) Automated software mechanisms, such as negative taxpayer identification number (TIN) checking, must be implemented on systems that process, store, or transmit taxpayer data to ensure compliance with the Taxpayer Browsing Protection Act, 6103 of the IRC (*26 USC 6103*), and the IRM 11.3, *Disclosure of Official Information* series. (IRS-defined) (L, M, H)

#

#

#

- (3) The IRS must implement initial automation of data categorization and security responses, focusing on tagging and managing access to sensitive documents.
(OMB M-22-09 (III)(D)(5)) (L, M, H)
- (4) Refer to IRM 10.5.5, *Privacy and Information Protection, Unauthorized Access, Attempted Access or Inspection of Taxpayer Records (UNAX) Program Policy, Guidance and Requirements*, for Unauthorized Access (UNAX) guidance.

Access Authorization

#####

10.8.1.4.1.2
(01-28-2025)
**AC-03 Access
Enforcement**

#

- (4) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.1.3
(01-28-2025)
**AC-04 Information Flow
Enforcement**

#

10.8.1.4.1.4
(01-28-2025)
**AC-05 Separation of
Duties**

#

10.8.1.4.1.5
(12-13-2022)
**AC-06 Least Privilege
(InTC)**

[illegible]

#

##

#

#

#

#

#

#

#

- (5) The following IRS-approved System-use Notification Message or Banners must be used: (IRS-defined) (L, M, H)

- a. Non-publicly accessible systems – long text:

THIS U.S. GOVERNMENT SYSTEM IS FOR AUTHORIZED USE ONLY!

Use of this system constitutes consent to monitoring, interception, recording, reading, copying or capturing by authorized personnel of all activities. Unauthorized use of this system is prohibited and subject to criminal and civil penalties, including all penalties applicable to willful unauthorized access (UNAX) or inspection of taxpayer records (under 18 U.S.C. 1030 and 26 U.S.C. 7213A and 26 U.S.C. 7431).

- b. Non-publicly accessible systems – short text (when the long text cannot be used due to technical limitations):

THIS U.S. GOVERNMENT SYSTEM IS FOR AUTHORIZED USE ONLY!

Use is consent to authorized monitoring, capturing, etc., & all UNAX penalties apply.

- c. Publicly accessible systems:

THIS U.S. GOVERNMENT SYSTEM IS FOR AUTHORIZED USE ONLY!

Warning: By accessing and using this U.S. government computer system, you are consenting to system monitoring, interception, recording, reading, copying or capturing by authorized personnel of all activities, including detection and prevention of any unauthorized use of this system. The system you are accessing may contain confidential tax information and is designed exclusively for use by authorized persons to interact with the IRS and retrieve confidential tax information using only their own account. Any other use of this system that is inconsistent with the intended purposes of the system is an unauthorized use of the system and strictly prohibited.

Unauthorized use of this system is prohibited and subject to criminal and civil penalties, including, but not limited to, penalties applicable to knowingly or intentionally accessing a computer without authorization or exceeding authorized access as defined under 18 U.S.C. 1030, and as applicable, penalties for the willful unauthorized access or inspection of taxpayer records under 26 U.S.C. 7213A and 26 U.S.C. 7431.

#

[illegible]

10.8.1.4.1.10
(12-13-2022)
AC-11 Device Lock

		#
		#
10.8.1.4.1.11		#
(07-08-2015)		#
AC-12 Session Termination		#
		#
		#
		#
		#
		#
		#
		#
		#
		#
		#
		#
10.8.1.4.1.12	(1) NIST has withdrawn this control. (L, M, H)	
(12-23-2013)		
AC-13 (Withdrawn)		
10.8.1.4.1.13		#
(12-23-2013)		
AC-14 Permitted Actions without Identification or Authentication		#
		#
		#
		#
		#
10.8.1.4.1.14	(1) NIST has withdrawn this control. (L, M, H)	
(12-23-2013)		
AC-15 (Withdrawn)		
10.8.1.4.1.15		#
(12-23-2013)		#
AC-16 Security and Privacy Attributes		
10.8.1.4.1.16		#
(01-28-2025)		
AC-17 Remote Access		#
		#
		#
		#
		#
		#
		#
		#
		#
		#
		#

#

- (8) Refer to IRM 10.8.1.4.18.6.2 Network Protection and Design within this IRM for additional guidance related to remote access. (L, M, H)

10.8.1.4.1.17
(12-13-2022)

AC-18 Wireless Access

#

#

- (13) Refer to IRM 10.8.26, *Information Technology (IT) Security, Wireless and Mobile Device Security Policy*, and NIST SP 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs)*, for additional guidance on wireless security. (L, M, H)

10.8.1.4.1.18

(12-13-2022)

AC-19 Access Control for Mobile Devices

[illegible]

#####

10.8.1.4.1.18.1
(03-01-2024)
**Telecommunication
Devices**

#####

10.8.1.4.1.18.1

10.8.1.4.1.19
(12-13-2022)
**AC-20 Use of External
Systems**

[illegible]

**##

##**

10.8.1.4.1.19.1
(12-13-2022)
**Personally-Owned and
Other Non-Government
Furnished Equipment**

#

- (7) Refer to IRM 10.8.1.4.10.6 MP-07 Media Use within this IRM for additional guidance on personally owned media and devices. (L, M, H)
- (8) Refer to IRM 10.8.1.4.1.18.1 Telecommunication Devices within this IRM for additional guidance. (L, M, H)

10.8.1.4.1.20
(09-28-2021)
**AC-21 Information
Sharing**

#

10.8.1.4.1.21
(12-12-2023)
**AC-22 Publicly
Accessible Content**

#

10.8.1.4.1.22
(12-23-2013)
**AC-23 Data Mining
Protection**

#

#

#

[illegible]

- #####

[illegible]

#####

- 10.8.1.4.2.2
(01-28-2025)
**AT-03 Role-Based
Training**

#

#

#

#

#

#

#

#

- (5) Refer to IRM 10.8.2 for additional information on security roles that require specialized security training and the assigned hours, per Treasury. (L, M, H)
- (6) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1.

10.8.1.4.2.3
(09-28-2021)

AT-04 Training Records#

#

- (3) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1.

10.8.1.4.2.4
(12-23-2013)

AT-05 (Withdrawn)

- (1) NIST has withdrawn this control. (L, M, H)

10.8.1.4.2.5
(09-28-2021)

AT-06 Training Feedback#
#

10.8.1.4.3
(09-28-2021)

**AU-01 Audit and
Accountability Policy
and Procedures**#

#

- (3) The IRS must review and update its current audit and accountability policy and procedures every three years or if there is a significant change. (AU-01c) (P, L, M, H)

- (5) For procedures relating to the development of audit and accountability control requirements, visit the *Enterprise Security Audit Trails (ESAT)* website. (L, M, H)

- (6) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.3.1
(12-12-2023)

AU-02 Event Logging

10.8.1.4.3.5
(09-28-2021)
**AU-06 Audit Record
Review, Analysis, and
Reporting (InTC)**

[illegible]

#####

Cat. No. 49446Y (04-30-2025)
Any line marked with a #
is for **Official Use Only**

#

10.8.1.4.3.7
(01-28-2025)
AU-08 Time Stamps

#

#

10.8.1.4.3.8
(01-28-2025)
**AU-09 Protection of
Audit Information**

#

#

[illegible]

10.8.1.4.3.9
(09-28-2021)
**AU-10 Non-Repudiation
(InTC)**

10.8.1.4.3.10
(05-09-2019)
**AU-11 Audit Record
Retention**

- (2) Refer to the IRM 1.15 series for additional guidance. (L, M, H)
- (3) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.3.11
(12-13-2022)
**AU-12 Audit Record
Generation (InTC)**

#####

10.8.1.4.3.12
(12-13-2022)
**AU-13 Monitoring for
Information Disclosure
(InTC)**

10.8.1.4.3.13
(12-23-2013)
AU-14 Session Audit

##

10.8.1.4.3.14 (1) NIST has withdrawn this control. (L, M, H)
(09-28-2021)
AU-15 (Withdrawn)

10.8.1.4.3.15
(09-28-2021)
**AU-16 Cross-
Organizational Audit
Logging**

#

10.8.1.4.4
(12-13-2022)
**CA-01 Assessment,
Authorization, and
Monitoring Policy and
Procedures**

##

[illegible]

##

#

##

- [illegible]

Cat. No. 49446Y (04-30-2025)
Any line marked with a #
is for **Official Use Only**

#

10.8.1.4.4.2.1
(05-09-2019)
**Interconnection Security
Agreements**

#

- (7) ISAs must be developed in accordance with *NIST SP 800-47 Rev 1*. (IRS-defined) (L, M, H)

[illegible]

##

[illegible]

#####

- 10.8.1.4.4.5
(01-28-2025)
CA-06 Authorization

#

#

- (2) System authorizations must be in accordance with *NIST SP 800-37 Rev 2*. (NIST SP 800-37) (L, M, H)
- (3) The final authorization package(s) must consist of the following deliverables: (*NIST SP 800-37 Rev 2*) (L, M, H)
 - a. Security and Privacy Plans
 - b. Security and Privacy Assessment Reports
 - c. Any relevant POA&Ms
 - d. Executive Summary
 - e. Supporting assessment evidence or other documentation as requested by the AO
- (4) Refer to *NIST SP 800-18 Rev 1* for guidance on SSPs. (*NIST SP 800-37 Rev 2*) (L, M, H)
- (5) The Authorization Decision Document must contain the following: *NIST SP 800-37 Rev 2*) (L, M, H)
 - a. Authorizing Decision;
 - b. Terms and Conditions for the authorization;
 - c. Authorization termination date; and
 - d. Risk Executive (function) input (if provided) (i.e., Executive Summary of Risk).

#

- (8) The IRS must identify at least one internal-facing FISMA Moderate application and make it fully operational and accessible over the public internet, by January 26, 2023. (*OMB M-22-09 (III)(D)(4)*) (L, M, H)

- (9) For further information on system authorizations, refer to the *Cybersecurity* web site. (L, M, H)
- (10) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.4.5.1
(12-12-2023)
**FISMA Reporting
Requirements**

#

#

#

- (5) Refer to Cybersecurity EFC for further details related to all FISMA requirements within this subsection. (L, M, H)

10.8.1.4.4.6
(01-28-2025)
**CA-07 Continuous
Monitoring (InTC)**

##

[illegible]

#

#

- (8) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.4.6.1
(12-23-2013)

Compliance Monitoring

#

10.8.1.4.4.7
(09-28-2021)
**CA-08 Penetration
Testing**

#

#

##

#####

#

#####

#

- (4) Refer to IRM 2.150.2, *Configuration Management, Configuration Management (CM) Process*, for additional guidance. (L, M, H)
- (5) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.5.1
(12-13-2022)
CM-02 Baseline
Configuration

#

#

- 10.8.1.4.5.2
(01-28-2025)
**CM-03 Configuration
Change Control**

#####

#

##

10.8.1.4.5.3
(01-28-2025)
CM-04 Impact Analysis

[illegible]

- 10.8.1.4.5.4
(01-28-2025)
**CM-05 Access
Restrictions for Change**

10.8.1.4.5.6
(12-13-2022)
**CM-07 Least
Functionality**

#

[illegible]

10.8.1.4.5.7
(01-28-2025)
**CM-08 System
Component Inventory**

#

#####

- (12) The IRS must create reliable asset inventories through participation in CISA's CDM program. (OMB M-22-09 (III)(B)(1)) (L, M, H)

10.8.1.4.5.8
(09-28-2021)
**CM-09 Configuration
Management Plan**

[illegible]

10.8.1.4.5.9
(09-28-2021)
**CM-10 Software Usage
Restrictions**

#

[illegible]

10.8.1.4.6
(09-28-2021)
**CP-01 Contingency
Planning Policy and
Procedures**

##

- (5) Refer to IRM 10.8.60, *Information Technology (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance*, for guidance on Information System Contingency Plan (ISCP) and Disaster Recovery. (L, M, H)

10.8.1.4.6.1
(01-28-2025)

CP-02 Contingency Plan

[illegible]

#

##

10.8.1.4.6.1.1
(12-23-2013)
**Emergency Response
Capability**

- 10.8.1.4.6.2
(12-13-2022)
**CP-03 Contingency
Training**

#

#

#

10.8.1.4.6.3
(09-28-2021)
**CP-04 Contingency Plan
Testing**

#

- (6) Refer to IRM 10.8.62, *Information Technology (IT) Security, Information Systems Contingency Plan (ISCP) and Disaster Recovery (DR) Testing, Training, and Exercise (TT&E) Program*, for additional guidance. (L, M, H)

10.8.1.4.6.4
(12-23-2013)
CP-05 (Withdrawn)

- (1) NIST has withdrawn this control.

10.8.1.4.6.5
(09-28-2021)
CP-06 Alternate Storage Site

#

#

#

#####

#

#

#

10.8.1.4.6.6
(01-28-2025)
**CP-07 Alternate
Processing Site**

#

#

#

- (7) Refer to IRM 10.8.60 for additional guidance on an alternate processing site.
(L, M, H)

10.8.1.4.6.7
(09-28-2021)
CP-08
Telecommunications
Services

#

#

#

#

10.8.1.4.6.9
(12-13-2022)
**CP-10 System Recovery
and Reconstitution**

10.8.1.4.7.1
(01-28-2025)
**IA-02 Identification and
Authentication
(Organizational Users)**

#

#

- (9) Standards and guidelines for the HSPD-12 PIV card can be found in *FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors*. (L, M, H)

a. Refer to the IRM 10.2 series for additional guidance on HSPD-12.

- 10.8.1.4.7.2
(12-12-2023)
**IA-03 Device
Identification and
Authentication**

#####

- (2) When authorizing users to access resources, the IRS must consider at least one device-level signal alongside identity information about the authenticated user. (OMB M-22-09 (III)(A)(3)) (L, M, H)
- (3) To promote consistent and auditable identity practices, the IRS enterprise identity systems must also be capable of supporting human authentication through non-graphical user interfaces, such as scripts and command line tools. (OMB M-22-09 (III)(A)(1)) (L, M, H)
- (4) Multi-factor authentication must be enforced at the application layer, instead of the network layer. (OMB M-22-09 (III)(A)(2)) (L, M, H)

10.8.1.4.7.3
(12-13-2022)
**IA-04 Identifier
Management (InTC)**

#####

- 10.8.1.4.7.4
(01-28-2025)
**IA-05 Authenticator
Management**

[illegible]

[illegible]

#

[illegible][illegible]

10.8.1.4.7.5
(09-28-2021)
**IA-06 Authenticator
Feedback**

10.8.1.4.7.6
(09-28-2021)
**IA-07 Cryptographic
Module Authentication**

#####

10.8.1.4.7.7
(12-12-2023)
**IA-08 Identification and
Authentication
(Non-Organizational
Users)**

[illegible]

#

- (6) E-authentication must be used in accordance with *OMB M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, and E-Government Act of 2002, Section 208 (*Public Law 107-347, 44 USC Ch 36*). (L, M, H)
- (7) Multi-factor authentication must be enforced at the application layer, instead of the network layer. (*OMB M-22-09 (III)(A)(2)*) (L, M, H)
- (8) The IRS must require users to use a phishing-resistant method to access agency-hosted accounts. For routine self-service access by IRS staff, contractors, and partners, IRS systems must discontinue support for authentication methods that fail to resist phishing, including protocols that register phone numbers for short message service (SMS) or voice calls, supply one-time codes, or receive push notifications. (*OMB M-22-09 (III)(A)(2)*) (L, M, H)

Note: These users include employees, contractors, and enterprise users, such as a mission or business partners, as described in *OMB M-19-17*.

- (9) The IRS must ensure public-facing agency systems that support multi-factor authentication must give users the option of using phishing-resistant authentication by January 26, 2023. (*OMB M-22-09 (III)(A)(2)*) (L, M, H)

Note: The ability of the taxpayer to access public documents (i.e., Finding Forms, Instructions & Publications; Requesting Accessible Forms, Instructions & Publications; Reading eBooks; Reading Publications and Instructions online) does not require multi-factor authentication.

10.8.1.4.7.8
(12-23-2013)
**IA-09 Service
Identification and
Authentication**

#

#

#####

#

#####

#

#####

#

#

#

##

##

10.8.1.4.7.12
(01-28-2025)

IA-13 Identity Providers and Authorization Servers

(1) Identity Providers and Authorization Servers requirements have not been identified for inclusion into the IRS control baseline at this time. (L, M, H)

10.8.1.4.8
(09-28-2021)

IR-01 Incident Response Policy and Procedures

##

(4) Refer to the *IRS CSIRC Computer Security Incident Reporting Procedures* for additional policy and procedures related to incident response. (L, M, H)

- 10.8.1.4.8.1
(01-28-2025)
**IR-02 Incident Response
Training**

#

#

#

- 10.8.1.4.8.2
(09-28-2021)
**IR-03 Incident Response
Testing**

#####

##

- (3) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.8.3
(01-28-2025)
**IR-04 Incident Handling
(InTC)**

[illegible]

#

- (8) For additional incident handling guidance refer to the *IRS CSIRC organization's Computer Security Incident Reporting Procedures*. (L, M, H)
- (9) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.8.4
(01-28-2025)
**IR-05 Incident
Monitoring**

[illegible]

- (3) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.8.5
(12-12-2023)
IR-06 Incident Reporting

#

[illegible]

[illegible]

#####

- (3) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

#

##

- 10.8.1.4.9.1
(01-28-2025)
**MA-02 Controlled
Maintenance**

[illegible]

10.8.1.4.9.3
(12-13-2022)
**MA-04 Non-Local
Maintenance**

#

10.8.1.4.9.4
(12-13-2022)
**MA-05 Maintenance
Personnel**

[illegible]

- (3) Refer to IRM 10.23.2, *Personal Security, Contractor Investigations* and IRM 10.2 series for additional guidance. (L, M, H)

10.8.1.4.9.5
(12-23-2013)
**MA-06 Timely
Maintenance**

##

#[illegible]

- #

#

##

#

##

#

10.8.1.4.10.3
(01-28-2025)
MP-04 Media Storage

#

- (3) SBU information must not be downloaded and/or remotely stored prior to receiving documented approval from the system AO. (IRS-defined) (L, M, H)

10.8.1.4.10.3.1
(01-28-2025)
**Portable Electronic
Devices (PEDs) as
Storage Media**

#

#

- 10.8.1.4.10.4
(01-28-2025)
MP-05 Media Transport

[illegible]

#

- (3) Refer to TD P 15-71, *Treasury Security Manual*, for additional guidance on transportation of media. (L, M, H)

10.8.1.4.10.5

(01-28-2025)

MP-06 Media**Sanitization**

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

- (2) Sanitization must be conducted in accordance with *NIST SP 800-88 Rev 1*. (L, M, H)

- a. IRS must use sanitization tools and products evaluated and approved by either NSA, DHS, or Department of Defense (DoD).
- b. For a list of approved NSA evaluated media destruction products refer to <https://www.nsa.gov/resources/Media-Destruction-Guidance>.

#

#

#

[illegible]

[illegible]

#

- (15) For additional guidance on media redaction before release, contact the Office of Disclosure *Office of Disclosure*. (L, M, H)
- (16) Refer to *NIST SP 800-88 Rev 1* for additional guidance. (L, M, H)
- (17) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.10.6
(01-28-2025)
MP-07 Media Use (InTC)

#

[illegible]

Portable Electronic Devices (PEDs)

- (1) Refer to IRM 10.8.26 for additional guidance on wireless capabilities within PEDs. (L, M, H)
- (2) Refer to IRM 10.8.26 for additional guidance on mobile computing devices. (L, M, H)

#

##

#####

##

- (3) Refer to the IRM 10.2 series for additional guidance on physical access, and employee and contractor identification requirements. (L, M, H)

#

11

#

#

#

#

#

#

#

#

#

#

#

π
#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

"

#

##

##

#

#

10.8.1.4.11.6 (1) NIST has withdrawn this control. (L, M, H)
(12-23-2013)
PE-07 (Withdrawn)

10.8.1.4.11.7
(01-28-2025)
**PE-08 Visitor Access
Records**

#

[illegible]

- 10.8.1.4.11.8
(09-28-2021)
**PE-09 Power Equipment
and Cabling**

- 10.8.1.4.11.9
(01-28-2025)
**PE-10 Emergency
Shutoff**

- 10.8.1.4.11.10
(09-28-2021)
PE-11 Emergency Power

#

10.8.1.4.11.11
(09-28-2021)
**PE-12 Emergency
Lighting**

#

10.8.1.4.11.12
(12-13-2022)
PE-13 Fire Protection

#

#

#

##

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

#####

#

#

##

10.8.1.4.11.17
(09-28-2021)
**PE-18 Location of
System Components**

##

10.8.1.4.11.18
(12-23-2013)
**PE-19 Information
Leakage**

#

10.8.1.4.11.19
(12-23-2013)
**PE-20 Asset Monitoring
and Tracking**

#

10.8.1.4.11.20
(09-28-2021)
**PE-21 Electromagnetic
Pulse Protection**

#

10.8.1.4.11.21
(09-28-2021)
**PE-22 Component
Marking**

#

10.8.1.4.11.22
(09-28-2021)
PE-23 Facility Location

#

##

- #
#

[illegible]

#

- (7) System security and privacy plans must be retained in accordance with Document 12829, GRS 3.2, Item 010 - Destroy 1 year(s) after the system is superseded by a new iteration or when no longer needed for agency/IT administrative purposes to ensure a continuity of security controls throughout the life of the system. (Document 12829)
- (8) Refer to *NIST SP 800-18 Rev 1* for guidance on security planning. (L, M, H)

[illegible]

#####

- 10.8.1.4.12.8
(09-28-2021)
**PL-09 Central
Management**

**#

#**

#

//

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

"

#

#

#

#

#

#

#

#

#

#

##

- (1) FISMA, PRIVACT, and OMB Circular No. A-130, Management Information as a Strategic Resource require federal agencies to develop, implement, and provide oversight for organization-wide information security and privacy programs to help ensure the confidentiality, integrity, and availability of federal information processed, stored, and transmitted by federal systems and to protect individual privacy. (*NIST SP 800-53*) (P)
 - a. The Program Management (PM) controls described in this subsection are implemented at the organization level and not directed at individual systems.
 - b. The PM controls have been designed to facilitate organizational compliance with applicable federal laws, executive orders, directives, policies, regulations, and standards.
 - c. The PM controls are independent of any *FIPS 199* impact levels and therefore, are not associated with the security control baselines described in *NIST SP 800-53B*.
 - d. Organizations document PM controls in the information security and privacy program plans.
 - i. The organization-wide information security program plan (refer to IRM 10.8.1.4.13.1 PM-01 Information Security Program Plan) and privacy program plan (refer to IRM 10.8.1.4.13.18 PM-18 Privacy Program Plan) supplement security and privacy plans (refer to IRM 10.8.1.4.12.1 PL-02 System Security and Privacy Plans) developed for organizational systems.
 - ii. Together, the system security and privacy plans for the individual systems and the information security and privacy program plans cover the totality of security and privacy controls employed by the organization.

#####

[illegible]

10.8.1.4.13.2
(09-28-2021)
**PM-02 Information
Security Program
Leadership Role**

##

#

#

- (6) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

#####

##

- (3) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.13.5
(12-12-2023)
PM-05 System Inventory

#

Note: Software includes firmware, operating systems, applications, and application services (e.g., cloud-based software), as well as products containing software.

- b. Refer to IRM 10.8.1.4.20 Supply Chain Risk Management Policy and Procedures within this IRM for additional guidance on software and software attestation (IRS-defined)

#

- (9) The IRS must designate a cryptographic inventory and migration lead by December 18, 2022, in accordance with *OMB M-23-02*, Migrating to Post-Quantum Cryptography. (*OMB M-23-02*) (O)

Note: The Office of the National Cyber Director (ONCD), in coordination with OMB, CISA, and the FedRAMP Program Management Office (PMO), will release instructions for the collection and transmission of inventories of cryptographic systems by February 16, 2023.

- (10) The IRS must inventory all currently deployed information systems and assets that contain cryptanalytically relevant quantum computer (CRQC)-vulnerable cryptographic systems and submit this inventory to ONCD and CISA by May 4, 2023, and annually thereafter: (*OMB M-23-02*) (O).
 - a. Including systems and assets deployed by the IRS or on behalf of the IRS, and
 - b. Including high impact systems, and
 - c. Including HVAs, and
 - d. Including systems or assets that:
 - i. Contain data expected to remain mission-sensitive in 2035; or
 - ii. Are logical access control systems based in asymmetric encryption (such as PKI) that use any of the algorithms:
 - Elliptic Curve Diffie-Hellman (ECDH) Key Exchange
 - Menezes-Qu-Vanstone (MQV) Key Exchange
 - Elliptic Curve Digital Signature Algorithm (ECDSA)
 - Diffie-Hellman (DH) Key Exchange
 - RSA Signature Algorithm
 - Digital Signature Algorithm
 - Other non-PQC Asymmetric Algorithm (not enumerated in the list above)

- 10.8.1.4.13.6
(12-12-2023)
PM-06 Measures of Performance

#

#

#

- (3) As directed by *EO 14028*, the IRS must formalize their participation in CDM via a memorandum of agreement with DHS. (*OMB M-22-09 (III) (B) (1)*) (L, M, H)
- (4) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.13.7
(01-28-2025)
**PM-07 Enterprise
Architecture**

#####

#

- (5) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.13.8
(12-13-2022)
PM-08 Critical
Infrastructure Plan

- ##

##

[illegible]

- (2) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.13.10
(09-28-2021)
**PM-10 Authorization
Process**

#

- (2) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

- #

#

#

#

#

#

#

#

#

#

#

#

#

#

#

##

10.8.1.4.13.12.1
(09-28-2021)
**IRS Insider Threat
Capability (InTC)**

##

##

- (3) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.13.15
(09-28-2021)
**PM-15 Security and
Privacy Groups and
Associations**

##

10.8.1.4.13.16
(09-28-2021)
**PM-16 Threat Awareness
Program (InTC)**

#

#####

(2) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

#

[illegible]

- 10.8.1.4.13.19
(09-28-2021)
**PM-19 Privacy Program
Leadership Role**

##

- ##

##

#####

- (2) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

#

#

"

#

#

#

#

#

#

#

#

#

#

#

#

11

#

#

#

#

#

π
#

#

#

#

#

#####

- 10.8.1.4.13.23
(09-28-2021)
**PM-23 Data Governance
Body**

#####

10.8.1.4.13.24
(09-28-2021)
**PM-24 Data Integrity
Board**

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


##

- (2) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.13.25
(12-13-2022)

PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research

#

- (2) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.13.26
(01-28-2025)

PM-26 Complaint Management

##

- #####

- [illegible]

#####

- | | | |
|-----------------------|-------------------------|---|
| 10.8.1.4.13.31 | Internal Revenue Manual | Cat. No. 49446Y (04-30-2025)
Any line marked with a #
is for Official Use Only |
|-----------------------|-------------------------|---|

10.8.1.4.13.32
(09-28-2021)
PM-32 Purposing

##

10.8.1.4.14
(09-28-2021)
**PS-01 Personnel
Security Policy and
Procedures**

[illegible]

10.8.1.4.14.1
(09-28-2021)
**PS-02 Position Risk
Designation**

##

#

- (2) Refer to IRM 10.8.2 for additional guidance on roles with IT security responsibilities. (L, M, H)

10.8.1.4.14.2
(12-13-2022)
**PS-03 Personnel
Screening (InTC)**

#

10.8.1.4.14.3
(01-28-2025)
PS-04 Personnel
Termination (InTC)

#

10.8.1.4.14.4
(01-28-2025)
PS-05 Personnel
Transfer (InTC)

#

#

- 10.8.1.4.14.8
(09-28-2021)
**PS-09 Position
Descriptions**

##

#####

##

- Federal tax information (FTI), PII, protected health information (PHI), certain procurement information, system vulnerabilities, case selection methodologies, systems information, enforcement procedures, investigation information.
 - Live data, which is defined as production data in use. Live means that when changing the data, it changes in production. The data may be extracted for testing, development, etc., in which case, it is no longer live. Live data often contains SBU.
- (2) Examples of non-PII SBU information that is protected by statute includes (but is not limited to): (PGLD) (L, M, H)
- 26 USC 6103 protected tax returns of corporations (contains corporate entity information).
 - 31 USC Bank Secrecy Act protected reports filed by financial institutions (includes some information that is not PII).
 - 18 USC Grand Jury Information protected by Rule 6(e) of the Federal Rules of Criminal Procedure.
 - 18 USC 1905 Information protected under the Trade Secrets Act for entities (trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association; or permits any income return or copy thereof or any book containing any abstract or particulars thereof to be seen or examined by any person except as provided by law).
 - IP addresses dynamically assigned to assets (e.g., dynamic host configuration protocol (DHCP)).
- (3) Refer to IRM 10.5.1 and the *PGLD* website for additional guidance on SBU or PII protection. (L, M, H)

10.8.1.4.16.1.2
(05-09-2019)

**Controlled Unclassified
Information (CUI)**

- (1) *Presidential EO 13556 of November 4, 2020*, establishes an open and uniform program for managing information that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Government-wide policies. Within the Order, it: (L, M, H)
- Adopts, defines, and institutes CUI categories as the exclusive designations for all unclassified information referred to as SBU in the Information Sharing Environment (ISE).
 - Establishes a corresponding new CUI Program for designating, marking, safeguarding, and disseminating information designated as CUI.
 - Designates the NARA as the Executive Agent, to oversee and implement the new CUI Program.
- (2) Per NARA Controlled Unclassified Information (CUI): Initial Implementation Guidance for *EO 13556*, Agency heads (i.e., IRS Commissioner) must perform the following: (L, M, H)
- a. Establish and manage an agency CUI program that develops and implements agency procedures, roles, and responsibilities regarding CUI in accordance with the Order and the CUI implementation guidance.
 - b. Provide for required training for affected personnel regarding implementation and maintenance of the IRS' CUI program in accordance with the CUI implementation guidance.

- c. Create a self-inspection program to ensure compliance with the Order and the CUI implementation guidance.
- d. Designate a senior agency official to assist the agency head in CUI implementation and ensure compliance with the Order and the CUI implementation guidance.

10.8.1.4.16.1.3

(04-30-2025)

Personally Identifiable Information (PII)

- (1) PII is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. (OMB Circular A-130) (L, M, H)
- (2) PII is any information about an individual maintained by an agency, including: (*NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*; *OMB M-10-22, Guidance for Online Use of Web Measurement and Customization Technologies*) (L, M, H)
 - a. Information that can be used to distinguish or trace an individual's identity, such as name, SSN, date and place of birth, mother's maiden name, or biometric records.
 - i. To distinguish an individual is to identify an individual such as SSN and Passport Number. However, a list of credit scores without any other information concerning the individual does not distinguish the individual.
 - ii. To trace an individual is to process sufficient information to make a determination about a specific aspect of an individual's activities or status, for example an audit log.
 - b. Information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
 - i. Linked information is information about or related to an individual that is logically associated with other information about the individual.
 - ii. Linkable information is information about or related to an individual for which there is a possibility of logical association with other information about the individual.

Note: The definition of PII is not anchored to any single category of information or technology. Rather, it demands a case-by-case assessment of the specific risk that an individual can be identified.

- (3) The following are examples of PII: (NIST SP 800-122) (L, M, H)
 - Personal characteristics (height; weight; sex; date and place of birth; age; hair color; eye color; race; ethnicity; scars; tattoos; gang affiliation; religious affiliation; mother's maiden name; distinguishing features; and biometric information such as fingerprints, DNA, and retinal scans).
 - A unique set of numbers or characters assigned to a specific individual (name; address; phone number; SSN; SEID; email or IP address; driver's license number; financial account or credit card number; and Automated Integrated Fingerprint Identification System (AIFIS) identifier, booking, or detention system number).
 - Descriptions of events or times (information in documents such as police reports, arrest reports, and medical records).
 - Descriptions of locations, such as Geographic Information System (GIS), electronic bracelet monitoring information, etc.
 - Name, such as full name, maiden name, mother's maiden name, or alias.

Internal Revenue Manual

- Cat. No. 49446Y (04-30-2025)
Any line marked with a #
is for **Official Use Only**

[illegible]

#

#

#

#

#

10.8.1.4.16.4.2
(01-28-2025)
**Vulnerability
Remediation**

#

#

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

10.8.1.4.16.5
(12-23-2013)
**RA-06 Technical
Surveillance
Countermeasures
Survey**

10.8.1.4.16.6
(09-28-2021)
RA-07 Risk Response

- (2) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.16.7

(09-28-2021)

RA-08 Privacy Impact Assessments

- (2) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.16.8

(12-13-2022)

RA-09 Criticality Analysis

10.8.1.4.16.9

(12-12-2023)

RA-10 Threat Hunting

10.8.1.4.17
(01-28-2025)

**SA-01 System and
Services Acquisition
Policy and Procedures**

#

- (2) The IRS must designate an official to manage the development, documentation, and dissemination of the system and services acquisition policy and procedures. (SA-01b) (P, L, M, H)
- (3) The IRS must review and update its current system and services acquisition policy and procedures every three years or if there is a significant change. (SA-01c) (P, L, M, H)
- (4) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.17.1
(09-28-2021)

**SA-02 Allocation of
Resources**

#

- (2) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.17.2
(09-28-2021)

**SA-03 System
Development Life Cycle
(SDLC)**

#

- (2) Refer to IRM 2.31.1, *Lifecycle Management, One Solution Delivery Life Cycle (OneSDLC) Guidance* and the *Enterprise Life Cycle Program Office* site for guidance on the ELC process. (L, M, H)
- (3) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.17.3

(01-28-2025)

**SA-04 Acquisition
Process**

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


##

#####

#

##

- (15) Refer to IRM 10.8.1.4.20 Supply Chain Risk Management Policy and Procedures within this IRM for additional guidance on software and software attestation. (L, M, H)
- (16) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.17.4
(01-28-2025)
**SA-05 System
Documentation**

#

##

- 10.8.1.4.17.8
(01-28-2025)
**SA-09 External System
Services**

#

#

- (5) Refer to IRM 11.3.24, *Disclosure of Official Information, Disclosures to Contractors*, for additional guidance. (L, M, H)
- (6) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.17.9
(09-28-2021)
**SA-10 Developer
Configuration
Management**

#

- (3) Refer to IRM 2.5, *Systems Development* series for additional guidance on system development. (L, M, H)

#####

- c. Identify opportunities for IPv6 pilots and complete at least one pilot of an IPv6-only operational system by the end of FY 2021 and report the results of the pilot to OMB, upon request;
 - d. Develop an IPv6 implementation plan by the end of FY 2021 that describes the transition plan and includes the following milestones and actions:
 - i. At least 20% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2023;
 - ii. At least 50% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2024;
 - iii. At least 80% of IP-enabled assets on Federal networks are operating in IPv6-only environments by the end of FY 2025; and
 - iv. Identify and justify Federal systems that cannot be converted to use IPv6 and provide a schedule for replacing or retiring these systems;
 - e. Update the Information Resources Management Strategic Plan as appropriate, to update all networked Federal systems (and the IP-enabled assets associated with these systems) to fully enable native IPv6 operation;
 - f. Work with external partners to identify systems that interface with networked Federal systems and develop plans to migrate all such network interfaces to the use of IPv6;
 - g. Complete the upgrade of public/external facing servers and services (e.g., web, email, domain name system (DNS), and internet service provider (ISP) services) and internal client applications that communicate with public internet services and supporting enterprise networks to operationally use native IPv6;
 - h. Ensure that plans for full support for production IPv6 services are included in IT security plans, architectures and acquisitions;
 - i. Ensure that all systems that support network operations or enterprise security services (e.g., IAM systems, firewalls and intrusion detection / protection systems, end-point security systems, security incident and event management systems, access control and policy enforcement systems, threat intelligence and reputation systems) are IPv6-capable and can operate in IPv6-only environments;
 - j. Follow applicable Federal guidance and leverage industry best practices, as appropriate, for the secure deployment and operation of IPv6 networks; and
 - k. Ensure that all security and privacy policy assessment, authorization and monitoring processes fully address the production use of IPv6 in Federal systems.
- (5) The following Federal IPv6 acquisition requirements must be applied: (*OMB M-21-07*) (L, M, H)
- a. Use the USGv6 Profile to define agency or acquisition specific requirements for IPv6 capabilities when purchasing networked information technology and services;
 - b. Require potential vendors to document compliance with such IPv6 requirement statements through the USGv6 Test Program; and
 - c. Provide a process for the CIO to waive the requirement to demonstrate IPv6 capabilities on a case-by-case basis.
- (6) To avoid any unnecessary duplication of generic testing requirements, the following IPv6 requirements must be applied: (*OMB M-21-07*) (L, M, H)

- a. Leverage the USGv6 Test Program for basic conformance and general interoperability testing of commercial products; and
- b. Ensure that agency or acquisition specific testing focus on specific systems integration, performance and information assurance testing not covered in the USGv6 Test Program.

10.8.1.4.18.1
(12-13-2022)
**SC-02 Separation of
System and User
Functionality**

#

10.8.1.4.18.2
(09-28-2021)
**SC-03 Security Function
Isolation**

#

10.8.1.4.18.3
(09-28-2021)
**SC-04 Information in
Shared System
Resources**

#

#

10.8.1.4.18.4

(01-28-2025)

**SC-05 Denial of Service
Protection**#

#

- (2) Refer to *NIST SP 800-61* and CISA for additional guidance on the types of DoS attacks. (L, M, H)

10.8.1.4.18.5

(12-23-2013)

**SC-06 Resource
Availability**#
#

10.8.1.4.18.6

(01-28-2025)

**SC-07 Boundary
Protection (InTC)**#

#

[illegible]

[illegible]

[illegible]

[illegible]

#

#

- (30) Refer to IRM 10.8.54, *Information Technology (IT) Security, Minimum Firewall Administration Requirements*, for additional guidance on firewalls. (L, M, H)
- (31) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.18.6.1
(01-28-2025)

Internet Security

- (1) Refer to IRM 2.25, *Integrated Enterprise Portal - Web Services* series, for guidance related to internet security. (L, M, H)

10.8.1.4.18.6.2
(01-28-2025)

Network Protection and Design

#

10.8.1.4.18.7
(12-13-2022)

SC-08 Transmission Confidentiality and Integrity

#

#

10.8.1.4.18.8 (1) NIST has withdrawn this control. (L, M, H)
(12-23-2013)
SC-09 (Withdrawn)

10.8.1.4.18.9
(01-28-2025)
**SC-10 Network
Disconnect**

##

##

##

10.8.1.4.18.10
(12-23-2013)
SC-11 Trusted Path

#

10.8.1.4.18.11
(01-28-2025)
**SC-12 Cryptographic
Key Establishment and
Management**

#

#

#

	#
	#
	#
10.8.1.4.18.12	#
(01-28-2025)	
SC-13 Cryptographic Protection	#
	#
	#
	#
	#
	#
	#
	#
	#
	#
	#
	#
	#
	#

- (2) All cryptographic implementations must use FIPS-validated encryption. (*NIST FIPS 140*) (L, M, H)
- (3) IRS servers must be configured to use TLS 1.2 and support TLS 1.3: (*NIST SP 800-52 Rev 2; OMB M-22-09 (III)(C)(1)*) (L, M, H)

Note: If interoperability permits, TLS 1.3 is preferred.

- a. TLS 1.1 or older must not be supported.

b. TLS must be implemented in accordance with *NIST SP 800-52 Rev 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*.
- (4) Refer to the following NIST websites, for additional guidance on FIPS-validated cryptographic modules: (L, M, H)
- <https://csrc.nist.gov/publications/PubsFIPS.html>

• <https://csrc.nist.gov/groups/STM/cmvp>

10.8.1.4.18.12.1	#
(07-08-2015)	#
Public Key/Private Key	#
	#
	#
	#
	#
	#

10.8.1.4.18.13 (1) NIST has withdrawn this control. (L, M, H)
(12-23-2013)

SC-14 (Withdrawn)

10.8.1.4.18.14
(09-28-2021)

**SC-15 Collaborative
Computing Devices and
Applications**

10.8.1.4.18.14.1
(01-28-2025)

**Collaborative
Technology and
Systems**

- (3) Refer to IRM 10.8.1.4.18.12 Cryptographic Protection and IRM 10.8.1.4.16.1.1 Sensitive But Unclassified (SBU) Information within this IRM for additional guidance. (L, M, H)

10.8.1.4.18.14.1.1
(12-13-2022)
**Internal Collaborative
Technology and
Systems (e.g.,
SharePoint, Centra)**

[illegible]

- (7) In addition to the requirements within this subsection, internal collaborative sites must also adhere to the requirements in IRM 10.8.1.4.18.14.1 Collaborative Technology and Systems within this IRM. (L, M, H)
- (8) Refer to IRM 10.8.22, *Information Technology (IT) Security, Web Server Security Policy* for additional guidance on SharePoint security requirements. (L, M, H)

10.8.1.4.18.14.1.2

(05-09-2019)

External Collaborative Technology and Systems

[illegible]

- (2) In addition to the requirements within this subsection, external collaborative sites must also adhere to the requirements in the IRM 10.8.1.4.18.14.1 Collaborative Technology and Systems subsection within this IRM. (L, M, H)

10.8.1.4.18.15

(09-28-2021)

**SC-16 Transmission of
Security and Privacy
Attributes**

#

#

10.8.1.4.18.16

(01-28-2025)

**SC-17 Public Key
Infrastructure (PKI)
Certificates**

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

- (3) PKI certificate transaction related records must be retained in accordance with Document 12839, GRS 3.2, Item 062 - Destroy/delete when seven years six months to 20 years six months old, based on the maximum level of operation of the appropriate CA and after the information record the PKI is designed to protect and/or access is destroyed according to an authorized schedule. (Document 12839)

- (4) Refer to IRM 10.8.52 for additional guidance. (L, M, H)

10.8.1.4.18.17

(01-28-2025)

SC-18 Mobile Code

#

#

#

#

#

#

#

#

#

##

- (2) If necessary, a formal request for a risk-based decision can be submitted in accordance with the process described in IRM 10.8.1.2 Risk Acceptance and Risk-Based Decisions within this IRM. (L, M, H)
- (3) Refer to *NIST SP 800-28 Ver 2, Guidelines on Active Content and Mobile Code*, for additional guidance. (L, M, H)

10.8.1.4.18.18
(09-28-2021)
SC-19 (Withdrawn)

- (1) NIST has withdrawn this control. (L, M, H)

10.8.1.4.18.19
(01-28-2025)
**SC-20 Secure
Name/Address
Resolution Service
(Authoritative Source)**

[illegible]

#

- (4) The IRS must provide any non-.gov domains, including hostnames used by internet-accessible information systems, used by the IRS to CISA and GSA, by March 27, 2022. (*OMB M-22-09 (III)(D)(5)*; *OMB M-23-10*) (L, M, H)
- (5) The IRS must use government domains (i.e., .gov or .mil) for all official communications, information, and services. (*OMB M-23-10*) (L, M, H)

Note: This requirement does not apply to third-party services operated by non-governmental entities on non-governmental domains that are needed to effectively interact with the public. Examples of such third-party services include social media services, source code collaboration, and vulnerability disclosure reporting systems.

- (6) The IRS must comply with all applicable “.gov” domain requirements on the “.gov” Registry’s website, by August 7, 2023. (*OMB M-23-10*) (L, M, H)
 - a. Previously registered domains must be reviewed. Any domains that do not meet Registry’s requirements must be identified to OMB.
 - b. To register or renew a .gov domain, the IRS must follow the process and the domain name requirements for Federal agencies on the .gov Registry’s site. Domain name requests must have the approval of the CIO.

Note: All questions or inquiries concerning *OMB M-23-10* should be addressed to the OMB Office of the Federal Chief Information Officer (OFCIO) via email: ofcio@omb.eop.gov. For management of current domains and other issues, address via email the .gov Registry at dotgov@cisa.dhs.gov.

#

- (8) Refer to IRM 10.8.5, *Information Technology (IT) Security, Domain Name System (DNS) Security Policy*, for additional guidance. (L, M, H)

10.8.1.4.18.20

(09-28-2021)

SC-21 Secure**Name/Address****Resolution Service****(Recursive or Caching****Resolver)**#

#

10.8.1.4.18.21

(09-28-2021)

SC-22 Architecture and**Provisioning for****Name/Address****Resolution Service**#

#

10.8.1.4.18.22

(09-28-2021)

SC-23 Session**Authenticity**#

#

10.8.1.4.18.23

(09-28-2021)

SC-24 Fail in Known**State**#

#

[illegible]

- (3) Per *OMB Circular No. A-130*, Appendix I, 4(i)(14): “All NIST FIPS Publication 199 moderate-impact and high-impact information must be encrypted at rest and in transit, unless encrypting such information is technically infeasible or would demonstrably affect the ability of agencies to carry out their respective missions, functions, or operations; and the risk of not encrypting is accepted by the AO and approved by the IRS CIO, in consultation with the SAOP.” (M, H)

10.8.1.4.18.28

(12-23-2013)

SC-29 Heterogeneity

#

#

10.8.1.4.18.29

(12-23-2013)

**SC-30 Concealment and
Misdirection**

#

#

10.8.1.4.18.30

(12-23-2013)

**SC-31 Covert Channel
Analysis**

#

#

10.8.1.4.18.31

(09-28-2021)

**SC-32 System
Partitioning**

#

#

10.8.1.4.18.32

(12-23-2013)

SC-33 (Withdrawn)

- (1) NIST has withdrawn this control. (L, M, H)

10.8.1.4.18.33

(12-23-2013)

**SC-34 Non-Modifiable
Executable Programs**

#

#

10.8.1.4.18.34

(09-28-2021)

**SC-35 External Malicious
Code Identification**

#

#

10.8.1.4.18.35

(12-23-2013)

**SC-36 Distributed
Processing and Storage**

#

#

10.8.1.4.18.36

(09-28-2021)

**SC-37 Out-of-Band
Channels**

#

#

#

#

#####

10.8.1.4.18.37
(05-09-2019)
**SC-38 Operations
Security (InTC)**

#

10.8.1.4.18.38
(09-28-2021)
SC-39 Process Isolation

##

10.8.1.4.18.39
(12-23-2013)
**SC-40 Wireless Link
Protection**

#

10.8.1.4.18.40
(07-08-2015)
**SC-41 Port and I/O
Device Access**

#

10.8.1.4.18.41 (09-28-2021) SC-42 Sensor Capability and Data		# #
10.8.1.4.18.42 (12-23-2013) SC-43 Usage Restrictions		# #
10.8.1.4.18.43 (12-23-2013) SC-44 Detonation Chambers		# #
10.8.1.4.18.44 (01-28-2025) SC-45 System Time Synchronization	(1) System Time Synchronization requirements have not been identified for inclusion into the IRS control baseline at this time. (L, M, H)	
10.8.1.4.18.45 (09-28-2021) SC-46 Cross Domain Policy Enforcement		# #
10.8.1.4.18.46 (09-28-2021) SC-47 Alternate Communications Paths		# #
10.8.1.4.18.47 (09-28-2021) SC-48 Sensor Relocation		# #
10.8.1.4.18.48 (09-28-2021) SC-49 Hardware- Enforced Separation and Policy Enforcement		# # #
10.8.1.4.18.49 (09-28-2021) SC-50 Software- Enforced Separation and Policy Enforcement		# # #
10.8.1.4.18.50 (09-28-2021) SC-51 Hardware-Based Protection		# #

[illegible]

- #####

SI-02 Flaw Remediation

[illegible]

- (3) Using extended detection and response (XDR) with automated remediation, the IRS must proactively quarantine and remove assets from the IRS network upon alerts and identification of unacceptable security hygiene results by authorized security information event management (SIEM) tools (e.g., Splunk, Log Rhythm). (NSA Adversary Emulation Study) (L, M, H)

- a. The IRS must ensure endpoint detection and response (EDR) tools (e.g., Rapid7, CrowdStrike, Palo Alto, Fortinet) meet CISA's technical requirements, are deployed widely, and provide inputs to XDR. (*OMB M-22-09 (III)(B)(2)*)
 - i. The IRS must work with CISA to identify implementation gaps, coordinate the deployment of EDR tools, and establish information-sharing capabilities, as described in *OMB M-22-01, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*.
- b. The IRS must use security, orchestration, automation, and response (SOAR) (e.g., Splunk Phantom, ServiceNow) to develop automated hunt and incident response playbooks and provide inputs to XDR. (*OMB M-21-31*)
- c. The IRS must use secure access service edge (SASE) (e.g., a combination of software-defined wide area network (SDWAN), cloud access security broker (CASB), secure web gateway (SWG), and firewall (FW) security) for security services for cloud technology. (CISA: Cloud Security Technical Reference Architecture)
- d. The IRS must use user and entity behavior analytics (UEBA) to detect anomalies of behavior and provide inputs to XDR. (*OMB M-22-09 (III)(A)(1)*)

Note: A quarantine process may be used to automatically remediate an asset and return the asset to the IRS network. For example, Symantec may identify an asset that is not up-to-date with patching and when the asset is used for a logon attempt, that the asset may be automatically patched and be permitted to return to the IRS network.

#

#

- (8) By April 3, 2023, the IRS is required to initiate vulnerability enumeration across all discovered assets, including all discovered nomadic/roaming devices (e.g., laptops), every 14 days. (*CISA BOD 23-01*) (L, M, H)

Note: CISA understands that in some instances achieving full vulnerability discovery on the entire enterprise may not complete in 14 days. Refer to BOD 23-01 Implementation Guidance for additional guidance.

- a. To the maximum extent possible and where available technologies support it, all vulnerability enumeration performed on managed endpoints (e.g., servers, workstations, desktops, laptops) and managed network devices (e.g., routers, switches, firewalls) must be conducted with privileged credentials.

Note: Both network-based credentialed scans and client- or agent-based vulnerability detection methods meet this requirement.

- b. All vulnerability detection signatures used must be updated at an interval no greater than 24 hours from the last vendor-released signature update.
- c. Where the capability is available, the IRS must perform the same type of vulnerability enumeration on mobile devices (e.g., iOS and Android) and other devices that reside outside of IRS on-premises networks.
- d. All vulnerability enumeration methods (e.g., for systems with specialized equipment or those unable to utilize privileged credentials) must be approved by CISA.
- (9) By April 3, 2023, the IRS must initiate automated ingestion of vulnerability enumeration results (i.e., detected vulnerabilities) into the CDM Agency Dashboard within 72 hours of discovery completion (or initiation of a new discovery cycle if previous full discovery has not been completed). (*CISA BOD 23-01*) (L, M, H)
- (10) By April 3, 2023, the IRS must develop and maintain the operational capability to initiate on-demand vulnerability enumeration to identify specific subsets of vulnerabilities within 72 hours of receiving a request from CISA and provide the available results to CISA within 7 days of request. (*CISA BOD 23-01*) (L, M, H)
- (11) Within 6 months of CISA publishing requirements for vulnerability enumeration performance data, the IRS must initiate the collection and reporting of vulnerability enumeration performance data, as relevant to this directive, to the CDM Dashboard. (*CISA BOD 23-01*) (L, M, H)
- (12) By April 3, 2023, the IRS and CISA, through the CDM program, must deploy an updated CDM Dashboard configuration that enables access to object-level vulnerability enumeration data for CISA analysts, as authorized in *EO 14028*. (*CISA BOD 23-01*) (L, M, H)

#

- (16) Vulnerabilities detected by CISA Cyber Hygiene scans for all internet-accessible systems must be remediated within the following timelines: (*CISA BOD 19-02*) (L, M, H)

#

- c. Refer to IRM 10.8.50 for additional Cyber Hygiene guidance.
- d. The IRS must proactively quarantine and remove assets from the IRS network for vulnerabilities detected by CISA Cyber Hygiene scans for all internet-accessible systems but not remediated per above timelines. (NSA Adversary Emulation Study)
 - i. No asset detected by the CISA Cyber Hygiene scan will be issued a POA&M, RBD, or Risk Acceptance Form and Tool (RAFT) unless approved by the CISO or CIO. (IRS-defined)

Note: An internet-accessible system is any system that is globally accessible over the public internet. It has a publicly routed IP address or a hostname that resolves publicly in DNS to such an address. It doesn't pertain to infrastructure that is internal to a bureau network that enables endpoints to be accessible over the internet, systems reachable from the internet but that require special configuration or access controls (e.g., via a VPN), or shared services.

- (17) Vulnerabilities identified by CISA within the CISA-managed vulnerability catalog must be remediated according to the timelines set forth in the catalog. (*CISA BOD 22-01*) (L, M, H)
- a. An asset(s) must be removed from the IRS network if remediation actions defined within the catalog cannot be accomplished in the required timeframe.
- Note:** Isolation/quarantine is a form of removal. Depending on the environment, appropriate isolation techniques may include decommissioning, removal of the vulnerable software product, network segmentation, isolation, software-defined perimeters, and proxies
- i. Assets with a CISA KEV Catalog vulnerability will not be issued a POA&M, RBD, or RAFT unless approved by the CISO or CIO. (IRS-defined)
- Note:** CISA provides a catalog, or repository, of known exploited vulnerabilities on the KEV website.
- (18) The IRS must maintain an effective and welcoming public vulnerability disclosure program for their internet-accessible systems, by September 2022. (*OMB M-22-09 (III)(D)(3)*) (L, M, H)
- (19) In accordance with *CISA BOD 23-02, Mitigating the Risk from Internet-Exposed Management Interfaces*, the IRS must employ capabilities to mediate all access to device management interfaces that are connected directly to, and accessible from, the public-facing internet, in alignment with *OMB M-22-09, NIST SP 800-207*, the TIC 3.0 Capability Catalog, and CISA's Zero Trust Maturity Model. (*CISA BOD 23-02*) (L, M, H)
- (20) Refer to IRM 10.8.50, for additional patch management guidance. (L, M, H)

10.8.1.4.19.2
(01-28-2025)
**SI-03 Malicious Code
Protection**

[illegible]

#

#

10.8.1.4.19.2.1
(01-28-2025)
**Electronic Mail (Email)
Security**

- (1) The IRS must securely configure email systems to protect the network where the systems reside and the data stored and transmitted by the email systems in accordance with *NIST SP 800-45 Ver 2, Guidelines on Electronic Mail Security*. (NIST SP 800-45) (L, M, H)
- (2) Users must sign email messages to ensure integrity and provide confirmation of the sender's identity. (*NIST SP 800-45*) (L, M, H)
- (3) When the confidentiality of the contents of an email message (containing proprietary or sensitive information) needs to be protected, users must encrypt the body of the email message using an IRS IT-approved solution for email encryption (e.g., digital certificates). (*NIST SP 800-45*) (L, M, H)

Note: Refer to the internal *Email Encryption* site for an IT-approved email encryption solution.

Note: Effective 8/16/24, the IRS blocks the ability to send external emails with encryption that bypasses detection mechanisms (such as S/MIME certificate and password protection).

- (4) Refer to IRM 1.10.3 and IRM 10.5.1 for additional guidance. (L, M, H)

10.8.1.4.19.2.1.1
(01-28-2025)
**Privately Owned Email
Accounts**

- (1) Automatic forwarding must not be used to send messages to non-IRS/Treasury accounts. (IRS-defined) (L, M, H)
- (2) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.19.3
(01-28-2025)
**SI-04 System Monitoring
(InTC)**

#

#####

#

#

#

#

10.8.1.4.19.4
(12-13-2022)
**SI-05 Security Alerts,
Advisories, and
Directives**

#

10.8.1.4.19.5
(09-28-2021)
**SI-06 Security and
Privacy Function
Verification**

#

10.8.1.4.19.6
(01-28-2025)
**SI-07 Software,
Firmware, and
Information Integrity**

#

[illegible]

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#####

10.8.1.4.19.10
(09-28-2021)
SI-11 Error Handling

##

10.8.1.4.19.11
(12-13-2022)
**SI-12 Information
Management and
Retention**

##

#

- (5) For controls allocated to the Privacy baseline, refer to the NIST SP 800-53 Security and Privacy Controls subsection of IRM 10.5.1. (L, M, H)

10.8.1.4.19.12
(12-23-2013)

**SI-13 Predictable Failure
Prevention**

#

10.8.1.4.19.13
(12-23-2013)

SI-14 Non-Persistence

#

10.8.1.4.19.14
(12-23-2013)

**SI-15 Information Output
Filtering**

#

10.8.1.4.19.15
(09-28-2021)

SI-16 Memory Protection

#

10.8.1.4.19.16	#
(12-23-2013)	#
SI-17 Fail-Safe Procedures	
10.8.1.4.19.17	#
(12-13-2022)	#
SI-18 Personally Identifiable Information Quality Operations	# # # #
10.8.1.4.19.18	#
(12-13-2022)	#
SI-19 De-Identification	#
10.8.1.4.19.19	#
(09-28-2021)	#
SI-20 Tainting	
10.8.1.4.19.20	#
(09-28-2021)	#
SI-21 Information Refresh	
10.8.1.4.19.21	#
(09-28-2021)	#
SI-22 Information Diversity	
10.8.1.4.19.22	#
(09-28-2021)	#
SI-23 Information Fragmentation	
10.8.1.4.20	#
(09-28-2021)	#
SR-01 Supply Chain Risk Management Policy and Procedures	# # # # # # # # # # # #

#####

- 10.8.1.4.20.1
(09-28-2021)
**SR-02 Supply Chain
Risk Management Plan**

[illegible]

10.8.1.4.20.2
(12-13-2022)
**SR-03 Supply Chain
Controls and Processes**

#

10.8.1.4.20.3
(09-28-2021)
SR-04 Provenance

10.8.1.4.20.4
(09-28-2021)
**SR-05 Acquisition
Strategies, Tools, and
Methods**

#

10.8.1.4.20.5
(12-12-2023)
**SR-06 Supplier
Assessments and
Reviews**

#

- (2) The IRS must collect attestation letters from software producers for third-party software that was developed, had a renewal, or had a major version update after September 14, 2022, in accordance with *OMB M-22-18*, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices and *OMB M-23-16*, Update to Memorandum M-22-18. (*OMB M-22-18*; *OMB M-23-16*) (L, M, H)
- a. The CIO must communicate relevant requirements to vendors and ensure attestation letters are collected in one central IRS system by January 12, 2023.
 - b. The IRS must collect attestation letters for “critical software” no later than three months after the attestation common form released by the CISA is approved by OMB under the Paperwork Reduction Act (PRA). (*OMB M-22-18*; *OMB M-23-16*) (CSW)
 - c. The IRS must collect attestation letters for all software no later than six months after the attestation common form released by the CISA is approved by OMB under the PRA. (*OMB M-22-18*; *OMB M-23-16*)

Note: A CISA repository for housing government-wide software attestation documentation will become available at a future date.

Note: The IRS is not required to collect attestations from software producers for products that are proprietary but freely obtained and publicly available.

- d. If a software producer cannot provide software attestation, the IRS must take appropriate steps to ensure that any documentation, concerning the producer’s inability to provide a complete self-attestation, must not become public by the IRS.
- e. If the software producer supplies documentation that the IRS finds satisfactory, the IRS may use the software, despite the producer’s inability to provide a complete self-attestation, via an approved RBD for an acceptance of risk by the SAISO/CISO or AO of the system where the software resides.
- f. A third-party assessment provided by either a certified FedRAMP Third Party Assessor Organization (3PAO) or one approved by the IRS must be acceptable in lieu of a software producer’s self-attestation, including in the case of open-source software or products incorporating open-source software, provided the 3PAO uses the NIST Guidance as the assessment baseline.

Note: *OMB M-22-18* does not apply to IRS-developed or inter-agency-developed software, although agencies are expected to take appropriate steps to adopt and implement secure software development practices for agency-developed software.

- (3) The CIO must develop a consistent process to communicate with software producers by January 12, 2023. (*OMB M-22-18*) (L, M, H)

- a. The CIO must request software producers to be product inclusive so that the same attestation may be readily provided to all purchasing agencies.
- b. The CIO must inform software producers that if the software producer cannot attest to one or more practices from the NIST Guidance identified in the standard self-attestation form, the IRS must require the following:
 - i. The software producer to identify those practices to which the software producer cannot attest;
 - ii. The software producer to document practices they have in place to mitigate those risks; and
 - iii. A POA&M to be developed.
- c. If a software producer cannot provide software attestation, the IRS must notify the software producer to take appropriate steps to ensure that any documentation concerning inability to provide software attestation is not posted publicly.
- d. An acceptable self-attestation must include the following minimum requirements:
 - i. The software producer's name;
 - ii. A description of which product or products the statement refers to (preferably focused at the company or product line level and inclusive of all unclassified products sold to Federal agencies);
 - iii. A statement attesting that the software producer follows secure development practices and tasks that are itemized in the standard self-attestation form;
 - iv. Self-attestation is the minimum level required; however, the IRS may make risk-based determinations that a third-party assessment is required due to the criticality of the service or product that is being acquired, as defined in *OMB M-21-30*, Protecting Critical Software Through Enhanced Security Measures.

Note: CISA and OMB have released a *Self Attestation Common Form* for agencies to use on March 11, 2024.

- (4) The IRS must retain self-attestation documentation unless the software producer posts it publicly and provides a link to the posting as part of its proposal response. (*OMB M-22-18*) (L, M, H)
- (5) A Software Bill of Materials (SBOM) must be required in solicitation guidance using data formats defined by CISA. The IRS must consider reciprocity of SBOM and other artifacts from software producers that are maintained by other Federal agencies. (*OMB M-22-18*) (L, M, H)

Note: If the IRS awards a contract that may be used by other agencies, the IRS is responsible for implementing the requirements of *OMB M-22-18*.

- (6) The CIO, in coordination with the chief procurement officer, must assess organizational training needs and develop training plans for the review and validation of full attestation documents and artifacts, by March 13, 2023. (*OMB M-22-18*) (L, M, H)
- (7) If the IRS is unable to meet OMB deadlines for any specific *OMB M-22-18* requirement(s), the IRS must submit a request for an extension or a waiver to the Director of OMB. The extension or waiver request must be transmitted 30 days before any relevant deadline. (*OMB M-22-18*) (L, M, H)

- a. If the IRS requests an extension for complying with *OMB M-22-18* requirements, the extension request must be accompanied by a plan for meeting the requirements.
- b. If the IRS requests a waiver for complying with the requirements of *OMB M-22-18*, the waiver request must be accompanied by a plan for mitigating any potential risks.

Note: Waivers may be requested only in the case of exceptional circumstances and for a limited duration.

- c. Deadlines for transmitting extension or waiver requests regarding *OMB M-22-18* requirements are as follows:

Requirement	Extension or Waiver Request Deadline	Requirement Deadline
To inventory all third-party software	November 13, 2022	December 13, 2022
To develop a consistent process to communicate with software producers	December 13, 2022	January 12, 2023
To ensure attestation letters are collected in one central IRS system	December 13, 2022	January 12, 2023
To assess organizational training needs and develop training plans for the review and validation of full attestation documents and artifacts	February 11, 2023	March 13, 2023
To collect attestation letters for “critical software”	May 12, 2024	June 11, 2024
To collect attestation letters for all software	August 12, 2024	September 11, 2024

Note: Specific instructions for submitting requests for extensions or waivers will be posted in *OMB MAX Portal*.

Note: CISA and OMB have released a *Self Attestation Common Form* for agencies to use on March 11, 2024.

##

#

##

#

##

##

#####

10.8.1.4.20.10

(09-28-2021)

SR-11 Component**Authenticity**

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

10.8.1.4.20.11

(09-28-2021)

SR-12 Component**Disposal**

#

#

#

#

#

#

#

#

#

#

#

#

#

#

This Page Intentionally Left Blank

Exhibit 10.8.1-1 (01-28-2025)**Terms and Acronyms****0-9****3PAO - Third Party Assessor Organization****A**

AARG – Assessment, Authorization & Risk Governance

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

- 1) Obtain and use information and related information processing services, and
- 2) Enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).

Account Manager - User account management involves the process of requesting, establishing, issuing, modifying, and closing user accounts; tracking users and their access authorization and privileges.

Accountability - The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information.

ACIO - Associate Chief Information Officer

Adequate Security - Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Note: This includes assuring that systems operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

Administrative Furlough - A planned event by an agency which is designed to absorb reductions necessitated by downsizing, reduced funding, lack of work, or any budget situation other than a lapse in appropriations. Furloughs that would potentially result from sequestration would generally be considered administrative furloughs. (OPM.gov)

Advanced Persistent Threat (APT) - An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat:

- (i) Pursues its objectives repeatedly over an extended period of time,
- (ii) Adapts to defenders' efforts to resist it, and
- (iii) Is determined to maintain the level of interaction needed to execute its objectives.

AI - Artificial Intelligence

AIFIS - Automated Integrated Fingerprint Identification System

AIS - Automated Information System

Exhibit 10.8.1-1 (Cont. 1) (01-28-2025)**Terms and Acronyms**

AP - Authority and Purpose

APNSA - Assistant to the President and National Security Advisor

Application Developers - Refer to Developers

ASHRAE - American Society of Heating, Refrigerating and Air-conditioning Engineers

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

Audit - An independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures.

Audit Trail - A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result.

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 they claim 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 or token).

Authorization - Access privileges granted to a user, program, or process or the act of granting those privileges.

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

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

Authorization Package - The evidence provided to the AO to be used in the security authorization decision process. Evidence includes, but is not limited to:

1. The SSP
2. The assessment results from the security certification
3. The POA&Ms

Authorized Personnel - Applies to all IRS personnel cleared with a requirement to access information systems (IS) for performing or assisting in a lawful and authorized government function.

Authorizing Official (AO) - Official with the authority to formally assume responsibility for operating a 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 system operations. Previously known as the Designated Approving Authority.

Availability - Ensuring timely and reliable access to and use of information.

Exhibit 10.8.1-1 (Cont. 2) (01-28-2025)**Terms and Acronyms**

Awareness (Information Security) - Activities which seek to focus an individual's attention on an (information security) issue or set of issues.

B

BIA - Business Impact Analysis

BEARS - Business Entitlement Access Request System - Use BEARS to request access to and perform recertifications on subapps (entitlements) which have been migrated from OL5081.

Binding Operational Directive (BOD) - A compulsory direction issued by CISA to federal, executive branch, departments and agencies for the purposes of safeguarding federal information and systems.

BGP - Border Gateway Protocol

BIOS - Basic Input/Output System

Blacklist - A list of discrete entities, such as hosts or applications, that have been previously determined to be associated with malicious activity.

Bureau(s) and IRS Head - Refer to Department

Bot - A bot also known as software robot (web robot or chat robot) is a software program or an application that runs repetitive tasks at a higher rate than would be possible for human alone.

Breach - The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses PII or (2) a person accesses or potentially accesses PII for an unauthorized purpose (i.e., a purpose unrelated to their official duties/functions). (*OMB M-17-12*, Treasury IR Plan)

Note: A breach is a type of incident.

Business Partner - A term used to denote an entity with which another entity has some form of alliance. This relationship may be a highly contractual, exclusive bond in which both entities commit not to ally with third parties.

BYOD - Bring Your Own Device

C

CAD – Computer-Aided Design

CASB - Cloud Access Security Broker

CAVP - Cryptographic Algorithm Validation Program

CD - Compact Disk

CDM - Continuous Diagnostics and Mitigation

CD-ROM - Compact Disc - Read Only Memory

Certificate - Refer to Digital Certificate

Certification Authority (CA) - A trusted entity in a PKI that issues and revokes certificates exacting compliance to a PKI policy.

Exhibit 10.8.1-1 (Cont. 3) (01-28-2025)**Terms and Acronyms**

CGI - Common Gateway Interface

CIO - Chief Information Officer

CIP - Critical Infrastructure Protection

CISO - Chief Information Security Officer

Classified Information - Information that has been determined pursuant to *EO 13526* or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Cloud Computing - A model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three cloud service delivery models (Software as a Service [SaaS], Platform as a Service [PaaS], and Infrastructure as a Service [IaaS]); and four models for enterprise access (Private, Community, Public, and Hybrid).

CM – Configuration Management

CMMI - Capability Maturity Model Integration

CMVP - Cryptographic Module Validation Program

CNSI - Classified National Security Information

Common Control - A Security control that is inherited by one or more organizational systems. Refer to Security Control Inheritance.

Common Vulnerabilities and Exposures (CVE) - A dictionary of common names (i.e., CVE Identifiers) for publicly known cybersecurity vulnerabilities. CVE's common identifiers make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization's security tools. If a report from a security tool incorporates CVE Identifiers, an individual can then quickly and accurately access fix information in one or more separate CVE-compatible database to remediate the problem. *CVE website.*

Common Vulnerability Scoring System (CVSS) - Organizations can reference CVSS in order to work on the action(s) that have the highest priority or present the greatest amount of risk. CVSS can measure how serious a given vulnerability is compared to other vulnerabilities so remediation efforts can be prioritized. The Base metrics produce a score ranging from 0 to 10. *CVSS website.*

Concurrent - Operating or occurring at the same time; running parallel; and/or acting in conjunction.

Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Control - Process of controlling modifications to hardware, firmware, software, and documentation to protect the system against improper modifications prior to, during, and after system implementation.

Exhibit 10.8.1-1 (Cont. 4) (01-28-2025)**Terms and Acronyms**

Configuration Control Board (CCB) - A group of qualified people with responsibility for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an system.

CONOPS - Concept of Operations

Contingency Plan - Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the Continuity of Operations Plan (COOP) or Disaster Recovery Plan for major disruptions.

Continuity of Operations Plan (COOP) - A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained within 12 hours for up to 30 days as a result of a disaster event before returning to normal operations.

Continuous Monitoring - Maintaining an ongoing awareness to support organizational risk decisions.

Controlled Area - A security area which requires one single authentication mechanism to ensure only authorized personnel have unescorted access. (per IRM 10.2.14)

Controlled Unclassified Information (CUI) - A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under EO 12958, as amended, but requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces "Sensitive But Unclassified" (SBU).

Controlled Unclassified Information (CUI) Program - The CUI Program is the program to standardize CUI handling by all Federal agencies. The Program includes the rules, organization, and procedures for CUI. (NARA, 2002.4)

Core hours - The time periods during the workday, workweek, or pay period that are within the tour of duty during which an employee covered by a flexible work schedule is required by the IRS to be present for work. (Refer to 5 USC 6122(a)(1).)

COTS - Commercial Off The Shelf

Countermeasures - Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of a system. Synonymous with security controls and safeguards.

CPIC (Capital Planning Investment Control) - The CPIC Program is a structured, integrated approach to managing Information Technology (IT) investments. It ensures that all IT investments align with the EPA mission and support business needs while minimizing risks and maximizing returns throughout the investment's lifecycle. The CPIC relies on a systematic approach to IT investment management in three distinct phases: select, control, and ongoing evaluation, to ensure each investment's objectives support the business and mission needs of the agency.

CPO - Chief Privacy Officer

CPU - Central Processing Unit

Critical Infrastructure Protection (CIP) - System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (CNSSI No. 4009)

Exhibit 10.8.1-1 (Cont. 5) (01-28-2025)**Terms and Acronyms**

Critical Software - Any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes: (As defined by NIST for EO 14028)

- Has direct or privileged access to networking or computing resources;
- Is designed to run with elevated privilege or manage privileges;
- 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.

CRQC - Cryptanalytically Relevant Quantum Computer

Cryptographic System - An active software or hardware implementation of one or more cryptographic algorithms that provide one or more of the following services: creation and exchange of encryption keys, encrypted connections, or creation and validation of digital signatures. (*OMB M-23-02*)

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

CSF – Cybersecurity Framework

CSIRC - Computer Security Incident Response Center

CSP - Cloud Service Provider

CSW - Critical Software

CUI - Controlled Unclassified Information

CWE - Common Weakness Enumeration

Cyber Event - Any observable occurrence in a network or system that may indicate a cyber incident has occurred. (Treasury IR Plan)

Cyber Hygiene Report - A weekly report by CISA, which operates under DHS. Cyber Hygiene leverages the Common Vulnerability Scoring System (CVSS), which is a vulnerability scoring system designed to provide a universally open and standardized method for rating IT vulnerabilities. CVSS helps organizations prioritize vulnerability management strategies by providing a score representative of the base, temporal, and environmental properties of vulnerabilities. (*CISA BOD 19-02*)

Cybersecurity and Infrastructure Security Agency (CISA) - An operational component under DHS. Responsible for protecting the Nation's critical infrastructure from physical and cyber threats. Develops and oversees the implementation of BODs and EDs, which require action on the part of certain federal agencies in the civilian executive branch.

D

Data at Rest - All data in computer storage (e.g., on hard disk drives, CDs/DVDs, floppy disks, thumb drives, PDAs, cellphones, other removable storage media) 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).

DBA - Database Administrator

De-identification - The process by which a collection of data is stripped of information which would allow the identification of the source of the data.

Exhibit 10.8.1-1 (Cont. 6) (01-28-2025)**Terms and Acronyms**

Demilitarized Zone (DMZ) - 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.

Denial of Service (DoS) - The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided.)

Department - Within the context of this IRM, the terms department, departments, departmental, etc. refer solely to the IRS unless there is a specific reference to Treasury. The terms "department employee(s)" and "Treasury employee(s)" also refer to the IRS.

Desktop Sharing - A common name for technologies and products that allow remote access and remote collaboration on a person's computer desktop through a graphical Terminal emulator.

Developer - A general term that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; (iv) and product resellers. Development of systems, components, or services can occur internally within organizations (i.e., in-house development) or through external entities. (CNSSI No. 4009) Refer to IRM 10.8.2 for definitions for program developer/programmer and web developer.

DH - Diffie-Hellman

DHCP - Dynamic Host Configuration Protocol

DHS - Department of Homeland Security

Digital Certificate - A digital representation of information used in conjunction with a public key encryption system, which at a minimum:

1. Identifies the certification authority issuing it;
2. Names or identifies its subscriber;
3. Contains the subscriber's public key;
4. Identifies its operational period.
5. Is digitally signed by the certification authority issuing it.

DISA - Defense Information Systems Agency

Discretionary Access Control (DAC) - A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).

DLP - Data Loss Prevention

DNS - Domain Name System

DNSSEC - Domain Name System (DNS) Security Extensions

DoD - Department of Defense

Download - To copy or transfer (software, data, character sets, etc.) from a distant to a nearby computer, from a larger to a smaller computer, or from a computer to a peripheral device.

DPCI - Derived PIV Credential Issuers

Exhibit 10.8.1-1 (Cont. 7) (01-28-2025)**Terms and Acronyms**

DPI - Deep Packet Inspection

DR - Disaster Recovery

DVD - Digital Video Disc

DVI - Digital Video Interface

E

EAP - Extensible Authentication Protocol

ECC-MTB - Enterprise Computing Center - Martinsburg

ECDH - Elliptic Curve Diffie-Hellman

ECDSA - Elliptic Curve Digital Signature Algorithm

ED - Emergency Directive

EDR - Endpoint Detection and Response

EFC - Enterprise FISMA Compliance

ELC - Enterprise Life Cycle

Elevated Privileges - Any user right assignment that is above the baseline indicated within this IRM.

Email - Electronic Mail

Encryption - Conversion of plaintext to ciphertext through the use of a cryptographic algorithm.

Endpoints - Includes the following: (FY 2017 CIO FISMA Metrics)

- Servers (including mainframe/minicomputers/midrange computers)
- Workstations (desktops laptops, Tablet PCs, and net-books)
- Virtual machines

Enterprise Architecture (EA) - The description of an enterprise's entire set of systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture.

EO - Executive Order

EOps - Enterprise Operations

ESAT - Enterprise Security Audit Trails

ESR – External System Review

EVIDACT - Foundations for Evidence-Based Policymaking Act of 2018 (P.L. 115-435), January 2019

F

FAM - U.S. Department of State Foreign Affairs Manual

Exhibit 10.8.1-1 (Cont. 8) (01-28-2025)**Terms and Acronyms**

FASC - Federal Acquisition Security Council

Federal Information Security Modernization Act of 2014 (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 systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

FedRAMP - Federal Risk and Authorization Management Program

FICAM - Federal, Identity, Credential and Access Management

FIPS - Federal Information Processing Standards

FIPS-Validated Cryptography - A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in *NIST FIPS 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). (*NIST SP 800-53 Rev 5*)

Fire Call - Used to represent an emergency, time-critical situation.

FW - Firewall

FMSS - Facilities Management and Security Services

FOCI - Foreign Ownership, Control or Influence

FOIA - Freedom of Information Act

FTI - Federal Taxpayer Information

FTP - File Transfer Protocol

FY - Fiscal Year

G

GAO - Government Accountability Office

Generic account, generic access, generic identification, generic logon - Terms refer to definition and implementation of user authentication information (such as user IDs and passwords) and procedures which are designed so that they do NOT require specific information associated with a unique individual but accept some nonspecific identification information to enable access.

GFE - Government Furnished Equipment

GIS - Geographic Information System

GMT - Greenwich Mean Time

GPS - Global Positioning System

GRS - General Records Schedules

GSA - General Services Administration

H

Exhibit 10.8.1-1 (Cont. 9) (01-28-2025)**Terms and Acronyms**

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

High Value Asset (HVA) - Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. HVA can fall into one of the three categories:

- Informational Value - The information or information system that processes, stores, or transmits the information is of high value to the Government or its adversaries.
- Mission Essential – The agency that owns the information or information system cannot accomplish its Primary Mission Essential Functions (PMEF), as approved in accordance with Presidential Policy Directive 40 (PPD-40) National Continuity Policy, within expected timelines without the information or information system.
- Federal Civilian Enterprise Essential (FCEE) – The information or information system serves a critical function in maintaining the security and resilience of the federal civilian enterprise.

HSPD - Homeland Security Presidential Directive

HSTS - Hypertext Transport Protocol (HTTP) Strict Transport Security

HTTP - Hypertext Transfer Protocol

HTTPS - Hypertext Transfer Protocol Secure

HVAC - Heating, Ventilation, and Air Conditioning

I

I&A - Identification & Authentication

IAM - Identity and Access Management

IANA - Internet Assigned Numbers Authority

ICMP - Internet Control Message Protocol

Identification - The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.

IDRS - Integrated Data Retrieval System

IEEE - Institute of Electrical and Electronics Engineers

IG - Interim Guidance

IMAP - Internet Message Access Protocol

Impact - The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or system availability.

Incident - An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or a system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. (Treasury IR Plan)

Exhibit 10.8.1-1 (Cont. 10) (01-28-2025)**Terms and Acronyms**

Incident Handling - The mitigation of violations of security policies and recommended practices.

Incident Response Plan - The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of malicious cyber-attacks against an organization's system(s).

Independent Assessor/Independent Assessment Team - Individuals or groups conducting impartial assessments of systems. Impartiality means that assessors are free from any perceived or actual conflicts of interest regarding development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted; assess their own work; act as management or employees of the organizations they are serving; or place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within an organization or can be contracted to public or private sector entities outside of organizations.

Information Assurance (IA) - Measures that protect and defend information and systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of systems by incorporating protection, detection, and reaction capabilities.

Information Owner - Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

IR - Incident Response

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

Information Sharing Environment (ISE) - 1. An approach that facilitates the sharing of terrorism and homeland security information; or 2. ISE in its broader application enables those in a trusted partnership to share, discover, and access controlled information.

Information System - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.

Information System Contingency Plan (ISCP) (previously known as ITCP – IT Contingency Plan) - Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters.

Information System Security Officer (ISSO) - Individual assigned responsibility by the SAISO, AO, management official, or system owner for maintaining the appropriate operational security posture for a system or program.

Information Technology (IT) - Any service or equipment or the 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 acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

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.

Exhibit 10.8.1-1 (Cont. 11) (01-28-2025)**Terms and Acronyms**

- 3) The term “information technology” does not include any equipment that:
- Is acquired by a contractor incidental to a contract, or
 - Contains imbedded 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 equipment, such as electronic thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, is not information technology.

InTC - Insider Threat Capability

Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. The property whereby an entity has not been modified in an unauthorized manner.

Interconnected Systems - A direct connection between two or more systems in different authorization boundaries for the purpose of exchanging information and/or allowing access to information, information services, and resources. An interconnection used for information exchange has at least three basic components: two (or more) endpoints and the mechanism by which the data flows (i.e., the “pipe” through which information is exchanged). The interconnection can be made from one location to another location or from one location to several locations. Refer to *NIST SP 800-47 Rev 1* for additional information.

Interconnection Security Agreement (ISA) - An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/MOA) between the organizations.

Internet-Accessible System - Any system that is globally accessible over the public internet. It has a publicly routed IP address or a hostname that resolve publicly in DNS to such an address. It doesn't pertain to infrastructure that is internal to a bureau network that enables endpoints to be accessible over the internet, systems reachable from the internet but that require special configuration or access controls (e.g., via a VPN), or shared services.

I/O - Input/Output

IoT - Internet of Things

IRM - Internal Revenue Manual

IRS - Internal Revenue Service

ISP - Internet Service Provider

ITIL - Information Technology Infrastructure Library

ITSCM - Information Technology Service Continuity Management

K

KEV - Known Exploited Vulnerability

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

Exhibit 10.8.1-1 (Cont. 12) (01-28-2025)**Terms and Acronyms**

Key Pair - Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and 2) even knowing one key, it is computationally infeasible to discover the other key.

Keystroke Monitoring - The process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails.

L

LAN - Local Area Network

LDAP - Lightweight Directory Access Protocol

Least Privilege - The security objective of granting users only those accesses they need to perform their official duties.

LERN - Labor/Employee Relations and Negotiations

Limited Area - A security area to which access is limited to authorized personnel by a two-factor authentication mechanism. All limited areas must either meet secured area criteria (as outlined in IRM 10.2.14) or provisions must be made to store protect able items in appropriate containers during non-duty hours. "Open office" refers to any area which is not designated as a limited area.

Live Data - Production data in use (e.g., electronic, hardcopy); might include SBU information (i.e., PII, PHI, taxpayer data, system-sensitive information).

LOW Impact System - A system in which all three security objectives (i.e., confidentiality, integrity, and availability) are assigned a *FIPS 199* potential impact of LOW.

LSS - Lean Six Sigma

LWOP - Leave Without Pay

M

MAC - Media Access Control

Major Application - An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

Major Incident - Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. (OMB M-17-05) Refer to also Breach.

Major Information System - A system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

Management Controls - The security controls (e.g., safeguards or countermeasures) for an system that focus on the management of risk and the management of system security.

Exhibit 10.8.1-1 (Cont. 13) (01-28-2025)**Terms and Acronyms**

Mass Storage Device - A storage drive: hard disk, solid state disk, or USB drive that makes it possible to store and port large amounts of data across computers, servers and within an IT environment.

Maximum Tolerable Downtime (MTD) - The amount of time mission/business processes can be disrupted without causing significant harm to the organization's mission.

MEF - Mission Essential Function

Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA) - A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/MOA defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.

Mission Critical - Any telecommunications or system that is defined as a national security system (FISMA) or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of the agency.

Mobile Code - Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient.

Mobile Computing Device - Portable computing and communications device with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices).

MODERATE Impact System - A system in which at least one security objective (e.g., confidentiality, integrity, or availability) is assigned a *FIPS 199* potential impact value of MODERATE and no security objective is assigned a *FIPS 199* potential impact value of HIGH.

MTIPS - Managed Trusted Internet Protocol Service

MQV - Menezes-Qu-Vanstone

Multi-factor Authentication (MFA) - Requires using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (i.e., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Refer to Authenticator.

Multi-Functional Device (MFD) - Also known as MFP (Multi-Function Product/ Printer/ Peripheral), or all-in-one (AIO), is an office machine which incorporates the functionality of multiple devices in one, so as to have a smaller footprint in the business environment, or to provide centralized document management, distribution, and production in a large-office setting. A typical MFP may act as a combination of some or all of the following devices: Printer, Scanner, Photocopier, Fax, Email.

N

NARA - National Archives and Records Administration

(NIAP) - A U.S. government initiative established to promote the use of evaluated systems products and champion the development and use of national and international standards for information technology security. NIAP was originally established as collaboration between the NIST and the NSA in fulfilling their respective responsibilities under P.L. 100-235 (Computer Security Act of 1987). NIST officially withdrew from the partnership in 2007 but NSA continues to manage and operate the program. The key operational component of NIAP is the Common Criteria Evaluation and Validation Scheme (CCEVS) which is the only U.S. government-sponsored and endorsed program for conducting internationally recognized security evaluations of COTS Information Assurance (IA) and IA-enabled information technology products. NIAP employs the CCEVS to provide govern-

Exhibit 10.8.1-1 (Cont. 14) (01-28-2025)**Terms and Acronyms**

ment oversight or “validation” to U.S. CC evaluations to ensure correct conformance to the International Common Criteria for IT Security Evaluation (ISO/IEC 15408).

National Security Information (NSI) - Any agency information (processed by telecommunications and/or systems) that must be protected at all times by procedures established for information that have been specifically authorized under criteria established by an EO or an act of Congress to be kept secret in the interest of national defense or foreign policy. The national security function, operation, or use of which involves: intelligence activities; cryptologic activities related to national security; command and control of military force; equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military/intelligence missions provided that this definition does not apply to a system that is used for routine administrative and business applications (including payroll, finance, logistics and personnel management applications).

NCP - National Checklist Program

NCPR - National Checklist Program Repository

NEF - National Essential Functions

Network Access - Access to an organizational system by a user (or a process acting on behalf of a user) communicating through a network (e.g., LAN, WAN, internet).

NFS - Network File System

NIACAP - National Information Assurance Certification and Accreditation Process

NIST - National Institute of Standards and Technology

NSA - National Security Agency

NSTISSI - National Security Telecommunications and Information Systems Security Instruction

Non-government furnished/owned devices - Includes devices owned by contractors and personally-owned.

Non-organizational User - An employee or an individual considered by the organization to have the equivalent status of an employee. Organizational users include contractors, guest researchers, or individuals detailed from other organizations. A non-organizational user is a user who is not an organizational user. (NIST)

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.

Notable Cyber Event - Any deviation from the norm or observable occurrence in a network or system that could have led to a cyber incident but was otherwise mitigated and the source or threat vector poses an ongoing risk to the IRS. (Treasury IR Plan)

NPE - Non- Person Entity is an entity with a digital identity that acts in cyberspace but is not a human actor. This can include organizations, hardware devices, software applications, and information artifacts.

NVD - National Vulnerability Database

O

OCC - Organizational Common Controls

OFCIO - Office of the Federal Chief Information Officer (OMB)

Exhibit 10.8.1-1 (Cont. 15) (01-28-2025)**Terms and Acronyms**

OIG - Office of the Inspector General

OMB - Office of Management and Budget

ONCD - Office of the National Cyber Director

OneSDLC - One Solution Delivery Life Cycle

OSS - Open Source Software

OPM - Office of Personnel Management

Operational Controls - The security controls (e.g., safeguards or countermeasures) for a system that primarily are implemented and executed by people (as opposed to systems).

Organizational User - An employee or an individual considered by the organization to have the equivalent status of an employee. Organizational users include contractors, guest researchers, or individuals detailed from other organizations. (NIST)

OS - Operating System

OVAL - Open Vulnerability Assessment Language

P

PACS - Physical Access Control Systems

PBX - Private Branch Exchange

PAM - Privileged Access Management

PCI - Personal Identity Verification (PIV) Card Issuers

PCLIA - Privacy and Civil Liberties Impact Assessment

PDF - Portable Document Format

PEAP - Protected Extensible Authentication Protocol

Personally Identifiable Information (PII) - Refer to IRM 10.8.1.4.16.1.3 Personally Identifiable Information (PII) within this IRM for a definition.

Personal Identification Number (PIN) - An alphanumeric code or password used to authenticate an identity.

Personal Identity Verification (PIV) - The process of creating and using a government wide secure and reliable form of identification for federal employees and contractors, in support of HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors.

Personal Identity Verification Card (PIV Card) - Physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) such that a claimed identity of the cardholder may be verified against the stored credentials by another person (human-readable and verifiable) or an automated process (computer-readable and verifiable).

PGLD - Privacy, Governmental Liaison and Disclosure

PHI - Protected Health Information

Exhibit 10.8.1-1 (Cont. 16) (01-28-2025)**Terms and Acronyms**

Physical Separation - Primarily deals with the use of separate devices (firewalls, proxy servers, etc.) with the intent of achieving system segmentation. This can further be augmented by implementing protected distribution system (e.g., steel pipes and guards) and separate sites such as data centers.

Plan of Action and Milestones (POA&M) - A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

PMEF - Primary Mission Essential Functions

PMO - Program Management Office

POC - Point of Contact

POP - Post Office Protocol

Portable Electronic Device (PED) - Any nonstationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes, but is not limited to: laptops, cellular telephones, thumb drives, video cameras, and pagers.

PRA - Paperwork Reduction Act

PRIVACT - Privacy Act of 1974 (P. L. 93-579)

Private Key - The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.

Privileged Account - An account with elevated privileges. Refer to Elevated Privileges.

Program - A program is the process of translating broadly stated mission needs into a set of operational requirements from which specific performance specifications are derived. A program consists of a functional area that supports a Treasury or IRS mission and has associated systems and budgetary resources. A program is an organized set of activities directed towards a common purpose, objective, goal, or understanding proposed by IRS to carry out responsibilities assigned to the organization. Examples of programs include: Compliance, Accounts Management, Submission Processing, production of U.S. currency, asset forfeiture, and bank supervision.

Program Management Controls - Complement the security controls of a system by focusing on the organization-wide information security requirements that are independent of any particular system and are essential for managing information security programs. Organizations are required to implement security program management controls to provide a foundation for the organization's information security program. May also be deemed as common controls by the organization since the controls are employed at the organization level and typically serve multiple systems.

PSO - Personnel Security Office

PTP - Point-to-Point

Public Information - This type of information may be disclosed to the public without restriction, but requires protection against erroneous manipulation or alteration. Example: public website.

Public Key - The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.

Public Key Cryptography - Encryption system that uses a public-private key pair for encryption and/or digital signature.

Exhibit 10.8.1-1 (Cont. 17) (01-28-2025)**Terms and Acronyms**

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.

R

RAFT - Risk Acceptance Form and Tool

Recovery Time Objective (RTO) - The overall length of time a system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business functions.

Remediation - The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, or uninstalling a software application.

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

Remote Maintenance - Maintenance activities conducted by individuals communicating external to a system security perimeter.

Removable Media - Any type of storage device that can be removed from a computer while the system is still running. Examples include CDs, DVDs, diskettes, and USB drives.

Review - Based on the Government Auditing Standards (2003), the IRS cannot perform self-audits, however, it can perform many of the audit activities in the context of reviews. The IRS reviews are primarily internal control reviews, based on definitions contained within this subsection, and comprised of assessments. This is a significant concept as it should reduce the amount of redundant work possible to conduct a review.

Risk - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (1) the adverse impacts that would arise if the circumstance or event occurs, and (2) the likelihood of occurrence.

Note: System-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Risk Assessment - The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of risk assessment is a list of estimated potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the RMF.

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 considered 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 considered 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).

Risk Management Framework (RMF) - A structured approach used to oversee and manage risk for an enterprise.

Exhibit 10.8.1-1 (Cont. 18) (01-28-2025)**Terms and Acronyms**

Role-Based Access Control (RBAC) - Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

RPA - Robotic Process Automation is a business process automation technology that automates manual tasks that are largely rules based, structured and repetitive using software robots, also known as bots. RPA tools map a process for a robot to follow which allows the bot to operate in place of a human. A RPA may be attended or unattended.

RPO - Recovery Point Objective

S

SA&A - Security Assessment & Authorization

Safeguards - Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for a system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Sanitization - Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.

SAOP - Senior Agency Official for Privacy

SAR - Security Assessment Report

SASE - Secure Access Service Edge

SBOM - Software Bill of Materials

SCADA - Supervisory Control and Data Acquisition

SCRM – Supply Chain Risk Management

Scanning - Refer to Vulnerability Scanning

SDWAN - Software-Defined Wide Area Network

SecOps – Security Operations

Security Area - Consists of either controlled or limited areas, which require individual access authentication to gain entry (per IRM 10.2.14)

Security Attribute - An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the system and are used to enable the implementation of access control and flow control policies, reflect special dissemination, handling or distribution instructions, or support other aspects of the information security policy.

Security Authorization - Refer to Authorization.

Security Category - The characterization of information or a system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation.

Exhibit 10.8.1-1 (Cont. 19) (01-28-2025)**Terms and Acronyms**

Security Content Automation Protocol (SCAP) - A method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation against a standardized set of security requirements.

Security Control Enhancements - Statements of security capability to 1) build in additional, but related, functionality to a basic control; and/or 2) increase the strength of a basic control.

Security Control Inheritance - A situation in which a system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. Refer to Common Control.

Security Controls - The management, operational, and technical control (i.e., safeguards or countermeasures) prescribed for a system to protect the confidentiality, integrity, and availability of the system and its information.

Security Domain - A collection of entities to which applies a single security policy executed by a single authority.

Security Information and Event Management (SIEM) Tool - Application that provides the ability to gather security data from system components and present that data as actionable information via a single interface.

Security Requirements - Requirements levied on a system that are derived from applicable laws, executive orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Security Role - An individual performing computer security responsibilities in some form or fashion. Refer to IRM 10.8.2 for additional roles and responsibilities guidance.

Security Test & Evaluation (ST&E) - Examination and analysis of the safeguards required to protect a system, as they have been applied in an operational environment, to determine the security posture of that system.

SEID - Standard Employee Identifier

Self-Assessment - A method for agency officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. For a self-assessment to be effective, a risk assessment must be conducted in conjunction with, or prior to the self-assessment. A self-assessment does not eliminate the need for a risk assessment.

SEMS - Secure Enterprise Messaging System

Senior Agency Information Security Officer (SAISO) - Official responsible for carrying out the CIO responsibilities under the FISMA and serving as the CIO's primary liaison to the agency's AOs, system owners, and system security officers.

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 USC 552a (the Privacy Act), which could result from inadvertent or deliberate disclosure, alteration, or destruction.

Sensitive Information (NIST SP 800-53) - Information where the loss, misuse, or unauthorized access or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 USC 552a (the Privacy Act); that has not been specifically authorized under criteria established by an EO or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Exhibit 10.8.1-1 (Cont. 20) (01-28-2025)**Terms and Acronyms**

Sensitivity Levels - A graduated system of marking (e.g., LOW, MODERATE, HIGH) information and information processing systems based on threats and risks that result if a threat is successfully conducted.

Service Account - Security accounts that are used by an OS or application to run a service or process. The purpose of the service accounts is to let the associated program login as a service and perform some high-level task even when no one is logged directly into the server.

Service Level Agreement (SLA) - Defines the specific responsibilities of the service provider and sets the customer expectations.

Session - A semi-permanent interactive information interchange, also known as a dialogue, a conversation or a meeting, between two or more communicating devices, or between a computer and user. A session is set up or established at a certain point in time, and torn down at a later point in time. An established communication session may involve more than one message in each direction. A session is typically, but not always, stateful, meaning that at least one of the communicating parties needs to save information about the session history in order to be able to communicate, as opposed to stateless communication, where the communication consists of independent requests with responses.

SI - System and Information Integrity

Significant Change - Also referred to as major change – A change that is likely to affect the security state of a system. Significant changes to a system may include for example: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Examples of significant changes to the environment of operation may include for example: (i) moving to a new facility; (ii) adding new core missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new/modified laws, directives, policies, or regulations. If a formal reauthorization action is initiated, the organization targets only the specific security controls affected by the changes and reuses previous assessment results wherever possible. (*NIST SP 800-37 Rev 2, F-7*)

Note: The examples of changes listed above are only significant when they meet the threshold established in the definition of significant change (i.e., a change that is likely to affect the security state of the system).

SMS - Short Message Service

SMTP - Simple Mail Transfer Protocol

SNMP - Simple Network Management Protocol

SOAR - Security, Orchestration, Automation, and Response

SOP - Standard Operating Procedure

SOW - Statement of Work

SP - Special Publication

Sponsor - An individual, separate from the process owner or developer and typically from within the business unit (selected by the business unit), receives authorization to run specific automation and have privileges to access to the production environment using authorized agency IAM services.

SRM - Security Risk Management

SSN - Social Security Number

Exhibit 10.8.1-1 (Cont. 21) (01-28-2025)**Terms and Acronyms**

Standalone - A desktop or laptop computer that is used on its own without requiring a connection to a network. A system that does not require a connection to any other computer for it to use an application (e.g., word processor or spreadsheet program); instead, the application programs stored on its hard drive are used. A standalone computer may be equipped with a printer, scanner, or external zip or hard drive.

STIG - Security Technical Implementation Guide

SWG - Software Web Gateway

System - Refer to Information System

System Administrator (SA) - Individual responsible for the installation and maintenance of a system, providing effective system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures.

System Development Life Cycle (SDLC) - The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

System Owner - Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of a system.

System Security Plan (SSP) - Formal document that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements.

T

Tailoring - The process by which a security control baseline is modified based on the following:

1. The application of scoping guidance;
2. The specification of compensating security controls, if needed; and
3. The specification of IRS-defined parameters in the security controls via explicit assignment and selection statements.

TAS - Taxpayer Advocate Services

TCP/IP - Transmission Control Protocol/Internet Protocol

TCSIRC - Treasury Computer Security Incident Response Center

TD - Treasury Directive

TD P - Treasury Directive Publication

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

TFTP - trivial FTP

Threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or DoS.

TIC - Trusted Internet Connection

Exhibit 10.8.1-1 (Cont. 22) (01-28-2025)**Terms and Acronyms**

TIGTA - Treasury Inspector General Tax Administration

TIN - Taxpayer Identification Number

Tour of Duty - A tour of duty consists of the hours during the day (a daily tour of duty) and the days of an administrative workweek (a weekly tour of duty) that constitutes an employee's regularly scheduled administrative workweek. (Refer to IRM 6.610.1.2.1, Establishing and Recording the Tour of Duty)

Training - Training is more formal than "awareness," having the goal of building knowledge and skills to facilitate security in one's job performance. The training level strives to produce relevant and needed security skills and competency by practitioners whose functional specialties are other than IT security (e.g., management, systems design, development, acquisition, auditing). Current training guidance encourages Role-Based Training.

Transport Layer Security (TLS) - An authentication and security protocol widely implemented in browsers and Web servers.

Treasury System - A system that is:

- a. Owned, leased, or operated by the IRS, departmental offices (DO), OIG and TIGTA, or a component thereof.
- b. Operated by a contractor on behalf of an IRS, DO, OIG, or a component thereof.

Trust Boundary - A border between two connected zones with different trust levels.

Trusted Network - The networks inside an organization's security perimeter.

TSSSOC - Treasury Shared Services Security Operations Center

TT&E - Testing, Training, and Exercise

U

USC - United States Code

UDP - User Datagram Protocol

UEBA - User and Entity Behavior Analytics

UEFI - Unified Extensible Firmware Interface

UHF - Ultra High Frequency

Unauthorized Personnel - Applies to all IRS personnel not cleared with a requirement to access information systems (IS) for performing or assisting in a lawful and authorized government function.

UNAX - Unauthorized Access

Uninterruptible Power Supply (UPS) - An electrical system or mechanism that provides emergency power when there is a failure of the main power source.

Unix - An operating system well known for its relative hardware independence and portable application interfaces. The different versions of Unix fall into the following three branches: System V, BSD Unix, and Open systems. Some of the popular Unix derivatives are: Linux, Solaris, HP-UX, and AIX.

Unprivileged Network Account - Any account that is not classified as a privileged network account.

UNS - User and Network Services

Exhibit 10.8.1-1 (Cont. 23) (01-28-2025)**Terms and Acronyms**

URL - Uniform Resource Locator

USB - Universal Serial Bus

User - Refer to IRS Personnel

USGCB - United States Government Configuration Baseline

USGv6 - Developed by NIST, it is the technical basis (standards and testing) to facilitate broad US Government (USG) initiatives in IPv6 adoption. The USGv6 Program provides a standards profile and product test program to facilitate the trustworthy acquisition of IPv6 enabled networked information technology products and services. The USGv6 Profile and USGv6 Test Program were designed to leverage and align to the maximum extent possible existing industry-led efforts on product test and certification and other profiling and testing efforts at the time.

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 a system and its resources.

UTC - Coordinated Universal Time

V

VHF - Very High Frequency

Verification - Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome). (CNSSI No. 4009)

Virtual Private Network (VPN) - A virtual network, built on top of existing physical networks that provide a secure communications tunnel for data and other information transmitted between networks.

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

Vulnerability Assessment - Formal description and evaluation of the vulnerabilities in a system.

Vulnerability & Patch Management - Patch management supports Vulnerability Management as a means to automate patching of software in response to vendor-discovered vulnerabilities. Effective patch management is a key (but not the only) requirement for effective vulnerability management. Vulnerability Management uses automated tools to find CVEs that are included in a report to be fixed, but does not itself focus on their remediation. Patch management tools often report what patches are present and assist with the automated patching of systems, but these tools do not necessarily correlate what they detect on systems to a set of known vulnerabilities.

Vulnerability Scanning - The process of proactively identifying vulnerabilities of a 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.

W

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

Exhibit 10.8.1-1 (Cont. 24) (01-28-2025)**Terms and Acronyms**

WAN - Wide Area Network

Web Conferencing - The utilization of technologies to conduct live meetings or presentations via the internet whereby each participant's computer is connected to other participants via the internet. Such a connection can be achieved either by downloading and installing an application onto each participant's computer or by accessing a web-based application via an internet browser.

White List - A list of discrete entities, such as hosts or applications that are known to be benign and are approved for use within an organization and/or system.

WLAN - Wireless Local Area Network

WORM - Write-Once-Read-Many

WWW - World Wide Web

X

XDR - Extended Detection and Response

XML - Extensible Markup Language

Z

Zero Trust (ZT) - Provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. (*NIST SP 800-207*)

Zero Trust Architecture (ZTA) - An enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan. (*NIST SP 800-207*)

Exhibit 10.8.1-2 (12-13-2022)**Related Resources****Public Law**

- Public Law 81-754, *Federal Records Act of 1950*, (Public Law 113-187, 2014 Amendments)
- Public Law 93-579, *Privacy Act of 1974*, as Amended (PRIVACT)
- Public Law 97-255, *Federal Managers' Financial Integrity Act (FMFIA) of 1982*
- Public Law 99-474, *The Computer Fraud and Abuse Act of 1986*
- Public Law 100-235, *Computer Security Act of 1987*
- Public Law 104-13, *Paperwork Reduction Act of 1995*
- Public Law 104-106, *National Defense Authorization Act for Fiscal Year*
- Public Law 105-35, *Taxpayer Browsing Protection Act of 1997*
- Public Law 106-398, *Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001*
- Public Law 107-347, *E-Government Act of 2002*, December 17, 2002
- Public Law 113-283, *Federal Information Security Modernization Act of 2014*, December 18, 2014
- Public Law 115-435, *Foundations for Evidence-Based Policymaking Act of 2018*, January 2019 (EVIDACT)

Executive Order

- Executive Order 10450: *Security Requirements for Government Employment*, April 27, 1953
- Executive Order 13010: *Critical Infrastructure Protection*, July 15, 1996
- Executive Order 13025: *Further Amendment to Executive Order 13010, as Amended, Critical Infrastructure Protection*, November 13, 1996
- Executive Order 13041: *Further Amendment to Executive Order 13010, as Amended, Critical Infrastructure Protection*, April 8, 1997
- Executive Order 13064: *Further Amendment to Executive Order 13010, as Amended, Critical Infrastructure Protection*, October 11, 1997
- Executive Order 13077: *Further Amendment to Executive Order 13010, as Amended, Critical Infrastructure Protection*, March 10, 1998
- Executive Order 13138: *Continuance of Certain Federal Advisory Committee*, September 30, 1999
- Executive Order 13526: *Classified National Security Information*, December 29, 2009
- Executive Order 13556: *Controlled Unclassified Information (CUI)*, November 4, 2010
- Executive Order 13587: *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, October 7, 2011
- Executive Order 13800: *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017
- Executive Order 13960: *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, December 3, 2020
- Executive Order 14028: *Improving the Nation's Cybersecurity*, May 12, 2021

Presidential Decision Directive (PDD)

- PDD 63, *Critical Infrastructure Protection*, May 22, 1998

Office of Management and Budget (OMB) Circular

- OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, August 6, 2022
- OMB Circular No. A-123, *Management's Responsibility for Internal Control*, December 21, 2004
- OMB Circular No. A-130, *Management Information as a Strategic Resource*, July 27, 2016

Office of Management and Budget (OMB) Memoranda

Exhibit 10.8.1-2 (Cont. 1) (12-13-2022)**Related Resources**

- OMB M-99-18, *Privacy Policies on Federal Web Sites*, June 2, 1999
- OMB M-01-05, *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy*, December 20, 2000
- OMB M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, June 25, 2010
- OMB M-14-03, *Enhancing the Security of Federal Information and Information Systems*, November 18, 2013
- OMB M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for Federal Civilian Government*, October 30, 2015
- OMB M-16-24, *Role and Designation of Senior Agency Officials for Privacy*, September 15, 2016
- OMB M-17-06, *Policies for Federal Agency Public Websites and Digital Services*, November 8, 2016
- OMB M-17-09, *Management of Federal High Assets*, December 9, 2016
- OMB M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017
- OMB M-17-15, *Rescission of Memoranda Related to Identity Management*, January 19, 2017
- OMB M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, December 10, 2018
- OMB M-19-13, *Category Management: Making Smarter Use of Common Contract Solutions and Practices*, March 20, 2019
- OMB M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, May 21, 2019
- OMB M-19-23, *Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance*, July 10, 2019
- OMB M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*, September 12, 2019
- OMB M-21-04, *Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act*, November 12, 2020
- OMB M-21-07, *Completing the Transition to Internet Protocol Version 6 (IPv6)*, November 19, 2020
- OMB M-21-30, *Protecting Critical Software Through Enhanced Security Measures*, August 10, 2021
- OMB M-21-31, *Improving the Federal Governments Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, August 27, 2021
- OMB M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*, October 8, 2021
- OMB M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, January 26, 2022
- OMB M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, September 14, 2022
- OMB M-23-02, *Migrating to Post-Quantum Cryptography*, November 18, 2022
- OMB M-23-03, *FY23 FISMA Guidance*, December 2, 2022
- OMB M-23-10, *The Registration and Use of .gov Domains in the Federal Government*, February 8, 2023
- OMB M-23-16, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, June 9, 2023
- OMB M-24-04, *FY24 FISMA Guidance*, December 4, 2023

The listed OMB Circulars and Memos are available on the White House website.

Federal Regulations

- Federal Telecommunications System 2000 (FTS 2000)
- Federal Acquisition Regulation (FAR)

Exhibit 10.8.1-2 (Cont. 2) (12-13-2022)**Related Resources**

- Federal Management Regulation (FMR)

Department of the Treasury Publications

- Department of the Treasury OCIO - Cybersecurity, Version 4.0, *Departmental Incident Response Plan*, May 23, 2023
- TD P 15-71, *Department of the Treasury Security Manual*, June 17, 2011
- TD P 85-01, Version 3.1.3, *Treasury Information Technology Security Program*, February 28, 2022
- Treasury Order (TO) 105-20, *Insider Threat Program*, January 6, 2020
- TD 80-05, *Records and Information Management Program*, June 26, 2002

Federal Risk and Authorization Management Program (FedRAMP)

- FedRAMP, U.S. Chief Information Officer, Office of Management & Budget (*Federal Cloud Computing Strategy*)
- *FedRAMP* website
- *FedRAMP Knowledgebase*

IRS Publications

- Document 12829, **General Records Schedules (GRS)**
- IRM 1.15, *Records and Information Management* series
- IRM 2.5, *Systems Development* series
- IRM 2.7.1, *Information Technology (IT) Operations, Inter-Center*
- IRM 2.25, *Integrated Enterprise Portal - Web Services* series
- IRM 2.31.1, *Lifecycle Management, One Solution Delivery Life Cycle (OneSDLC) Guidance*
- IRM 2.149, *IT Asset Management* series
- IRM 2.150.2, *Configuration Management, Configuration Management (CM) Process*
- RM 6.610.1, *Hours of Duty, IRS Hours of Duty*
- IRM 6.751.1, *Discipline and Disciplinary Actions: Policies, Responsibilities Authorities, and Guidance*
- IRM 6.752, *Disciplinary Suspensions and Adverse Actions* series
- IRM 10.2, *Physical Security Program* series
- IRM 10.5, *Privacy and Information Protection* series
- IRM 10.6, *Continuity Operations* series
- IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*
- IRM 10.8.5, *Information Technology (IT) Security, Domain Name System (DNS) Security Policy*
- IRM 10.8.13, *Information Technology (IT) Security, Business Impact Analysis (BIA) Security Policy*
- IRM 10.8.15, *Information Technology (IT) Security, General Platform Operating System Security Policy*
- IRM 10.8.22, *Information Technology (IT) Security, Web Server Security Policy*
- IRM 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy*
- IRM 10.8.26, *Information Technology (IT) Security, Wireless and Mobile Device Security Policy*
- IRM 10.8.50, *Information Technology (IT) Security, Enterprise Incident, Vulnerability, and Security Patch Management*
- IRM 10.8.52, *Information Technology (IT) Security, IRS Public Key Infrastructure (PKI) X.509 Certificate Policy*
- IRM 10.8.54, *Information Technology (IT) Security, Minimum Firewall Administration Requirements*
- 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 Systems Contingency Plan (ISCP) and Disaster Recovery (DR) Testing, Training, and Exercise (TT&E) Program*

Exhibit 10.8.1-2 (Cont. 3) (12-13-2022)**Related Resources**

- IRM 10.8.63, *Information Technology (IT) Security, Central Log Server Security Policy*
- IRM 10.9.1, *National Security Information, Classified National Security Information (CNSI)*
- IRM 10.23.1, *Personnel Security, National Security Positions and Access to Classified Information*
- IRM 10.23.2, *Personnel Security, Contractor Investigations*
- IRM 10.23.3, *Personnel Security, Personnel Security/Suitability for Employment and Personnel Security Operations*
- IRM 11.3.1, *Disclosure of Official Information, Introduction to Disclosures*
- IRM 11.3.24, *Disclosure of Official Information, Disclosures to Contractors*
- IRM 13.1, *Taxpayer Advocate Case Procedures series*
- IRM 21.1, *Accounts Management and Compliance Services Operations series*
- IRS Ethics Handbook, Document 12011
- IRS Managers Guide to Penalty Determinations, Document 11500
- IRS Publication 4812, *Contractor Security & Privacy Controls - Handling and Protecting Information or Information Systems*
- Policy Statement 2-90 (formerly P-1-144), *Designing safeguards for computer systems* (located at IRM 1.2.1.3.2)

The IRS Office of Service-wide Policy, Directives and Electronic Research (SPDER), in partnership with LEXIS-NEXIS, has made all IRMs available to all IRS employees.

IRMs are available on the *IMD IRM Numerical Index* site.

Cybersecurity IRMs are available on the *IRM Part 10 Security, Privacy, Assurance and Artificial Intelligence* site.

General Accounting Office (GAO)

- *Executive Guide on Information Security Management*, May 1998
- *Information Security Risk Assessment, Practices of Leading Organizations*, November 1999
- *Federal Information System Controls Audit Manual (FISCAM)*, February 2009

The listed GAO publications are available on the GAO website.

National Institute of Standards and Technology (NIST) Publications

- *FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors*, January 2022
- *NIST FIPS 140-2, Security Requirements for Cryptographic Modules*, December 3, 2002
- *NIST FIPS 140-3, Security Requirements for Cryptographic Modules*, March 22, 2019
- *NIST FIPS 199, Standards for Security Categorization of Federal Information and Information Systems*, February 1, 2004
- *NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems*, March 1, 2006
- *NIST SP 800-207, Zero Trust Architecture*, August 2020
- *NIST SP 800-189, Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation*, December 2019
- *NIST SP 800-166, Derived PIV Application and Data Model Test Guidelines*, June 6, 2016
- *NIST SP 800-161, Revision 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, May 2022
- *NIST SP 800-160 Volume 1 Revision 1, Engineering of Trustworthy Secure Systems*, November 2022
- *NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs)*, February 2012
- *NIST SP 800-152, A Profile for U. S. Federal Cryptographic Key Management Systems*, October 2015
- *NIST SP 800-147, BIOS Protection Guidelines*, April 2011

Exhibit 10.8.1-2 (Cont. 4) (12-13-2022)**Related Resources**

- *NIST SP 800-146, Cloud Computing Synopsis and Recommendations*, May 2012
- *NIST SP 800-145, The NIST Definition of Cloud Computing*, September 2011
- *NIST SP 800-144, Guidelines on Security and Privacy in Public Cloud Computing*, December 2011
- *NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011
- *NIST SP 800-126, Revision 3, The Technical Specifications for the Security Content Automation Protocol (SCAP): SCAP Version 1.3*, February 2018
- *NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010
- *NIST SP 800-119, Guidelines for the Secure Deployment of IPv6*, December 2010
- *NIST SP 800-116 Revision 1, Guidelines for the Use of PIV Credentials in Facility Access*, June 2018
- *NIST SP 800-115, Technical Guide to Information Security Testing and Assessment*, September 2008
- *NIST SP 800-88, Revision 1, Guidelines for Media Sanitization*, December 2014
- *NIST SP 800-84, Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006
- *NIST SP 800-81-2, Secure Domain Name System (DNS) Deployment Guide*, September 2013
- *NIST SP 800-79-2, Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*, July 2015
- *NIST SP 800-78-4, Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, May 2015
- *NIST SP 800-76-2, Biometric Specifications for Personal Identity Verification*, July 2013
- *NIST SP 800-73-4, Interfaces for Personal Identity Verification*, May 2015 (Updated 2/8/2016)
- *NIST SP 800-70 Revision 4, National Checklist Program for IT Products-Guidelines for Checklist Users and Developers*, May 2018
- *NIST SP 800-63-3, Digital Identity Guidelines*, June 2017
- *NIST SP 800-63B, Digital Identity Guidelines: Authentication and Lifecycle Management*, March 2, 2020
- *NIST SP 800-63A, Digital Identity Guidelines: Enrollment and Identity Proofing*, March 2, 2020
- *NIST SP 800-61 Revision 2, Computer Security Incident Handling Guide*, August 2012
- *NIST SP 800-57 Part 3 Revision 1, Recommendation for Key Management, Part 3 Application-Specific Key Management Guidance*, January 2015
- *NIST SP 800-53 Revision 5.1.1, Security and Privacy Controls for Federal Information Systems and Organizations*, September 2020 (Updated 11/07/2023)
- *NIST SP 800-53A Revision 5, Assessing Security and Privacy Controls in Information Systems and Organizations*, January 2022
- *NIST SP 800-53B, Control Baselines for Information Systems and Organizations*, October 2020 (Updated 12/10/2020)
- *NIST SP 800-52 Rev 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, August 29, 2019
- *NIST SP 800-47 Rev 1, Managing the Security of Information Exchanges*, July 2021
- *NIST SP 800-45 Ver 2, Guidelines on Electronic Mail Security*, February 2007
- *NIST SP 800-41 Revision 1, Guidelines on Firewalls and Firewall Policy*, September 2009
- *NIST SP 800-40 Rev 4, Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technologies*, April 2022
- *NIST SP 800-37 Revision 2, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach for Security and Privacy*, December 20, 2018
- *NIST SP 800-34 Revision 1, Contingency Planning Guide for Federal Information Systems*, November 11, 2010
- *NIST SP 800-30 Revision 1, Guide for Conducting Risk Assessments*, September 2012

Exhibit 10.8.1-2 (Cont. 5) (12-13-2022)**Related Resources**

- *NIST SP 800-28 Version 2, Guidelines on Active Content and Mobile Code*, March 2008
- *NIST SP 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems*, February 2006
- *NIST SP 800-12 Revision 1, An Introduction to Computer Security: The NIST Handbook*, June 2017
- *NIST Publications*.

Other Publications

- National Security Agency, Information Systems Security Organization, *Controlled Access Protection Profile*, October 1999
- National Information Assurance Certification and Accreditation Process (NIACAP), NSTISSI No. 1000, April 2000
- National Information Assurance Partnership (NIAP), *Security Requirements Profiling*, August 2000
- Security, Privacy, and Critical Infrastructure Committee, Federal Information Technology Security Assessment Framework, November 2000
- Security, Privacy, and Critical Infrastructure Committee, *Securing Electronic Government*, January 2001
- NARA, *Controlled Unclassified Information (CUI) Office Notice 2011-01: Initial Implementation Guidance for Executive Order 13556*, June 2011
- NARA, *General Records Schedules (GRS)*
- CISA, *Cloud Security Technical Reference Architecture*, Version 2.9, June 2022
- CISA BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible System*, April 2019
- CISA BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, November 2021
- CISA BOD 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks*, October 2022
- CISA BOD 23-02, *Mitigating the Risk from Internet-Exposed Management Interfaces*, June 2023
- Code of Federal Regulations, Title 32, *Controlled Unclassified Information* (32 C.F.R. 2002)
- DHS TIC – Department of Homeland Security, *Trusted Internet Connections (TIC)*

