



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.2

APRIL 29, 2025

EFFECTIVE DATE

(04-29-2025)

PURPOSE

- (1) This transmits revised IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*.

MATERIAL CHANGES

- (1) 10.8.1.1.1 Background: Original (1) removed as it duplicated language already in the Authority subsection.
- (2) 10.8.2.1.4 Roles and Responsibilities: Original (2) incorporated into (1).
- (3) IRM 10.8.2.1.4 Program Management and Review: (2) New informative language added.
- (4) IRM 10.8.2.1.7 Related Resources: (1) Informative language added to existing paragraph.
- (5) IRM 10.8.2.2 Risk Acceptance and Risk-Based Decisions (RBD):
 - Subsection title updated.
 - (2) Note - RBD document reference updated.
- (6) IRM 10.8.2.3 IT Security Roles and Responsibilities: New (4) Conflict of interest language added from NIST SP 800-37 and 800-100.
- (7) IRM 10.8.2.3.1.1 Agency Head:
 - (1) Updated to align with NIST SP 800-37.
 - (2) Updated to align with NIST SP 800-37. Original (5)a), (4)c), and (4)d) incorporated.
 - (3) New language from NIST SP 800-37 added.
 - (4) New language from NIST SP 800-37 added.
 - (5) Updated to align with TD P 85-01.
 - (6) Language from original (4) and (5) combined, and updated to align with FISMA.
 - (7) New language from P.L. 115-435.
- (8) IRM 10.8.2.3.1.2 Chief Information Officer (CIO):
 - (1) Replaced non-specific language with TD P 85-01 language.
 - (2) Updated to align with TD P 85-01.
 - (4) Updated to align with Taxpayer First Act.
 - (5) Updated to align with NIST SP 800-37.
 - (6) Added NIST SP 800-37 language and incorporated original (7)c), d), e), f), j).
 - (7) New RMF language from NIST SP 800-37 added.
 - (8) Updated to align with Treasury's Incident Response Plan.
 - (9) Updated to align with Treasury's Incident Response Plan.
 - (10) Updated to align with TD 85-02.
 - (11) New language from EO 13833 added.
 - Original (9) Removed duplicate language already address by TD P 85-01.
 - (12) Updated to align with FISMA.
 - (13) Updated to align with NIST SP 800-137.

- (9) IRM 10.8.2.3.1.3 Chief Data Officer (CDO): New subsection and CDO responsibilities from Foundations for Evidence-Based Policymaking Act added.
- (10) IRM 10.8.2.3.1.4 Senior Agency Information Security Officer (SAISO)/Chief Information Security Officer (CISO):
- (3) Original (3)b) language.
 - (4) Updated to align with TD P 85-01.
 - (6) Removed duplicate CSIRC language.
 - (7) New Treasury Incident Response Plan language added.
 - (8) Updated to align with FISMA.
 - (9) New RMF language from NIST SP 800-37.
 - Original (7) removed. Duplicated language already address by TD P 85-01.
 - Original (8) removed. Duplicated language already address by TD P 85-01.
 - Original (9) removed as part of IGM 10-IT-0824-0013 revisions.
 - Original (10) removed. Repetitive reference to IRM 10.8.27.
 - Original (11) removed. Duplicated TD P 85-01 and NIST SP 800-53.
- (11) IRM 10.8.2.3.1.4.1 Security Control Assessor:
- (1) Updated to align with TD P 85-01 and original (2) incorporated.
 - (2) New TD P 85-01 language added.
 - (3) Updated to align with TD P 85-01.
 - (4) Updated to align with NIST SP 800-37.
 - (5) New RMF language from NIST SP 800-37 added.
 - (6) New NIST SP 800-137 language added.
 - Original (3) removed duplicated language already address by TD P 85-01.
 - Original (5) removed.
- (12) IRM 10.8.2.3.1.4.2 Risk Executive (Function):
- (1) Updated to align with TD P 85-01.
 - (2) New TD P 85-01 language added.
 - (3) New TD P 85-01 language added.
- (13) IRM 10.8.2.3.1.4.3 Common Control Provider:
- (1) Updated to align with NIST SP 800-37.
 - (2) Updated to align with NIST SP 800-37.
 - (3) New NIST SP 800-37 language added.
- (14) IRM 10.8.2.3.1.5 Senior Management/Executives:
- (1) Updated to align with OMB A-130 and original (4) incorporated.
 - Original (3) removed guidance established via the AO responsibilities.
- (15) IRM 10.8.2.3.1.6 System Owner:
- Subsection title updated; removed Mission or Business Owner from title and aligned with NIST SP 800-37 and 800-53.
 - (1) Updated to align with NIST SP 800-37.
 - (1)a) Moved to new Mission or Business Owner subsection.
 - (2) New NIST SP 800-39 language added.
 - (3) New NIST SP 800-18 language added.
 - (4) Original (3)a) relocated to be a separate paragraph.
 - (6) Updated to align with NIST SP 800-37 and removed redundant language.

- (7) New RMF language from NIST SP 800-37 added.
 - (8) New NIST SP 800-34 language added.
 - (10) New NIST SP 800-18 language added.
 - Original (5) removed duplicated language.
 - Original (6) removed duplicated language in IRM 10.8.60 and 10.8.62.
 - Original (7) removed duplicated language in IRM 10.8.60 and procedural guidance found in a contingency plan.
 - Original (8) removed duplicated language.
 - Original (9) removed duplicated language in IRM 10.8.21.
 - Original (10) removed duplicated language in IRM 10.8.6.
 - Original (11) removed duplicated language in IRM 10.8.15.
 - Original (12) removed duplicated language in IRM 10.8.15.
 - Original (13) removed duplicated language in IRM 10.8.22.
 - Original (14) removed duplicated language in IRM 10.8.50.
 - Original (15) removed IRM 10.8.54 reference.
- (16) IRM 10.8.2.3.1.7 Mission or Business Owner:
- New subsection created.
 - (1) New NIST SP 800-37 language added.
 - (2) New NIST SP 800-37 language added.
 - (3) Original 10.8.2.3.1.3.5 (1)a) incorporated; conflict of interest language added.
- (17) IRM 10.8.2.3.1.8 Information Owner:
- (1) Updated to align with NIST SP 800-37.
 - (2) Original (2)a) relocated to be a separate paragraph.
 - (4) New NIST SP 800-37 language added.
 - (6) New RMF NIST SP 800-37 language added.
- (18) IRM 10.8.2.3.1.9 Authorizing Official (AO):
- (2) Original (2)a) relocated to be a separate paragraph.
 - (6) Updated to align with NIST SP 800-137.
- (19) IRM 10.8.2.3.1.9.1 Authorizing Official Designated Representative (AODR):
- (1) Updated to align with NIST SP 800-37.
 - (5) New RMF NIST SP 800-37 language added.
 - Original (2) Removed AO responsibility.
- (20) IRM 10.8.2.3.1.10 Chief Acquisition Officer (CAO):
- New subsection added.
 - New NIST SP 800-37 language added.
- (21) IRM 10.8.2.3.1.11 System Security Officer:
- Subsection title changed to align with NIST SP 800-37 and 800-53.
 - (1) Language from TD P 85-01 added.
 - (2) Original (5)b) relocated to be a separate paragraph.
 - (3) Original (1)a) relocated to be a separate paragraph.
 - (4) Updated to align with TD P 85-01.
 - (7) Original (8)a) relocated to be a separate paragraph.
 - (8) Updated to align with Treasury ISCM framework.
 - (9) New NIST SP 800-12 language added.

- (10) New NIST SP 800-37 language added.
 - (11) New NIST SP 800-37 RMF language added.
 - (12) New NIST SP 800-37 RMF support language added.
 - Original (2) Removed redundant language.
 - Original (3) Removed redundant language addressed by TD P 85-01 and NIST SP 800-37.
 - Original (4) Removed redundant language addressed by NIST SP 800-37.
 - Original (5) Removed redundant language addressed by NIST SP 800-37.
- (22) IRM 10.8.2.3.1.12 Managers:
- Subsection title updated to align with TD P 85-01.
 - Original (3) Removed obsoleted language; NIST SP 800-16 has been obsoleted.
 - Original (4) Removed redundant language addressed by TD P 85-01.
- (23) IRM 10.8.2.3.1.13 Contracting Officer: (4) Added NIST SP 800-12 language added.
- (24) IRM 10.8.2.3.1.13.1 Contracting Officer's Representative (COR):
- Subsection title corrected.
 - (1) Updated to align with FAR.
 - Original (3) Removed obsoleted language; NIST SP 800-16 has been obsoleted.
 - Original (4) Removed duplicate language addressed by contracting officer guidance.
- (25) IRM 10.8.2.3.1.14 Enterprise Architect:
- (1) New NIST SP 800-37 language added.
 - (3) New RMF NIST SP 800-37 language added.
 - Original (1) and (2) Removed none enterprise architect language.
- (26) IRM 10.8.2.3.1.15 Systems Security Engineer:
- Subsection title updated to align with NIST SP 800-37.
 - (1) Updated to align with NIST SP 800-37.
- (27) IRM 10.8.2.3.1.16 Security and Privacy Architect:
- New subsection added to align with NIST SP 800-37.
 - (1), (2), (3), (4), & (5) New NIST SP 800-37 language added.
- (28) IRM 10.8.2.3.1.17 Chief Financial Officer (CFO):
- (1) Updated to align with NIST SP 800-100.
 - Original (2) Removed CFO Act of 1990 language relevant to the Treasury CFO.
- (29) IRM 10.8.2.3.1.18 Privacy Officer:
- (1) Updated to align with OMB A-130.
 - (3) New NIST SP 800-37 RMF language added.
 - (4) New OMB A-130 language added.
 - (5) Updated to align with Treasury Incident Response Plan.
 - (3) New NIST SP 800-53 language added.
 - Original (4) Removed reference to an exhibit that has been removed.
- (30) IRM 10.8.2.3.1.18.1 IRS Privacy Offices: Original (1)e) Removed reference to an exhibit that has been removed.
- (31) IRM 10.8.2.3.1.18.2 System Privacy Officer:

- New subsection added.
 - (1) New NIST SP 800-37 language added.
 - (2) New RMF NIST SP 800-37 language added.
- (32) IRM 10.8.2.3.1.19 Physical Security Officer:
- (1) Original (1) & (2) combined and updated to align with NIST SP 800-100.
 - Original (3) Removed redundant language addressed by NIST SP 800-100.
 - Original (6) Removed reference.
- (33) IRM 10.8.2.3.1.20 Personnel Security Officer:
- (1) Updated to align with NIST SP 800-100.
 - (3) Updated to align with NIST SP 800-100.
- (34) IRM 10.8.2.3.1.21 Employee:
- (3) Updated to align with TD P 85-01.
 - (4) New NIST SP 800-37 language added.
 - (5) Removed duplicate language; language updated for clarification.
 - Original (5) Removed duplicate guidance; (5)b) incorporated into original (4).
 - Original (7) Removed language addressed in IRM 10.8.27.
 - Original (8) Removed reference.
- (35) IRM 10.8.2.3.1.22 Contractor:
- (2) Added new TD P 85-01 language.
 - (3) Updated to align with TD P 85-01.
 - (4) Added new TD P 85-01 language.
 - (5) Removed duplicate language; language updated for clarification.
 - (7) Added reference to IRM 10.8.27.
 - Original (4) Removed duplicate language; original (4)b) incorporate into original (3)
- (36) IRM 10.8.2.3.1.24 Key-Recovery Agent:
- Subsection title updated to align with NIST SP 800-130.
 - (1) New NIST SP 800-130 language added.
 - (2) New NIST SP 800-130 language added.
 - (3) Updated to align with NIST SP 800-130 language.
 - Original (1), (2), (3), & (4) Removed generalized (non-responsibility) language.
- (37) IRM 10.8.2.3.1.34 Integrated Data Retrieval System (IDRS) Security Analyst: Responsibilities relocated to IRM 10.8.34.
- (38) IRM 10.8.2.3.1.35 Integrated Data Retrieval System (IDRS) Security Account Administrator: Responsibilities relocated to IRM 10.8.34.
- (39) IRM 10.8.2.3.1.36 Computer Audit Specialist (CAS): Subsection title updated.
- (40) IRM 10.8.2.3.2.1 IRS Information Technology Cybersecurity Organization: (5) Language relocated from 10.8.1.4.4.2.1 (5) incorporated into the subsection.
- (41) IRM 10.8.2.3.2.2 IRS Information Technology User (IT) and Network Services (UNS) Organization:
- Subsection title updated.
 - (7) Language relocated from 10.8.1.4.4.2.1 (4) incorporated into the subsection.

- (42) IRM 10.8.2.3.2.3 Computer Security Incident Response Center (CSIRC): (3)f) Removed reference to exhibit that has been removed.
- (43) IRM 10.8.2.3.2.5 IRS Patch and Vulnerability Group (PVG):
- (1) Original (1)a) relocated to be a separate paragraph. New language added from NIST SP 800-40 language pertaining to PVG's function.
 - (2) Updated to align with NIST SP 800-40r2 language. Note added to provide insight into the NIST SP 800-40 revisions and how they build on each other.
- (44) Exhibit 10.8.2-1 Roles that Require Specialized Training: IG Memo IT-10-0424-0008 revisions incorporated. Incorporates NICE Framework language.
- (45) Original Exhibit 10.8.2-2 Incident, Breach, and Event Definitions: Definitions incorporated into Exhibit 10.8.2-2 Terms and Acronyms.
- (46) Exhibit 10.8.2-2 Terms and Acronyms:
- The following acronyms were added: AODR, CAO, CDO, CISA, CNSI, EFO, IRB, NICE, SA, SSE, and SSO.
 - The following acronyms were removed: BIA, BR, CCRB, CFR, COTS, EC&MA, EOPS OSPMO, EOPS SOSD, FEA, GSP, ISSE, IUUD, KISAM, MOA, MOU, NOSS, NSI, OGE, OPM, SSP, and USR.
 - ATO acronym corrected.
 - Availability definition revised.
 - Breach definition incorporated from original Exhibit 10.8.2-2.
 - Campus IDRS Security Officer definition removed.
 - Certification Authority acronym and definition removed.
 - Chief Information Officer (CIO) definition removed; duplicated language in the CIO subsection.
 - Contingency Plan definition revised.
 - Controlled Unclassified Information (CUI) acronym and definition added.
 - Cyber Event definition incorporated from original Exhibit 10.8.2-2.
 - Denial of Authorization definition removed.
 - Department definition removed.
 - Disaster Recover Plan (DRP) acronym and definition removed.
 - DMZ definition added to acronym.
 - Ensure definition added.
 - FISMA acronym corrected and definition revised.
 - Form 14201 definition removed.
 - Identification definition revised.
 - Impact definition revised.
 - Impact Level definition added.
 - Incident definition incorporated from original Exhibit 10.8.2-2.
 - Incident Handling definition revised.
 - Information Owner definition removed.
 - Information System Owner definition removed.
 - Information System Security Officer (ISSO) definition removed; Reference to new SSO acronym added.
 - ISCM acronym added to Information Security Continuous Monitoring definition title.
 - Information Technology (IT) definition revised.
 - Integrity definition revised.
 - Key Pair definition removed.
 - Least Privilege definition revised.
 - Live Data definition removed.
 - Major Incident definition incorporated from original Exhibit 10.8.2-2.

- MD5 definition added.
- Memorandum of Agreement (MOA) acronym and definition added.
- Memorandum of Understanding (MOU) acronym and definition added.
- Non-repudiation definition revised.
- Notable Cyber Event definition incorporated from original Exhibit 10.8.2-2.
- Plan of Action and Milestones (POA&M) definition revised.
- Private Key definition revised.
- Public Information definition removed.
- Public Key definition revised.
- Public Key Infrastructure (PKI) acronym and definition removed.
- Remediation definition revised.
- Risk definition revised.
- Risk Assessment definition revised.
- Safeguards definition revised.
- Sensitive Information definition removed; Reference to CUI acronym added.
- Significant Cyber Enter definition incorporated from original Exhibit 10.8.2-2.
- Suspected Breach definition incorporated from original Exhibit 10.8.2-2.
- Suspected Incident definition incorporated from original Exhibit 10.8.2-2.
- System definition revised.
- SSP acronym added to System Security Plan definition.
- Technical Controls definition removed.
- UNS acronym corrected.
- Vulnerability definition revised.
- Vulnerability Assessment definition revised.

(47) Exhibit 10.8.2-3 Related Resources:

- TD P 85-01, Treasury Information Technology Security Programs revised.
- TD 85-02, Treasury Software Piracy Policy added.
- TD 87-04, Personal Use of Government Information Technology Resources revised.
- Treasury, Information Security Continuous Monitoring (ISCM) Framework revised.
- Treasury, Departmental Incident Response Plan (IRP) revised.
- TD P 15-03, Intelligence Information Systems Security Policy Manual removed.
- TCIO Memo 17-01 removed.
- IRM 10.4.x series removed.
- IRM 10.8.1 title revised.
- IRM 10.8.12 added.
- IRM 10.8.13 added.
- IRM 10.8.15 title corrected. IRM 10.8.52 added.
- IRM 10.8.60 title corrected.
- IRM 10.8.63 added.
- IRM 10.9.1 title revised.
- FIPS 199 added.
- NIST SP 800-12 added.
- NIST SP 800-16 removed.
- NIST SP 800-18 revised.
- NIST SP 800-34 added.
- NIST SP 800-37 revised.
- NIST SP 800-39 added.
- NIST SP 800-40 Revision 2 added.
- NIST SP 800-40 Revision 3 revised.
- NIST SP 800-53 revised.
- NIST SP 800-53A removed.
- NIST SP 800-57 removed.

- NIST SP 800-60 Revision 1 Volume I added.
- NIST SP 800-60 Revision 1 Volume II added.
- NIST SP 800-61 removed.
- NIST SP 800-64 removed.
- NIST SP 800-100 revised.
- NIST SP 800-137 added.
- NIST SP 800-160 Volume 1 Revision 1 added.
- NIST SP 800-160 Volume 2 Revision 1 added.
- NIST SP 800-181 added.
- CNSSI 4009 added.
- Title 48 FAR added.
- Executive Order 13833 added.
- Executive Order 13103 added.
- FISMA URL removed.
- OMB M-16-14 added.
- OMB M-20-04 added.
- OMB M-21-13 added.
- OMB A-130 revised.
- Privacy Act of 1974 revised.
- Taxpayer Browsing Protection Act of 1997 revised.
- Chief Financial Officers Act of 1990 added.
- Federal Information Security Modernization Act (FISMA) of 2014 added.
- Consolidated Appropriations Act, 2016 revised.
- Foundations for Evidence-Based Policymaking Act of 2018 added.
- Taxpayer First Act added.
- U.S. Code Title 5 revised.
- U.S. Code Title 31 added.
- U.S. Code Title 44 added.
- Presidential Policy Directive (PPD) 41 removed.
- URLs for public laws, executive orders, OMB memoranda, and U.S. Codes added.

- (48) Editorial changes were made throughout the IRM, to include: reviewing and updating for plain language, grammar, spelling, punctuation, titles, website addresses, legal and IRM references.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 10.8.2 dated November 7, 2023. This IRM incorporates the following interim guidance (IG) memorandums: IT-10-1023-0007, Authorizing Official Designated Representative (AODR), dated January 01, 2024; IT-10-0424-0008, NICE Framework Training, dated August 01, 2024; and IT-10-0824-0013, Senior Agency Information Security Officer (SAISO)/Chief Information Security Officer (CISO) Responsibilities, dated October 01, 2024. This IRM supplements IRM 10.8.1, *Information Technology (IT) Security, Security Policy*.

AUDIENCE

All personnel responsible for ensuring security is provided for IRS information and systems. This IRM applies to all employees, contractors and vendors of the IRS.

Rajiv Uppal
Chief Information Officer

10.8.2

IT Security Roles and Responsibilities

Table of Contents

10.8.2.1 Program Scope and Objectives

10.8.2.1.1 Background

10.8.2.1.2 Authority

10.8.2.1.3 Roles and Responsibilities

10.8.2.1.4 Program Management and Review

10.8.2.1.5 Program Controls

10.8.2.1.6 Terms and Acronyms

10.8.2.1.7 Related Resources

10.8.2.2 Risk Acceptance and Risk-Based Decisions (RBD)

10.8.2.3 IT Security Roles and Responsibilities

10.8.2.3.1 Key Governance and Related Roles & Responsibilities

10.8.2.3.1.1 Agency Head

10.8.2.3.1.2 Chief Information Officer (CIO)

10.8.2.3.1.3 Chief Data Officer (CDO)

10.8.2.3.1.4 Senior Agency Information Security Officer (SAISO)/Chief Information Security Officer (CISO)

10.8.2.3.1.4.1 Security Control Assessor

10.8.2.3.1.4.2 Risk Executive (Function)

10.8.2.3.1.4.3 Common Control Provider

10.8.2.3.1.5 Senior Management/Executives

10.8.2.3.1.6 System Owner

10.8.2.3.1.6.1 Business System Planner (BSP)

10.8.2.3.1.6.1.1 Security Program Management Officer (SPMO)

10.8.2.3.1.7 Mission or Business Owner

10.8.2.3.1.8 Information Owner

10.8.2.3.1.9 Authorizing Official (AO)

10.8.2.3.1.9.1 Authorizing Official Designated Representative (AODR)

10.8.2.3.1.10 Chief Acquisition Officer (CAO)

10.8.2.3.1.11 System Security Officer (SSO)

10.8.2.3.1.12 Manager

10.8.2.3.1.13 Contracting Officer

10.8.2.3.1.13.1 Contracting Officer's Representative (COR)

10.8.2.3.1.14 Enterprise Architect

10.8.2.3.1.15 Systems Security Engineer

10.8.2.3.1.16 Security and Privacy Architect

10.8.2.3.1.17 Chief Financial Officer (CFO)

- 10.8.2.3.1.18 Privacy Officer
 - 10.8.2.3.1.18.1 IRS Privacy Offices
 - 10.8.2.3.1.18.2 System Privacy Officer
- 10.8.2.3.1.19 Physical Security Officer
- 10.8.2.3.1.20 Personnel Security Officer
- 10.8.2.3.1.21 Employee
- 10.8.2.3.1.22 Contractor
- 10.8.2.3.1.23 Database Administrator (DBA)
- 10.8.2.3.1.24 Key-Recovery Agent
- 10.8.2.3.1.25 Network Administrator
- 10.8.2.3.1.26 Program Developer/Programmer
- 10.8.2.3.1.27 Web Developer
- 10.8.2.3.1.28 Resource Access Control Facility (RACF) Specialist
- 10.8.2.3.1.29 Security Specialist (SecSpec)
- 10.8.2.3.1.30 System Administrator (SA)
- 10.8.2.3.1.31 Systems Operations Staff
- 10.8.2.3.1.32 Telecommunications Specialist
- 10.8.2.3.1.33 User Administrator (UA)
- 10.8.2.3.1.34 Integrated Data Retrieval System (IDRS) Security Analyst
- 10.8.2.3.1.35 Integrated Data Retrieval System (IDRS) Security Account Administrator
- 10.8.2.3.1.36 Computer Audit Specialist (CAS)
- 10.8.2.3.1.37 Functional Workstation Specialist
- 10.8.2.3.1.38 Management/Program Analyst
- 10.8.2.3.1.39 System Designer
- 10.8.2.3.1.40 Technical Support Staff (Desktop)
- 10.8.2.3.1.41 Security Staff (Physical Security)
- 10.8.2.3.1.42 Cyber Critical Infrastructure Protection (CIP) Coordinator
- 10.8.2.3.2 Organization/Functional Roles and Responsibilities
 - 10.8.2.3.2.1 IRS Information Technology Cybersecurity Organization
 - 10.8.2.3.2.2 IRS Information Technology (IT) User and Network Services (UNS) Organization
 - 10.8.2.3.2.3 Computer Security Incident Response Center (CSIRC)
 - 10.8.2.3.2.4 Situational Awareness Management Center (SAMC)
 - 10.8.2.3.2.5 IRS Patch and Vulnerability Group (PVG)

Exhibits

- 10.8.2-1 Roles That Require Specialized Training
- 10.8.2-2 Terms and Acronyms
- 10.8.2-3 Related Resources

10.8.2.1
(11-07-2023)
Program Scope and Objectives

- (1) **Overview:** This IRM establishes the information technology (IT) security roles and responsibilities relevant to sensitive information and systems for IRS organizations and employees.
- (2) **Program Purpose:** Develop and publish policies to protect the IRS against potential security threats, risks, and vulnerabilities to ensure compliance with federal mandates and legislation.
- (3) **Audience:** The provisions in this manual apply to:
 - a. All offices and business, operating, and functional units within the IRS.
 - b. Individuals and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, who use or operate systems that store, process or transmit IRS information or connect to an IRS network or system.
- (4) **Policy Owner:** Chief Information Officer
- (5) **Program Owner:** Cybersecurity, Cybersecurity Threat Response and Remediation, an organization within Cybersecurity.
- (6) **Program Goals:** To protect the confidentiality, integrity, and availability of IRS information and systems.

10.8.2.1.1
(04-29-2025)
Background

- (1) IRM 10.8.2 has been aligned to the roles and responsibilities described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-100, *Information Security Handbook: A Guide for Managers* and SP 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- (2) IRM 10.8.2 is part of the IRM 10.8, Information Technology (IT) Security series for IRS IT Cybersecurity.

10.8.2.1.2
(04-29-2025)
Authority

- (1) All IRS systems and applications are required to comply with Executive Orders (EOs), Office of Management and Budget (OMB), Federal Information Security Modernization Act of 2014 (FISMA), NIST, Department of Homeland Security (DHS), Treasury, and IRS guidelines as they apply.
- (2) Treasury Directive Publication (TD P) 85-01, *Department of the Treasury Information Technology Security Program* and federal regulations require senior management/executive officials establish an IT security program, which includes the identification of roles and responsibilities that support IT security.

10.8.2.1.3
(04-29-2025)
Roles and Responsibilities

- (1) The IRS implements IT security roles and responsibilities to ensure the confidentiality, integrity, and availability of its systems, applications, and information. This IRM covers roles and responsibilities that support the IT security program.

Note: Refer to IRM 10.5.1, *Privacy and Information Protection, Privacy Policy*, for a description of privacy roles and responsibilities.
- (2) Although IRM 10.8.2 is intended to be the primary source for general IT security roles and responsibilities, all documents in the 10.8 series, additional applicable policy suites of IRMs and applicable business unit procedural guidance (e.g., standard operating procedures (SOP)) must be carefully

reviewed for an individual to comprehensively understand their role and specific responsibilities in their environmental context. IRMs in the 10.8 series provide explicit requirements where security roles and responsibilities are delineated.

- a. Due to each document having its own update lifecycle, there may be instances where updated roles and responsibilities are published in supplementary policies which have not yet been added to this IRM. In those instances, the newer published roles and responsibilities must be implicitly followed along with those stated in this IRM.

10.8.2.1.4
(04-29-2025)
**Program Management
and Review**

- (1) The IRS security policy program establishes a framework of controls to ensure the inclusion of security into the IRS IT environment. This framework is provided through the issuance of security policies via the IRM 10.8 series and the development of security requirements checklists. Stakeholders are notified when revisions to the security policies and security requirements checklists are made.
- (2) It is the policy of the IRS to:
 - a. Establish and manage an information security program within its organizations. This IRM provides uniform policies and guidance to be used by each organization.
 - b. Protect all IT resources belonging to, or used by, the IRS at a level commensurate with the risk and magnitude of harm that could result from loss, misuse, or unauthorized access to that IT resource.
 - c. Protect its information resources and allow the use, access, disposition, and disclosure of information in accordance with applicable laws, policies, federal regulations, OMB guidance, Treasury Directives (TDs), NIST Publications, National Archives and Records Administration (NARA) guidance, other regulatory guidance, and best practice methodologies.
 - d. Use best practice methodologies (e.g., Capability Maturity Model Integration (CMMI), Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve IRS IT process and service efficiency and effectiveness.

10.8.2.1.5
(11-07-2023)
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, Cybersecurity and Infrastructure Security Agency (CISA), NIST, 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 revision process.
- (3) For information systems that store, process, or transmit classified information, refer to IRM 10.9.1 , *Classified National Security Information (CNSI)*, for guidance on protecting classified information.

- (4) In the event there is a discrepancy between this IRM and IRM 10.8.1, **Information Technology (IT) Security, Security Policy**, IRM 10.8.1 has precedence, unless the security controls/requirements in this IRM are more restrictive.
- 10.8.2.1.6
(11-07-2023)
Terms and Acronyms
- (1) Refer to Exhibit 10.8.2-2, Terms and Acronyms for a list of terms, acronyms, and definitions.
- 10.8.2.1.7
(04-29-2025)
Related Resources
- (1) In addition to federal guidance cited throughout this IRM, this IRM incorporates IRS-defined policy, regulatory and mandated guidance, and policy from other sources. Refer to Exhibit 10.8.2-3, Related Resources for a list of related resources and references.
- 10.8.2.2
(04-29-2025)
Risk Acceptance and Risk-Based Decisions (RBD)
- (1) Any exception to this IRM requires that the authorizing official (AO) make a risk acceptance decision.
- (2) Users must submit risk-based decision (RBD) requests in accordance with Cybersecurity's Security Risk Management (SRM) risk acceptance process documented in the Request for Risk Acceptance and Risk Based Decision (RBD) standard operating procedures (SOP).
- (3) Refer to IRM 10.8.1 for additional guidance on risk acceptance and RBDs.
- 10.8.2.3
(04-29-2025)
IT Security Roles and Responsibilities
- (1) This IRM establishes the IT security roles and responsibilities for the IRS.
- a. In accordance with IRM 10.8.1, the IRS must implement security roles and responsibilities in accordance with federal laws and IT security guidelines that are appropriate for specific operations and functions.
- (2) The following roles and responsibilities are based on FISMA, NIST, and Department of the Treasury guidance and policies.
- (3) Throughout this IRM, roles may be identified as being responsible for creating, updating, and maintaining documentation. This may be accomplished through agreements and coordination with other organizational entities. When this is done, it does not relieve the individual with the role of the responsibility, but rather requires effective communication between the two parties.
- (4) The IRS must ensure there are no conflicts of interest when assigning the same individual to multiple risk management roles. [NIST: SP 800-37 | NIST: SP 800-100]
- Example:** Authorizing officials cannot occupy the role of system owner or common control provider for systems or common controls they are authorizing. In addition, combining multiple roles for security and privacy requires care because the two disciplines may require different expertise, and in some circumstances, the priorities may be competing.
- Note:** If a conflict of interest is unavoidable, only the agency head can formally waive the conflict of interest.

10.8.2.3.1
(04-29-2025)

**Key Governance and
Related Roles &
Responsibilities**

- (1) There are several governance stakeholders common to most organizations that span the organization. These stakeholders include senior management/executive official, a chief information officer (CIO), information security personnel, and a chief financial officer (CFO), among others. The specific requirements of each role may differ with the degree of information security governance centralization or in response to the specific missions and needs of an organization. [NIST: SP 800-100]
- (2) The following subsections provide functional roles and responsibilities for personnel who have security-related governance responsibility for the protection of information systems they operate, manage and support. These roles are defined in accordance with FISMA, NIST, OMB, Treasury and IRS Policy and Guidelines.

10.8.2.3.1.1
(04-29-2025)

Agency Head

- (1) The agency head is a senior official in the agency responsible and accountable for providing information security protections commensurate with the risk to organizational operations and assets, individuals, other organizations, and the Nation—that is, risk resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; and the information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. [NIST: SP 800-37]

Note: For the IRS, the agency head is the IRS commissioner, acting commissioner, or senior IRS executive acting on behalf of the IRS.

- (2) The agency head ensures that: [NIST SP 800-37]
 - a. Information security and privacy management processes are integrated with strategic and operational planning processes;
 - b. Senior management/executive officials provide information security, for the information and information systems supporting the operations and assets under their control;
 - c. Senior agency officials for privacy are designated who are responsible and accountable for ensuring compliance with applicable privacy requirements, managing privacy risk, and the organization's privacy program;
 - d. The agency has adequately trained personnel to assist in complying with security and privacy requirements in legislation, EOs, policies, directives, instructions, standards, and guidelines; and
 - e. Privacy interests are protected and that personally identifiable information (PII) is managed responsibly within the agency.
- (3) The head of agency establishes: [NIST: SP 800-37]
 - a. The agency commitment and the actions required to effectively manage security and privacy risk and protect the missions and business functions being carried out by the organization.
 - b. Security and privacy accountability and provides active support and oversight of monitoring and improvement for the security and privacy programs.
- (4) The agency head is responsible for the following risk management framework (RMF) tasks: [NIST: SP 800-37]

- a. Identify and assign individuals to specific roles associated with security and privacy risk management; and
- b. Establish a risk management strategy for the organization that includes a determination of risk tolerance.

[illegible]

- (6) The agency head is responsible for: [Federal: P.L. 113-283 Sec. 3554]
 - a. Providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of:
 - i. Information collected or maintained by or on behalf of the agency.
 - ii. Information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.
 - b. Complying with the requirements of FISMA Section 3544 and related policies, procedures, standards, and guidelines, including:
 - i. Information security standards promulgated under the U.S. Code Section 11331 of Title 40.
 - ii. Information security standards and guidelines for national security systems issued in accordance with law and as directed by the President.
 - c. Designating the CIO, who reports directly to the agency head;
 - d. Implementing policies and procedures to cost-effectively reduce risks to an acceptable level;

- 10.8.2.3.1.2
(04-29-2025)
**Chief Information Officer
(CIO)**

#####

- (3) The CIO must have Top Secret Sensitive Compartmented Information (TS-SCI) access. [OMB: M-20-04]
- (4) The CIO has the following responsibilities: [Federal: Taxpayer First Act, Section 2101]
 - a. Be responsible for the development, implementation, and maintenance of IT for the IRS;
 - b. Ensure the IT of the IRS is secure and integrated;
 - c. Maintain operational control of all IT for the IRS;
 - d. Be the principal advocate for the IT needs of the IRS;
 - e. Consult with the chief procurement officer (CPO) to ensure the acquisition of IT for the IRS is consistent with IRS security policies and the strategic plan for the IRS IT needs; and
 - f. Develop and implement a multiyear strategic plan for the IT needs of the IRS, which:
 - (i) Includes performance measurements of such technology and of the implementation of such plan
 - (ii) Includes a plan for an integrated enterprise architecture of the IT of the IRS;
 - (iii) Includes and takes into account the resources needed to accomplish such plan;
 - (iv) Takes into account planned major acquisitions of IT by the IRS; and
 - (v) Aligns with the needs and strategic plan of the IRS.
- (5) The CIO has the following responsibilities: [NIST: SP 800-37]
 - a. Designate a SAISO/CISO, who carries out the CIO's responsibilities for system and program security planning and assessments;
 - b. Develop and maintain an agency-wide information security program including information security policies, procedures, and control techniques to address system security planning and all applicable requirements;
 - c. Determines, in conjunction with the AO, the appropriate allocation of resources dedicated to the protection of the organization's missions and business functions and the information systems supporting those missions/business functions based on organizational priorities;
 - d. For information systems that process PII, the CIO and AO coordinate any determination about the allocation of resources dedicated to the protection of those systems with the chief privacy officer;
 - e. Ensure that personnel with significant responsibilities for system and program security plans and assessments are trained;
 - f. Assists senior management/executive officials concerning their security responsibilities; and
 - g. Report annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.
- (6) The CIO, with the support of the senior accountable official for risk management, the risk executive (function), and the senior agency information security officer/chief information security officer, works closely with authorizing officials and their designated representatives to help ensure that: [NIST: SP 800-37]

- a. An IRS-wide security program is effectively implemented resulting in security for all IRS systems and environments of operation;
- b. Security and privacy (including supply chain) risk management considerations are integrated into programming/planning/budgeting cycles, enterprise architectures, the system development life cycle (SDLC), and acquisitions;
- c. IRS systems and common controls are covered by approved system security plans (SSP)s and possess current authorizations;
- d. Security activities required across the IRS are accomplished in an efficient, cost-effective, and timely manner; and
- e. There is centralized reporting of security activities.

(7) The CIO is responsible for the following RMF tasks: [NIST: SP 800-37]

Note: The CIO is identified as having “Primary Responsibility” for these RMF tasks. These tasks may be shared responsibilities with other RMF roles. For tasks in which the AO is identified as having a “Supporting Role”, see NIST SP 800-37.

- a. Identify and assign individuals to specific roles associated with security and privacy risk management.

(8) The CIO has the following responsibilities: [Treasury: IRP]

- a. Empower IRS CSIRC to investigate and respond to incidents;
- b. Ensure that Treasury Shared Services Security Operations Center (TSOC) gets immediate notifications of events/incidents from the incident response teams and/or IRS CISO;
- c. Ensure execution of the IRS internal response, including engagement of IRS privacy personnel with respect to breaches and appropriate escalation to senior IRS and Treasury officials; and
- d. Notify the Treasury CIO of events and incidents that may be considered for a major incident declaration or have impact to mission essential functions.

#

[illegible]

#

- (10) The CIO has the following software piracy responsibilities: [Treasury: TD 85-02]
- a. Develop and implement an enterprise-level plan that ensures that the agency is in compliance with EO 13103;
 - b. Coordinate with Department of Treasury bureaus and offices an initial assessment of the agency's existing policies and practices with respect to the use and management of computer software through qualified personnel or an outside contractor;
 - c. Maintain an electronic enterprise list of Treasury Department authorized and supported software. The list indicates by bureaus and offices, terms of licenses, authorized number of users, and physical location of software;
 - d. Perform spot audits. Periodic audit checks are done to ensure bureaus and offices are in compliance with software license agreements; and
 - e. Establish centralized software acquisition whenever possible.
- (11) The CIO is a member of any investment or related board of the IRS with purview over IT, or any board responsible for setting IRS-wide IT standards. [EO: 13833]
- (12) The CIO, as tasked by FISMA, administers training and oversee personnel with significant information security responsibilities. To accomplish this, the CIO works with the SAISO/CISO to: [Federal: P.L. 113-283]
- a. Establish overall strategy for the information security awareness and training program;
 - b. Ensure that the agency head, senior managers, system and information owners, and others understand the concepts and strategy of the information security awareness and training program, and are informed of the progress of the program's implementation;
 - c. Ensure that the agency's information security awareness and training program is funded;
 - d. Ensure that an effective information security awareness effort is developed and employed such that all personnel are routinely or continuously exposed to awareness messages through posters, email messages, logon banners, and other techniques; and
 - e. Ensure that effective tracking and reporting mechanisms are in place.
- (13) The CIO has the following information security continuous monitoring (ISCM) responsibilities: [NIST: SP 800-137]
- a. Lead the organization's ISCM program;

- b. Ensure that an effective ISCM program is established and implemented for the organization by establishing expectations and requirements for the organization's ISCM program;
- c. Work closely with authorizing officials to provide funding, personnel, and other resources to support ISCM; and
- d. Maintain high-level communications and working group relationships among organizational entities.

10.8.2.3.1.3
(04-29-2025)

Chief Data Officer (CDO)

- (1) The chief data officer (CDO) of an agency is designated on the basis of demonstrated training and experience in data management, governance (including creation, application, and maintenance of data standards), collection, analysis, protection, use, and dissemination, including with respect to any statistical and related techniques to protect and de-identify confidential data. [Federal: P.L. 115-435, Section 3520]
- (2) The CDO has the following responsibilities: [Federal: P.L. 115-435, Section 3520]
 - a. Be responsible for lifecycle data management;
 - b. Coordinate with any official in the agency responsible for using, protecting, disseminating, and generating data to ensure that the data needs of the agency are met;
 - c. Manage data assets of the agency, including the standardization of data format, sharing of data assets, and publication of data assets in accordance with applicable law;
 - d. In carrying out the requirements under paragraphs (2)c and (2)e, consult with any statistical official of the agency (as designated under section 314 of title 5);
 - e. Carry out the requirements of the agency under subsections (b) through (d), (f), and (i) of section 3506, section 3507, and section 3511 of title 44;
 - f. Ensure that, to the extent practicable, agency data conforms with data management best practices;
 - g. Engage agency employees, the public, and contractors in using public data assets and encourage collaborative approaches on improving data use;
 - h. Support the performance improvement officer of the agency in identifying and using data to carry out the functions described in section 1124(a)(2) of title 31;
 - i. Support the evaluation officer of the agency in obtaining data to carry out the functions described in section 313(d) of title 5;
 - j. Review the impact of the infrastructure of the agency on data asset accessibility and coordinate with the CIO of the agency to improve such infrastructure to reduce barriers that inhibit data asset accessibility;
 - k. Ensure that, to the extent practicable, the agency maximizes the use of data in the agency, including for the production of evidence (as defined in section 3561 of title 44), cybersecurity, and the improvement of agency operations;
 - l. Identify points of contact for roles and responsibilities related to open data use and implementation (as required by the Director);
 - m. Serve as the agency liaison to other agencies and the OMB on the best way to use existing agency data for statistical purposes (as defined in section 3561 of Foundations for Evidence-Based Policymaking Act of 2018); and

- n. Comply with any regulation and guidance issued under subchapter III, including the acquisition and maintenance of any required certification and training.
- (3) Delegation of Responsibilities: [Federal: P.L. 115-435, Section 3520]
- a. In general – To the extent necessary to comply with statistical laws, the CDO may delegate any responsibility to the head of a statistical agency or unit (as defined in section 3561 of title 44) within the agency.
 - b. Consultation – To the extent permissible under law, the individual to whom a responsibility has been delegated to must consult with the CDO of the agency in carrying out such responsibility.
 - c. Deference – The CDO must defer to the individual to whom a responsibility has been delegated to regarding the necessary delegation of such responsibility with respect to any data acquired, maintained, or disseminated by the agency under applicable statistical law.
- (4) The CDO submits to the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Oversight and Government Reform of the House of Representatives an annual report on the compliance of the agency with the requirements of subchapter I of title 44, including information on each requirement that the agency could not carry out and, if applicable, what the agency needs to carry out such requirement. [Federal: P.L. 115-435, Section 3520]

10.8.2.3.1.4
(04-29-2025)
**Senior Agency
Information Security
Officer (SAISO)/Chief
Information Security
Officer (CISO)**

- (1) The SAISO/CISO is an organizational official responsible for carrying out the CIO security responsibilities under FISMA and serves as the primary liaison for the CIO to the organization's AOs, system owners, common control providers, and system security officers (SSOs). [NIST: SP 800-37]
- Note:** At the IRS, the associate CIO (ACIO), IRS IT cybersecurity organization is the SAISO/CISO.
- (2) The SAISO/CISO collaborates with the chief privacy officer to ensure coordination between privacy and security activities. [OMB: A-130 Appendix I (3)(b)(11)]

#

#

#####

- #####

#

- (8) The SAISO/CISO, through delegation by the CIO, has the following responsibilities: [Federal: P.L. 113-283 Section 3554 | NIST: SP 800-100]
- a. Carry out the CIO's FISMA responsibilities delegated to them;
 - b. Possess the qualifications, training and experience required to administer information security program functions;
 - c. Maintain information security duties as their primary responsibility;
 - d. Head an office with the mission of assisting in achieving FISMA compliance;
 - e. Develop, document, and implement an agency wide information security program to provide security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source;
 - f. Periodically assess risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;
 - g. Develop and maintain risk-based, cost-effective information security policies, procedures, and control techniques to address all applicable requirements throughout the life cycle of each agency information system to ensure compliance with applicable requirements;
 - h. Facilitate development of subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
 - i. Periodically test and evaluate the effectiveness of information security policies, procedures, and practices;
 - j. Establish and maintain a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;
 - k. Develop and implement procedures for detecting, investigating, reporting, responding, and resolving security incidents;
 - l. Train and oversee IRS personnel, contractors, and others with significant responsibilities for information security with respect to such responsibilities;
 - m. Ensure preparation and maintenance of plans and procedures to provide continuity of operations for information systems that support the operations and assets of the agency; Ensure that contingency plans for IT systems are developed, maintained and tested;
 - n. Support the agency CIO in annual reporting to the agency head on the effectiveness of the agency information security program, including progress of remedial actions; and
 - o. Assist senior management/executive officials concerning their responsibilities.
- (9) The SAISO/CISO is responsible for the following RMF tasks: [NIST: SP 800-37]

Note: The SAISO/CISO is identified as having "Primary Responsibility" for these RMF tasks. These tasks may be shared responsibilities with other RMF roles. For tasks in which the SAISO/CISO is identified as having a "Supporting Role", see NIST SP 800-37.

- a. Assess organization-wide security and privacy risk and update the risk assessment results on an ongoing basis;
 - b. Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems;
 - c. Updated security and privacy plans; updated plans of action and milestones; updated security and privacy assessment reports; and
 - d. Report the security and privacy posture of the system to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy.
- (10) The SAISO/CISO has the following ISCM responsibilities: [NIST: SP 800-137 | Treasury: ISCM]
- a. Establish, implement, and maintain the organization's ISCM program;
 - b. Develop organizational program guidance (i.e., policies/procedures) for continuous monitoring of the security program and information systems;
 - c. Develop configuration management guidance for the organization;
 - d. Consolidate and analyzes POA&Ms to determine organizational security weaknesses and deficiencies;
 - e. Acquire or develop and maintain automated tools to support ISCM and ongoing authorizations;
 - f. Provide training on the organization's ISCM program and process;
 - g. Provide support to information owners/information system owners and common control providers on how to implement ISCM for their information systems; and
 - h. Develop and maintain any supplemental policy or guidance to the Treasury ISCM framework.

10.8.2.3.1.4.1
(04-29-2025)
Security Control
Assessor

#

#

(4) The control assessor has the following responsibilities: [NIST: SP 800-37]

- a. Conduct a comprehensive assessment of controls and control enhancements implemented within or inherited by a system to determine the effectiveness of the controls (i.e., the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization);

Note: For system-level control assessments, control assessors do not assess inherited controls, and only assess the system-implemented portions of hybrid controls.

- b. Assess the implemented controls using the assessment procedures specified in the security and privacy assessment plans.
- c. Prepare security and privacy assessment reports containing the results and findings from the assessment;
- d. Provide an assessment of the severity of the deficiencies discovered in the system, environment of operation, and common controls;
- e. Provide recommended corrective actions to address identified vulnerabilities;
- f. Prepare a security and privacy assessment report containing the results and findings from the assessment.

(5) The control assessor is responsible for the following RMF tasks: [NIST: SP 800-37]

Note: The security control assessor is identified as having “Primary Responsibility” for these RMF tasks. These tasks may be shared responsibilities with other RMF roles. For tasks in which the AO is identified as having a “Supporting Role”, see NIST SP 800-37.

- a. Develop, review, and approve plans to assess implemented controls;
- b. Assess the controls in accordance with the assessment procedures described in assessment plans;
- c. Prepare the assessment reports documenting the findings and recommendations from the control assessments;
- d. Conduct initial remediation actions on the controls and reassess remediated controls; and
- e. Update security and privacy assessment reports.

(6) The security control assessor performs the following ISCM responsibilities: [NIST: SP 800-137]

- a. Provide input into the types of security-related information gathered;

- 10.8.2.3.1.4.2
(04-29-2025)
**Risk Executive
(Function)**

##

- (1) The common control provider is an IRS official or group responsible for the development, implementation, assessment, and monitoring of common controls (i.e., security controls inherited by information systems). [NIST: SP 800-37]

Note: Organizations can have multiple common control providers depending on how information security responsibilities are allocated organization-wide. Common control providers may also be information system owners when the common controls are resident within an information system.

- (2) The common control provider has the following responsibilities: [NIST: SP 800-37]
 - a. Ensure the documentation of common controls to be utilized in a system's security documentation (e.g., (SSP));
 - b. Ensure that required assessments of common controls are carried out by qualified assessors with an appropriate level of independence;
 - c. Document assessment findings in a security assessment report;
 - d. Produce a POA&M for all controls having weaknesses or deficiencies; and
 - e. Make security plans, security assessment reports, and POA&Ms for common controls (or a summary of such information) available to information system owners inheriting those controls after the information is

reviewed and approved by the senior management/executive official or executive with oversight responsibility for those controls.

- (3) The common control provider is responsible for the following RMF tasks: [NIST: SP 800-37]

Note: The common control provider is identified as having “Primary Responsibility” for these RMF tasks. These tasks may be shared responsibilities with other RMF roles. For tasks in which the common control provider is identified as having a “Supporting Role”, see NIST SP 800-37.

- a. Select the controls for the system and the environment of operation;
 - b. Tailor the controls selected for the system and the environment of operation;
 - c. Document the controls for the system and environment of operation in security and privacy plans;
 - d. Develop and implement a system-level strategy for monitoring control effectiveness that is consistent with and supplements the organizational continuous monitoring strategy;
 - e. Implement the controls in the security and privacy plans;
 - f. Document changes to planned control implementations based on the “as-implemented” state of controls;
 - g. Conduct initial remediation actions on the controls and reassess remediated controls;
 - h. Prepare the POA&Ms based on the findings and recommendations of the assessment reports;
 - i. Assemble the authorization package and submit the package to the authorizing official for an authorization decision;
 - j. Analyze and determine the risk from the operation or use of the system or the provision of common controls;
 - k. Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system;
 - l. Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones;
 - m. Update plans, assessment reports, and plans of action and milestones based on the results of the continuous monitoring process; and
 - n. Report the security and privacy posture of the system to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy.
- (4) The common control provider has the following ISCM responsibilities: [NIST: SP 800-137]
- a. Establish processes and procedures in support of ongoing monitoring of common controls;
 - b. Develop and document an ISCM strategy for assigned common controls;
 - c. Participate in the organization’s configuration management process;
 - d. Establish and maintain an inventory of components associated with the common controls;
 - e. Conduct security impact analyses on changes that affect the common controls;
 - f. Ensure security controls are assessed according to the ISCM strategy;
 - g. Prepare and submit security status reports in accordance with organizational policy/procedures;

- h. Conduct remediation activities as necessary to maintain common control authorization;
- i. Update/revise the common security control monitoring process as required;
- j. Update critical security documents as changes occur; and
- k. Distribute critical security documents to individual information owners/ system owners, and other senior leaders in accordance with organizational policy/procedures.

10.8.2.3.1.5
(04-29-2025)

**Senior Management/
Executives**

- (1) Executive agencies within the federal government shall: [OMB: A-130]
 - a. Plan for security in all phases of the system life cycle;
 - b. Ensure appropriate officials are assigned security responsibility;
 - c. Review security controls annually (i.e., FISMA annual security program review); and
 - d. Formally authorize (accredit) processing prior to operations (as an AO) and periodically thereafter.
 - e. Balance mission and business priorities versus any security risks that might be applicable.
- (2) FISMA, OMB, Department of Treasury, and FISMA guidance specify that senior management/executive officials are subordinate to the Commissioner and are responsible for:
 - a. Exercising oversight to ensure that a program manager is assigned for each system;
 - b. Exercising oversight over cybersecurity awareness training funding; and
 - c. Annually validating and updating the master inventory of information systems.

10.8.2.3.1.6
(04-29-2025)

System Owner

- (1) The system owner is the agency official responsible for the overall procurement, development, integration, modification, operation, maintenance, and disposal of a system. The system owner may rely on the assistance and advice of the SSO, system operators, and other IT staff in the implementation of security responsibilities. [NIST: SP 800-37 | Treasury: TD P 85-01]
- (2) The system owner serves both as an owner and as the central point of contact between the authorization process and the owners of components of the system including, for example: (i) applications, networking, servers, or workstations; (ii) owners/stewards of information processed, stored, or transmitted by the system; and (iii) owners of the missions and business functions supported by the system. [NIST: SP 800-39]
- (3) The system owner must be identified in the security plan for each system. [NIST: SP 800-18]

#

[illegible]

- (6) The system owner has the following responsibilities: [NIST: SP 800-37]
- a. Address the operational interests of the user community (i.e., users who require access to the information system to satisfy mission, business, or operational requirements);
 - b. Ensure compliance with the information security requirements;
 - c. Develop and maintain, in coordination with the SSO and privacy officer, the security and privacy plans and ensures that the system is deployed and operated in accordance with the selected and implemented controls;
 - d. Decide, in coordination with the information owner/steward, who has access to the system (and with what types of privileges or access rights);
 - e. Ensure that system users and support personnel receive the requisite security and privacy training;
 - f. Inform organizational officials of the need to conduct the authorization, ensure that resources are available for the effort, and provide the required system access, information, and documentation to control assessors;
 - g. Receive the security and privacy assessment results from the control assessors;
 - h. Ensure appropriate steps to reduce or eliminate vulnerabilities or security and privacy risks are taken; and
 - i. Assemble the authorization package and submit the package to the authorizing official or the authorizing official designated representative for adjudication.
- (7) The system owner is responsible for the following RMF tasks: [NIST: SP 800-37]

Note: The system owner is identified as having “Primary Responsibility” for these RMF tasks. These tasks may be shared responsibilities with other RMF roles. For tasks in which the system owner is identified as having a “Supporting Role”, see NIST SP 800-37.

- a. Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system;
- b. Identify assets that require protection;
- c. Identify the types of information to be processed, stored, and transmitted by the system;
- d. Identify and understand all stages of the information life cycle for each information type processed, stored, or transmitted by the system;
- e. Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis;
- f. Define the security and privacy requirements for the system and the environment of operation;
- g. Register the system with organizational program or management offices;
- h. Document the characteristics of the system;
- i. Categorize the system and document the security categorization results;
- j. Select the controls for the system and the environment of operation;
- k. Tailor the controls selected for the system and the environment of operation;

- l. Document the controls for the system and environment of operation in security and privacy plans;
 - m. Develop and implement a system-level strategy for monitoring control effectiveness that is consistent with and supplements the organizational continuous monitoring strategy;
 - n. Implement the controls in the security and privacy plans;
 - o. Document changes to planned control implementations based on the “as-implemented” state of controls;
 - p. Conduct initial remediation actions on the controls and reassess remediated controls;
 - q. Prepare the POA&M based on the findings and recommendations of the assessment reports;
 - r. Assemble the authorization package and submit the package to the authorizing official for an authorization decision;
 - s. Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system;
 - t. Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones;
 - u. Update plans, assessment reports, and plans of action and milestones based on the results of the continuous monitoring process;
 - v. Report the security and privacy posture of the system to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy; and
 - w. Implement a system disposal strategy and execute required actions when a system is removed from operation.
- (8) The system owner has the following contingency plan responsibilities: [NIST: SP 800-34]
- a. Ensure they’re identified in a system’s contingency plans as the system owner;
 - b. Conduct tabletop exercises;
 - c. Facilitate functional exercises; and
 - d. Carry out responsibilities as defined within a system’s contingency plans.
- (9) The system owner has the following ISCM responsibilities: [NIST: SP 800-137]
- a. Establish processes and procedures in support of system-level implementation of the organization’s ISCM program. This includes developing and documenting an ISCM strategy for the information system;
 - b. Participate in the organization’s configuration management process;
 - c. Establish and maintain an inventory of components associated with the information system;
 - d. Conduct security impact analyses on changes to the information system;
 - e. Conduct, or ensuring conduct of, assessment of security controls according to the ISCM strategy;
 - f. Prepare and submit security status reports in accordance with organizational policy and procedures;
 - g. Conduct remediation activities as necessary to maintain system authorization;
 - h. Revise the system-level security control monitoring process as required;
 - i. Review ISCM reports from common control providers to verify that the common controls continue to provide adequate protection for the information system; and
 - j. Update critical security documents based on the results of ISCM.

- (10) The system owner must: [NIST: SP 800-18]
 - a. Be identified in the SSP for each system;
 - b. Be assigned in writing; and
 - c. Have their contact information contained in the SSP.

10.8.2.3.1.6.1
(07-12-2010)
**Business System
Planner (BSP)**

- (1) The business system planner (BSP) performs duties outlined for senior management/executives.

10.8.2.3.1.6.1.1
(05-16-2014)
**Security Program
Management Officer
(SPMO)**

- (1) The security program management officers (SPMOs) have been established within the business units and IRS IT Cybersecurity organization to support their AO and other staff with the successful completion of that office's security related responsibilities, including the successful completion of all FISMA requirements.
- (2) The SPMO supports the BSP functions, system owners, FISMA activities and shall provide other security-related support for other security activities.
- (3) The SPMO provides SSOs for the systems owned by their respective business unit.
 - a. When there is no SSO assigned for a system, the SPMO shall assume the role of the SSO.
- (4) The SPMO, in support of FISMA, has the following responsibilities:
 - a. Ensure development and implementation of the IRS security program strategy to meet FISMA requirements;
 - b. Ensure currency of the FISMA Master Inventory;
 - c. Coordinate and ensure completion of annual security reviews;
 - d. Make security determinations (such as prioritization) for weakness reporting;
 - e. Ensure timely completion of POA&M weaknesses and obtain AO or AO point of contact (POC) concurrence;

Note: POA&Ms are approved by the AO (e.g., as a part of the accreditation process or prior to establishing in TFIMS), and are managed, and completed as planned.

 - f. Collaborate with other SPMOs to ensure consistency of FISMA activities across business units;
 - g. Serve as the security point of contact for business unit staff supporting FISMA and as the cybersecurity interface into the business unit;
 - h. Identify needs and implement IT security awareness training to current and newly assigned personnel in the business unit; and
 - i. Present all training and orientation materials to AOs and various POCs, at minimum, annually.
- (5) The SPMO, for weaknesses and POA&Ms, has the following responsibilities:
 - a. Identify and track, with SSO support, the corrective actions to mitigate the weaknesses in the POA&M through status updates, changes to milestones, and additional comments;
 - b. Identify the scheduled completion date, cost, and resources needed to mitigate each weakness;

- c. Validate the effectiveness of the corrective actions during continuous monitoring or security control assessment (SCA);
- d. Combine and review all high level security weaknesses from the self-assessment, risk assessment, Treasury Inspector General for Tax Administration (TIGTA) audits, GAO audits, and internal reviews into POA&M weaknesses;
- e. As determined by their business unit, consolidate self-assessment scores for their business unit applications then brief POCs and AOs on results; and
- f. Support the development of answers to the self-assessment questions that cross multiple business units.

10.8.2.3.1.7
(04-29-2025)

**Mission or Business
Owner**

- (1) The mission or business owner has the following responsibilities: [NIST: SP 800-37]
 - a. Be the senior official or executive within an organization with specific mission or line of business responsibilities and that has a security or privacy interest in the organizational systems supporting those missions or lines of business;
 - b. Be a key stakeholder that has a significant role in establishing organizational mission and business processes and the protection needs and security and privacy requirements that ensure the successful conduct of the organization's missions and business operations;
 - c. Provide essential inputs to the risk management strategy;
 - d. Play an active part in a system's life cycle development; and
 - e. May also serve in the role of authorizing official.
- (2) The mission or business owner is responsible for the following RMF tasks: [NIST: SP 800-37]

Note: The mission or business owner is identified as having "Primary Responsibility" for these RMF tasks. These tasks may be shared responsibilities with other RMF roles. For tasks in which the mission or business owner is identified as having a "Supporting Role", see NIST SP 800-37.

- a. Establish, document, and publish organizationally-tailored control baselines and/or cybersecurity framework profiles;
 - b. Identify the missions, business functions, and mission/business processes that the system is intended to support;
 - c. Identify stakeholders who have an interest in the design, development, implementation, assessment, operation, maintenance, or disposal of the system;
 - d. Define the security and privacy requirements for the system and the environment of operation; and
 - e. Determine the placement of the system within the enterprise architecture.
- (3) If the mission or business owner has been approved to perform the functions of acquisition, management, and operation and maintenance of an information system, then they perform the system owner responsibilities defined within this IRM.

Note: To avoid a conflict of interest, the mission or business owner may not serve as the AO for a system in which they're performing the responsibilities of the system owner.

- (1) The information owner is an IRS official with statutory, management, or operational authority for specified information and responsibility for establishing the policies and procedures governing its generation, collection, processing, dissemination, and disposal. [NIST: SP 800-37]

Note: At the IRS, the information owner is the business and functional unit owner.

[illegible]

- (4) The information owner provides input to system owners regarding the security and privacy requirements and controls for the systems where the information is processed, stored, or transmitted. [NIST: SP 800-37]
- (5) The information owner, in collaboration with the AO, must approve (in writing) the following prior to them happening: [NIST: SP 800-37]
 - a. The physical removal of sensitive but unclassified (SBU) information from IRS facilities.
 - b. The download and remote storage of SBU information outside of IRS facilities.

Note: These fall within the area of the information owner's responsibility to protect information under their purview.

- (6) The information owner is responsible for the following RMF tasks: [NIST: SP 800-37]

Note: The information owner is identified as having “Primary Responsibility” for these RMF tasks. These tasks may be shared responsibilities with other

- a. Identify the types of information to be processed, stored, and transmitted by the system;
- b. Identify and understand all stages of the information life cycle for each information type processed, stored, or transmitted by the system;
- c. Define the security and privacy requirements for the system and the environment of operation; and
- d. Categorize the system and document the security categorization results.

(7) Refer to the Mission or Business Owner subsection within this IRM for mission or business owner responsibilities.

#####

(4) The AO has the following responsibilities: [NIST: SP 800-37]

- a. Be the only organizational official who can accept the security and privacy risk to organizational operations, organizational assets, and individuals;
- b. Typically have budgetary oversight for the system or are responsible for the mission and/or business operations supported by the system;
- c. Be in a management position with a level of authority commensurate with understanding and accepting such security and privacy risks;
- d. Approve plans (e.g., system security, privacy, assessment), memorandums of agreement or understanding, and plans of action and milestones;
- e. Determine whether significant changes in the information systems or environments of operation require reauthorization;
- f. Coordinate their activities with common control providers, system owners, chief information officers, senior agency information security officers, senior agency officials for privacy, system security and privacy officers, control assessors, senior accountable officials for risk management/risk executive (function), and other interested parties during the authorization process;
- g. May delegate the coordinating and conducting of the day-to-day activities associated with managing risk to information systems and the organization to the authorizing official designated representative (AODR), which includes carrying out many of the activities related to the execution of the RMF.

Note: Day-to-day activities do not include signing security authorization decision letters. The designated representative is to confer with the AO on decisions where the acceptance of risk to the organization is involved. The AO will then be required to officially accept the risk by signing the associated security authorization decision letter (i.e., the acceptability of risk to the agency).

Note: The only activity that cannot be delegated by the AO is the security accreditation decision and the signing of the associated security authorization decision letter (i.e., the acceptability of risk to the agency).

- h. Be responsible and accountable for ensuring that authorization activities and functions that are delegated to authorizing official designated representatives are carried out as specified;

(5) The AO is responsible for the following RMF tasks the following: [NIST: SP 800-37]

Note: The AO is identified as having “Primary Responsibility” for these RMF tasks. These tasks may be shared responsibilities with other RMF roles. For tasks in which the AO is identified as having a “Supporting Role”, see NIST SP 800-37.

- a. Determine the authorization boundary of the system;

- b. Review and approve the security categorization results and decision;
- c. Review and approve the security and privacy plans for the system and the environment of operation;
- d. Select the appropriate assessor or assessment team for the type of control assessment to be conducted;
- e. Develop, review, and approve plans to assess implemented controls;
- f. Analyze and determine the risk from the operation or use of the system or the provision of common controls;
- g. Identify and implement a preferred course of action in response to the risk determined;
- h. Determine if the risk from the operation or use of the information system or the provision or use of common controls is acceptable;

Note: The explicit acceptance of risk is the responsibility of the AO and cannot be delegated to other officials within the organization.

- i. Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk;
- j. Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in POA&Ms; and
- k. Review the security and privacy posture of the system on an ongoing basis to determine whether the risk remains acceptable.

(6) The AO has the following ISCM responsibilities: [NIST: SP 800-137]

- a. Assume responsibility for ensuring the organization's ISCM program is applied with respect to a given information system under their purview;
- b. Ensure the security posture of the information system is maintained;
- c. Review security status reports and critical security documents and determines if the risk to the organization from operation of the information system remains acceptable;
- d. In consultation with the SSO, determine whether significant information system changes require system reauthorization;

(7) The AO must: [NIST: SP 800-18]

- a. Be identified in the SSP for each system;
- b. Be assigned in writing; and
- c. Have their contact information contained in the system security plan.

10.8.2.3.1.9.1
(04-29-2025)

**Authorizing Official
Designated
Representative (AODR)**

(1) The AODR is an organizational official designated by the AO who is empowered to act on behalf of the AO to coordinate and conduct the required day-to-day activities associated with managing risk to information systems and the organization. This includes carrying out many of the activities related to the execution of the RMF. [NIST: SP 800-37]

(2) The AODR can be empowered by the AO (i.e., delegated) to make certain decisions with regard to the planning and resourcing security authorization process, such as: [NIST: SP 800-39]

- a. Approval of the security plan and security assessment plan; and
- b. Approve and monitor the implementation of POA&Ms, and the assessment/determination of risk.

(3) The AODR has the following responsibilities: [NIST: SP 800-39]

- a. Prepare the final authorization package;

- b. Obtain the AO's signature on the authorizing decision document (i.e., authorization letter); and
 - c. Transmit the authorization package to appropriate organizational officials.
- (4) The only activity that cannot be delegated to the AODR by the AO is the authorization decision and signing of the associated authorization decision document (i.e., the acceptance of risk to organizational operations and assets, individuals, other, organizations, and the Nation); to include authorization letters and risk based decision memos. [NIST: SP 800-37]
- (5) The AODR is responsible for the following RMF tasks: [NIST: SP 800-37]

Note: The AODR is identified as having "Primary Responsibility" for these RMF tasks. These tasks may be shared responsibilities with other RMF roles. For tasks in which the AODR is identified as having a "Supporting Role", see NIST SP 800-37.

- a. Review and approve the security categorization results and decision;
- b. Review and approve the security and privacy plans for the system and the environment of operation;
- c. Select the appropriate assessor or assessment team for the type of control assessment to be conducted;
- d. Develop, review, and approve plans to assess implemented controls;
- e. Analyze and determine the risk from the operation or use of the system or the provision of common controls;
- f. Identify and implement a preferred course of action in response to the risk determined; and
- g. Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk.

10.8.2.3.1.10
(04-29-2025)

**Chief Acquisition Officer
(CAO)**

- (1) The chief acquisition officer (CAO) is an organizational official designated by the head of agency. [NIST: SP 800-37]
- (2) The CAO advises and assists the head of agency and other agency officials to ensure that the mission of the agency is achieved through the management of the agency's acquisition activities. [NIST: SP 800-37]
- (3) The CAO has the following responsibilities: [NIST: SP 800-37]
- a. Monitor the performance of acquisition activities and programs;
 - b. Establish clear lines of authority, accountability, and responsibility for acquisition decision making within the agency;
 - c. Manage the direction and implementation of acquisition policy for the agency;
 - d. Establish policies, procedures, and practices that promote full and open competition from responsible sources to fulfill best value requirements considering the nature of the property or service procured; and
 - e. Coordinate with mission or business owners, AOs, senior accountable official for risk management, system owners, common control providers, SAISO/CISO, SAOP, and risk executive (function) to ensure that security and privacy requirements are defined in organizational procurements and acquisitions.
- (4) The CAO is identified as having a support role for several RMF tasks. Refer to NIST SP 800-37 Rev2 for these RMF tasks. [NIST: SP 800-37]

10.8.2.3.1.11
(04-29-2025)
**System Security Officer
(SSO)**

[illegible]

- (5) The SSO is a voting member on the CCB for the systems and applications for which they are assigned. [NIST: SP 800-53]

Note: SPMO is currently the voting member on the CCB.

- (6) The SSO supports the SPMO in FISMA activities. [IRS: IRS-defined]
- (7) The SSO supports the ISCM program by assisting the system owner in completing ISCM responsibilities and by participating in the configuration management process. [NIST: SP 800-137]
- (8) The SSO, in support of the Treasury ISCM framework, has the following responsibilities: [Treasury: ISCM]
- Establish and maintain processes and procedures in support of system-level implementation of the Treasury ISCM Framework;
 - Oversee and coordinate day-to-day operational ISCM activities associated with ensuring system security as described in NIST SP 800-137, **Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations**, and Section 5 - ISCM Operational Security of the Treasury ISCM Framework;
 - Review security control implementations and assessment priority ratings from common control providers to verify that the common controls continue to provide adequate protection for the information system; and
 - Update critical security documents based on the results of ISCM.
- (9) The SSO is the agency official assigned responsibility by the SAISO/CISO, AO, or system owner for ensuring that the appropriate operational security posture is maintained for an information system or program. [NIST: SP 800-18]
- (10) The SSO has the following responsibilities: [NIST: SP 800-37]
- Be an individual responsible for ensuring that the security posture is maintained for an organizational system and works in close collaboration with the system owner;
 - Have the knowledge and expertise to manage the security aspects of an organizational system and, in many organizations, is assigned responsibility for the day-to-day system security operations;
- Note:** This responsibility includes, but is not limited to, physical and environmental protection; personnel security; incident handling; and security training and awareness.
- Assist in the development of the system-level security policies and procedures and ensure compliance with those policies and procedures;
 - In close coordination with the system owner, play an active role in the monitoring of a system and its environment of operation to include developing and updating security plans, managing and controlling changes to the system, and assessing the security impact of those changes; and
 - Be responsible for aspects of the system that protect information and information systems from unauthorized system activity or behavior to provide confidentiality, integrity, and availability.

Note: SSO and system privacy officer responsibilities overlap regarding aspects of the system that protect the security of PII.

- (11) The SSO is responsible for the following RMF tasks: [NIST: SP 800-37]

Note: The SSO is identified as having “Primary Responsibility” for these RMF tasks. These tasks may be shared responsibilities with other RMF roles.

- a. Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis;
 - b. Allocate security and privacy requirements to the system and to the environment of operation; and
 - c. Allocate security and privacy controls to the system and to the environment of operation.
- (12) The SSO functions in a “Support Role” for the following RMF tasks: [NIST: SP 800-37]
- a. Identify the types of information to be processed, stored, and transmitted by the system;
 - b. Define the security and privacy requirements for the system and the environment of operation;
 - c. Register the system with organizational program or management offices;
 - d. Document the characteristics of the system;
 - e. Categorize the system and document the security categorization results;
 - f. Select the controls for the system and the environment of operation;
 - g. Tailor the controls selected for the system and the environment of operation;
 - h. Document the controls for the system and environment of operation in security and privacy plans;
 - i. Develop and implement a system-level strategy for monitoring control effectiveness that is consistent with and supplements the organizational continuous monitoring strategy;
 - j. Implement the controls in the security and privacy plans;
 - k. Document changes to planned control implementations based on the “as-implemented” state of controls;
 - l. Develop, review, and approve plans to assess implemented controls;
 - m. Assess the controls in accordance with the assessment procedures described in assessment plans;
 - n. Prepare the assessment reports documenting the findings and recommendations from the control assessments;
 - o. Conduct initial remediation actions on the controls and reassess remediated controls;
 - p. Prepare the plan of action and milestones based on the findings and recommendations of the assessment reports;
 - q. Assemble the authorization package and submit the package to the authorizing official for an authorization decision;
 - r. Identify and implement a preferred course of action in response to the risk determined;
 - s. Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk;
 - t. Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system;
 - u. Assess the controls implemented within and inherited by the system in accordance with the continuous monitoring strategy;
 - v. Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones;
 - w. Update plans, assessment reports, and plans of action and milestones based on the results of the continuous monitoring process;

- 10.8.2.3.1.12
(04-29-2025)
Manager

#

- Cat. No. 49072Q (04-29-2025)
Any line marked with a #
is for **Official Use Only**

- (4) Managers have the following responsibilities: [IRS: IRS-defined]
- a. Ensure employees are informed of appropriate uses of government IT resources as a part of their introductory training, orientation, or the initial implementation of this IRM. These requirements are part of the employees' mandatory annual cybersecurity awareness training; and
 - b. Ensure IT resources are being used appropriately and take corrective action, as needed.

Note: Refer to IRM 10.8.27, *Information Technology (IT) Security, Personal Use Of Government Furnished Information Technology and Resources*, for additional guidance.

10.8.2.3.1.13
(04-29-2025)

Contracting Officer

#

- (2) The contracting officer is responsible for managing contracts/acquisitions and overseeing their implementation, in accordance with IRM 1.1.32, *Organization and Office of the Chief Procurement Officer*.
- (3) The contract offices and procurement offices have the following responsibilities: [IRS: IRS-defined]
- a. Work in partnership with the SAISO/CISO to ensure that agency contracting policies adequately address the security and privacy requirements;
 - b. Coordinate with the SAISO/CISO to ensure that all agency contracts and procurements are compliant with the agency's security and privacy policies;
 - c. Ensure that all personnel with responsibilities in the agency's procurement process are properly trained in security and privacy policies; and
 - d. Collaborate with the SAISO/CISO to monitor contract performance for compliance with the agency's security and privacy policies.

Note: Refer to IRM 1.1.32 for additional guidance.

- (4) The procurement (or acquisitions) office has the following responsibilities: [NIST: SP 800-12]
- a. Ensure that organizational procurements have been reviewed by appropriate approving officials; and
 - b. Be knowledgeable of security and privacy standards and bring potential security and privacy issues to the attention of those requesting such technology.

10.8.2.3.1.13.1
(04-29-2025)

Contracting Officer's Representative (COR)

- (1) The contracting officer's representative (COR): [Federal: FAR Subpart 1.6]
- a. Must be a federal employee;
 - b. Must be a qualified employee appointed by the contracting officer; and
 - c. Act as its technical representative in managing the technical aspects of a particular contract.

#

10.8.2.3.1.14
(04-29-2025)
Enterprise Architect

- (1) The enterprise architect is an individual or group responsible for working with the leadership and subject matter experts in an organization to build a holistic view of the organization's missions and business functions, mission/business processes, information, and IT assets. [NIST: SP 800-137]
- (2) With respect to information security and privacy, the enterprise architect has the following responsibilities: [NIST: SP 800-137]
 - a. Coordinate with security and privacy architects to determine the optimal placement of systems/system elements within the enterprise architecture and to address security and privacy issues between systems and the enterprise architecture;
 - b. Assist with determining appropriate control implementations and initial configuration baselines as they relate to the enterprise architecture;
 - c. Assist in reducing complexity within the IT infrastructure to facilitate security;
 - d. Collaborate with system owners and authorizing officials to facilitate authorization boundary determinations and allocation of controls to system elements;
 - e. Serve as part of the Risk Executive (function); and
 - f. Assist with integration of the organizational risk management strategy and system-level security and privacy requirements into program, planning, and budgeting activities, the SDLC, acquisition processes, security and privacy (including supply chain) risk management, and systems engineering processes.
- (3) The enterprise architect is responsible for the following RMF tasks: [NIST: SP 800-37]

Note: The enterprise architect is identified as having "Primary Responsibility" for these RMF tasks. These tasks may be shared responsibilities with other RMF roles. For tasks in which the enterprise architect is identified as having a "Supporting Role", see NIST SP 800-37.

- a. Determine the placement of the system within the enterprise architecture.

10.8.2.3.1.15
(04-29-2025)
**Systems Security
Engineer**

- (1) The systems security engineer is an individual, group, or organization responsible for conducting systems security engineering activities as part of the SDLC. Systems security engineering is a process that captures and refines security requirements for systems and ensures that the requirements are effectively integrated into systems and system elements through security architecting, design, development, and configuration. [NIST: SP 800-37]
- (2) The systems security engineer has the following responsibilities: [NIST: SP 800-37]
 - a. Are part of the development team, designs and develops organizational systems or upgrades existing systems along with ensures continuous monitoring requirements are addressed at the system level;
 - b. Employ best practices when implementing security controls within an information system including software engineering methodologies, security engineering principles, secure design, secure architecture, and secure coding techniques;
 - c. Coordinate their activities with SAISOs/CISOs, security architects, system owners, common control providers, and SSOs;
 - d. Activities associated with protecting information and information systems from unauthorized system activity or behavior to provide confidentiality, integrity, and availability.

Note: Systems security engineer and privacy engineer responsibilities overlap regarding activities associated with protecting the security of PII.

- (3) The systems security engineer has the following ISCM responsibilities: [Treasury: ISCM]
 - a. Capture and refine security requirements and ensure that the requirements are effectively integrated into IT component products and systems through purposeful security architecting, design, development, and configuration;
 - b. Collaborate with system development teams to design and develop organizational systems or upgrade legacy systems;
 - c. Employ best practices when implementing security controls within an system including software engineering methodologies, system/security engineering principles, secure design, secure architecture, and secure coding techniques; and
 - d. Coordinate their security-related activities with security architects, CISOs, system owners, common control providers, and SSOs.

10.8.2.3.1.16
(04-29-2025)
**Security and Privacy
Architect**

- (1) The security and privacy architect is an individual, group, or organization responsible for ensuring that stakeholder protection needs and the corresponding system requirements necessary to protect organizational missions and business functions and individuals' privacy are adequately addressed in the enterprise architecture including reference models, segment architectures, and solution architectures (systems supporting mission and business processes). [NIST: SP 800-37]
- (2) The security and privacy architect serves as the primary liaison between the enterprise architect and the systems security engineer and coordinates with system owners, common control providers, and SSOs on the allocation of controls. [NIST: SP 800-37]

- (3) Security and privacy architects, in coordination with SSOs, advise AOs, CIOs, senior accountable officials for risk management or risk executive (function), SAISOs/CISOs, and SAOPs on a range of security and privacy issues. Examples include establishing authorization boundaries; establishing security or privacy alerts; assessing the severity of deficiencies in the system or controls; developing plans of action and milestones; creating risk mitigation approaches; and potential adverse effects of identified vulnerabilities or privacy risks. [NIST: SP 800-37]
- (4) When the security architect and privacy architect are separate roles: [NIST: SP 800-37]
 - a. The security architect is generally responsible for aspects of the enterprise architecture that protect information and information systems from unauthorized system activity or behavior to provide confidentiality, integrity, and availability.
 - b. The privacy architect is responsible for aspects of the enterprise architecture that ensure compliance with privacy requirements and manage the privacy risks to individuals associated with the processing of PII.
 - c. Security architect and privacy architect responsibilities overlap regarding aspects of the enterprise architecture that protect the security of PII.
- (5) The security and privacy architect is responsible for the following RMF tasks: [NIST: SP 800-37]

Note: The security architect is identified as having “Primary Responsibility” for these RMF tasks. These tasks may be shared responsibilities with other RMF roles. For tasks in which the security architect is identified as having a “Supporting Role”, see NIST SP 800-37.

- a. Determine the placement of the system within the enterprise architecture;
- b. Allocate security and privacy requirements to the system and to the environment of operation; and
- c. Allocate security and privacy controls to the system and to the environment of operation.

10.8.2.3.1.17
(04-29-2025)
**Chief Financial Officer
(CFO)**

- (1) The CFO is the senior financial advisor to the investment review board (IRB) and the agency head. Information security investments fall within the purview of the CFO and are included in the CFO’s reports. [NIST: SP 800-100]

10.8.2.3.1.18
(04-29-2025)
Privacy Officer

- (1) The role of the privacy officer and/or senior agency official for privacy (SAOP) is designated by the head of agency and has agency-wide responsibility and accountability for developing, implementing, and maintaining an agency-wide privacy program to manage privacy risks, develop and evaluate privacy policy, and ensure compliance with all applicable statutes, regulations, and policies regarding the creation, collection, use, processing, storage, maintenance, dissemination, disclosure, and disposal of PII by programs and information systems. [OMB: A-130 Appendix I (5)(f)]

Note: This role within the IRS is assigned to the Chief Privacy Officer of Privacy, Governmental Liaison and Disclosure (PGLD).

Note: For more information about PGLD, refer to IRM 1.1.27, *Organization and Staffing, Privacy, Governmental Liaison and Disclosure (PGLD)* and the PGLD website.

- (2) The privacy officer has the following responsibilities: [NIST: SP 800-37]
- a. Coordinate with the senior agency information security officer to ensure coordination of privacy and information security activities;
 - b. Review and approve the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information;
 - c. Designate which privacy controls will be treated as program management, common, system-specific, and hybrid privacy controls;
 - d. Identify assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks;
 - e. Review and approve privacy plans for information systems prior to authorization, reauthorization, or ongoing authorization;
 - f. Review authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information to ensure compliance with privacy requirements and manage privacy risks;
 - g. Conduct and document the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency; and
 - h. Establish and maintain a privacy continuous monitoring program to maintain ongoing awareness of privacy risks and assess privacy controls at a frequency sufficient to ensure compliance with privacy requirements and manage privacy risks.
- (3) The privacy officer is responsible for the following RMF tasks: [NIST: SP 800-37]

Note: The privacy officer is identified as having “Primary Responsibility” for these RMF tasks. These tasks may be shared responsibilities with other RMF roles. For tasks in which the privacy officer is identified as having a “Supporting Role”, see NIST SP 800-37.

- a. Identify and assign individuals to specific roles associated with security and privacy risk management;
- b. Assess organization-wide security and privacy risk and update the risk assessment results on an ongoing basis;
- c. Identify, document, and publish organization-wide common controls that are available for inheritance by organizational systems;
- d. Identify and understand all stages of the information life cycle for each information type processed, stored, or transmitted by the system;
- e. Review and approve the security categorization results and decision;
- f. Assemble the authorization package and submit the package to the authorizing official for an authorization decision;
- g. Monitor the information system and its environment of operation for changes that impact the security and privacy posture of the system; and
- h. Report the security and privacy posture of the system to the authorizing official and other organizational officials on an ongoing basis in accordance with the organizational continuous monitoring strategy.

- (4) The SAOP (i.e., privacy officer) has the following responsibilities: [OMB: A-130 Appendix I (4)(e)]
- a. Develop and maintain a privacy program plan that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the SAOP and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks;
 - b. Develop and maintain a PCM strategy and PCM program to maintain ongoing awareness of privacy risks and assess privacy controls at a frequency sufficient to ensure compliance with applicable privacy requirements and manage privacy risks;
 - c. Conduct and document the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency across all agency risk management tiers to ensure continued compliance with applicable privacy requirements and manage privacy risks;
 - d. Identify assessment methodologies and metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manage privacy risks;
 - e. Designate which privacy controls will be treated as program management, common, information system-specific, and hybrid privacy controls at the agency;
 - f. Review IT capital investment plans and budgetary requests to ensure that privacy requirements (and associated privacy controls), as well as any associated costs, are explicitly identified and included, with respect to any IT resources that will be used to create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII;
 - g. Review and approve, in accordance with FIPS 199 and NIST SP 800-60, the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII;
 - h. Review and approve the privacy plans for agency information systems prior to authorization, reauthorization, or ongoing authorization;
 - i. Review authorization packages for information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to ensure compliance with applicable privacy requirements and manage privacy risks, prior to authorizing officials making risk determination and acceptance decisions; and
 - j. Coordinate with the CIO, the senior agency information security officer, and other agency officials in implementation of these requirements.

#

[illegible]

[illegible]

- 10.8.2.3.1.18.1
(04-29-2025)
IRS Privacy Offices

- ##

##

10.8.2.3.1.18.2
(04-29-2025)
System Privacy Officer

- (1) The system privacy officer is an individual responsible for ensuring that the privacy posture is maintained for an organizational system and works in close collaboration with the system owner. [NIST: SP 800-37]
- (2) The system privacy officer has the following responsibilities: [NIST: SP 800-37]
 - a. Serves as a principal advisor on all matters, technical and otherwise, involving the privacy controls for the system.
 - b. Have the knowledge and expertise to manage the privacy aspects of an organizational system and, in many organizations, is assigned responsibility for the day-to-day system privacy operations.

Note: This responsibility includes, but is not limited to, physical and environmental protection; personnel security; incident handling; and privacy training and awareness.

- c. Assist in the development of the system-level privacy policies and procedures and ensure compliance with those policies and procedures.
- d. Coordinates with the system owner and plays an active role in the monitoring of a system and its environment of operation to include developing and updating privacy plans, managing and controlling changes to the system, and assessing the privacy impact of those changes.
- e. Is responsible for aspects of the system that ensure compliance with privacy requirements and manage the privacy risks to individuals associated with the processing of PII.

Note: SSO and system privacy officer responsibilities overlap regarding aspects of the system that protect the security of PII.

- (3) The system privacy officer is responsible for the following RMF tasks: [NIST: SP 800-37]

Note: The system privacy officer is identified as having “Primary Responsibility” for these RMF tasks. These tasks may be shared responsibilities with other RMF roles. For tasks in which the system privacy officer is identified as having a “Supporting Role”, see NIST SP 800-37.

- a. Conduct a system-level risk assessment and update the risk assessment results on an ongoing basis;
- b. Define the security and privacy requirements for the system and the environment of operation;
- c. Allocate security and privacy requirements to the system and to the environment of operation; and
- d. Allocate security and privacy controls to the system and to the environment of operation.

10.8.2.3.1.19
(04-29-2025)

Physical Security Officer

- (1) The physical security officer is responsible for the overall enforcement, implementation and management of physical security controls across an organization, to include integration with applicable information security controls. As information security programs are developed, senior agency officials work to ensure this coordination of complementary controls. [NIST: SP 800-100]

Note: Within the IRS, the chief, facilities management and security services (FMSS), serves as the senior official with responsibility for ensuring physical security requirements are established and achieved.

- (2) In consideration of information security, the physical security officer, serves as the senior official responsible for: [NIST: SP 800-100]
 - Developing, promulgating, implementing, and monitoring the organization’s physical security programs, to include appropriate controls for alternate work sites;
 - Ensuring organizational implementation and monitoring of access controls (e.g., authorization, access, visitor control);

- Coordinating organizational environmental controls (e.g., ongoing and emergency power support and backups, fire protection, temperature and humidity controls, water damage); and
- Overseeing and managing controls for delivery and removal of assets.

Note: The delivery and removal of assets relates to physical security, not IT inventory.

- (3) Refer to IRM 10.2, *Physical Security Program* series for additional guidance on physical security officer roles & responsibilities.

10.8.2.3.1.20
(04-29-2025)
**Personnel Security
Officer**

- (1) The personnel security officer is responsible for the overall implementation and management of personnel security controls across an organization, to include integration with specific information security controls. [NIST: SP 800-100]
- (2) The Director of Personnel Security and Investigations is responsible for the overall implementation and management of personnel security controls across the IRS, including integration with specific information security controls.
- (3) In consideration of information security, the personnel security officer serves as the senior official and has the following responsibilities: [NIST: SP 800-100]
- a. Develop, promulgate, implement and monitor the organization's personnel security programs;
 - b. Develop and implement position categorization (including third-party controls), access agreements, and personnel screening, termination, and transfers; and
 - c. Ensure consistent and appropriate sanctions for personnel violating management, operation, or technical information security controls.

10.8.2.3.1.21
(04-29-2025)
Employee

- (1) The provisions within this IRM apply to individuals and organizations having contractual arrangements with the IRS, including employees (IRS personnel, consultants, detailees, temporary employees, and interns) which use or operate IT systems.
- (2) An IRS employee (i.e., system user) is an individual or (system) process acting on behalf of an individual that is authorized to access information and information systems to perform assigned duties. System user responsibilities include, but are not limited to, adhering to organizational policies that govern acceptable use of organizational systems; using the organization-provided information technology resources for defined purposes only; and reporting anomalous or suspicious system behavior. [NIST: SP 800-37]
- (3) IRS employees are prohibited from using personal email accounts for official business: [Federal: P.L. 114-113, Section 402]

#

[illegible]

- (5) IRS Employees must: [IRS: IRS-defined]
 - a. Comply with all executive, legislative, Department of Treasury and IRS security policies and procedures;
 - b. Immediately report any incidents of loss or mishandling of IRS IT resources to the IRS CSIRC, their immediate supervisor, and TIGTA;
 - c. Contact *CSIRC* in the event of a suspected incident;

- d. Follow directions given from CSIRC during an incident or as suspicious activities are evaluated;
- e. Attend/complete initial security and privacy briefings and acknowledge completion in writing;
- f. Not access sensitive IT systems until they receive the appropriate clearance for the system;
- g. Complete and acknowledge the completion (i.e., Form 11370) of UNAX training;
- h. Be responsible for protecting any SBU data including PII or tax information that they have in their possession, whether it is paper-based or in electronic form;
- i. Immediately report any incidents of mishandling, tampering, or the loss of a laptop computer to IRS IT cybersecurity organization;
- j. Minimize the threat of viruses from portable mass storage devices (including, but not limited to, flash disks, pen drives, key drives, and thumb drives), by ensuring that these devices have no additional software or firmware beyond storage management and encryption. Also, never knowingly circumvent anti-virus safeguards; and
- k. Escort visitors of IRS facilities.

Note: Refer to IRM 10.8.26, *Information Technology (IT) Security, Government Furnished and Personally Owned Mobile Device Security Policy*, for additional guidance.

- (6) Employees with a mobile computing device(s) must follow all requirements as outlined in IRM 10.8.26 and IRM 10.8.1.
- (7) Refer to IRM 10.8.27 for user responsibilities pertaining to the use of government furnished IT equipment.

10.8.2.3.1.22
(04-29-2025)
Contractor

- (1) The provisions within this IRM apply to individuals and organizations having contractual arrangements with the IRS, including contractors, vendors, and outsourcing providers, which use or operate IT systems.
- (2) An IRS employee (i.e., system user), which includes contractors, is an individual or (system) process acting on behalf of an individual that is authorized to access information and information systems to perform assigned duties. System user responsibilities include, but are not limited to, adhering to organizational policies that govern acceptable use of organizational systems; using the organization-provided information technology resources for defined purposes only; and reporting anomalous or suspicious system behavior. [NIST: SP 800-37]
- (3) IRS contractors are prohibited from using personal email accounts for official business: [Federal: P.L. 114-113, Section 402]

#

[illegible]

(5) Contractors must: [IRS: IRS-defined]

- a. Comply with all executive, legislative and Department of Treasury and IRS security policies and procedures;
- b. Contact *CSIRC* in the event of a suspected incident;
- c. Immediately report any incidents of loss or mishandling of IRS information technology resources to the appropriate supervisor and CSIRC;
- d. Follow directions given from the CSIRC during an incident or as suspicious activities are evaluated;
- e. Attend/complete initial security and privacy briefings and acknowledge completion in writing;
- f. Not access sensitive or classified IT systems until they have received the appropriate clearance for the system;
- g. Complete any acknowledge completion (e.g., Form 11370) of UNAX training;
- h. Be responsible for protecting any SBU data including PII or tax information that they have in their possession, whether it is paper-based or in electronic form;
- i. Immediately report any incidents of mishandling, tampering, or the loss of a laptop computer to IRS Information Technology Cybersecurity organization; and
- j. Minimize the threat of viruses from portable mass storage devices (including, but not limited to, flash disks, pen drives, key drives, and thumb drives), by ensuring that these devices have no additional software or firmware beyond storage management and encryption. Also, never knowingly circumvent anti-virus safeguards.

Note: Refer to IRM 10.8.26 for additional guidance.

- (6) Contractors with government furnished IT equipment (e.g., laptop) must follow all requirements outlined in IRM 10.8.26 and IRM 10.8.1.
- (7) Refer to IRM 10.8.27 for user responsibilities pertaining to the use of government furnished IT equipment.

10.8.2.3.1.23
(11-27-2019)

**Database Administrator
(DBA)**

- (1) Database administrators (DBAs) perform all activities related to maintaining a correctly performing and secure database environment. Responsibilities include design (in conjunction with application developers), implementation, and maintenance of the database system as described in IRM 10.8.21, **Information Technology (IT) Security, Database Security Policy**, and associated IRMs.
- (2) The primary security role of any DBA is to administer and maintain database repositories for proper use by authorized individuals.
- (3) Individuals assigned security responsibilities for database management system (DBMS) environments, including the security specialist (SecSpec) and DBA, must obtain database security technical training necessary to implement the requirements of this IRM. The training must cover the security features specific to the DBMS products the individuals are required to support.
- (4) DBA role accounts have the least level of elevated privileges required to perform DBA-related duties and do not include root or root-level access. DBAs who require the ability to perform certain system administrator functions such as account creation or the editing of system configuration files use a separate system administrator role account that provides these capabilities, but do not receive full system administrator privileges.

- a. DBA's system administrator accounts with limited privileges must be monitored and audited in accordance with IRM 10.8.1. The implementing organization is required to coordinate this activity with the ACIO Cybersecurity.
- (5) At a minimum, the DBA have the following responsibilities:
 - a. Establish security for database objects within the database and for the DBMS according to IRS security policies;
 - b. Support disaster/recovery planning, documentation and implementation efforts for the database(s);
 - c. Establish database points of consistency;
 - d. Coordinate with the SA to integrate database backups into the system related backup and recovery, including creating the backups if necessary;
 - e. Periodically test backup copies of the databases;
 - f. Recover the database to a current or previous state, if necessary;
 - g. Recover individual objects (e.g., data rows) to a current or previous state;
 - h. Identify database requirements of system resources;
 - i. Provide network requirements for the database to the organizations responsible for designing and implementing network services;
 - j. Manage the database configuration (e.g., architecture, internal settings) according to the SA&A operating system security configuration;
 - k. Support Security Assessments and Authorization efforts;
 - l. Monitor/manage database performance and capacity;
 - m. Monitor user activities where appropriate; and
 - n. Enable and configure audit logging on all IRS systems in accordance with IRM 10.8.1, and all other applicable configuration IRMs.

10.8.2.3.1.24
(04-29-2025)

Key-Recovery Agent

- (1) A key-recovery agent is established as part of the cryptographic key management system (CKMS) security policy. [NIST: SP 800-130]
- (2) A key-recovery agent is allowed to recover keys from backup or archive storage after identity verification and authorization of the requesting entity is performed in accordance with the CKMS security policy. [NIST: SP 800-130]
- (3) The key-recovery agent provides support during key recovery procedures. [NIST: SP 800-130]

10.8.2.3.1.25
(11-27-2019)

Network Administrator

- (1) Network administrators (NAs) are responsible for the day-to-day administration of the network devices under their purview.
- (2) At a minimum, NAs have the following responsibilities:
 - a. Configure network device parameters within the documented security standards, using the applicable IRMs, policies and system life cycle documentation;
 - b. Ensure the proper installation, testing, protection and use of network device software, including installing network software fixes and upgrades;
 - c. Maintain the configuration of wireless networks or network devices under their control in accordance with the requirements of IRM 10.8.55, *Information Technology (IT) Security, Network Security Policy*;
 - d. Enable and configure audit logging on all IRS systems in accordance with IRM 10.8.1, and all other applicable configuration IRMs;

- e. Maintain current documentation that properly defines the hardware and software configuration of the network devices and connections for which they are responsible;
- f. Ensure inventories are accurately maintained;
- g. Recommend and implement processes, changes and improvements to programs, procedures and network devices;
- h. Monitor network performance; performing network diagnostics; analyzing network traffic patterns; and
- i. Support disaster recovery planning, documentation, and implementation efforts for the network.

(3) NAs support CSIRC efforts and security incident handling.

(4) NAs apply patches and hot fixes as directed, following configuration management policies and procedures.

Note: Refer to IRM 10.8.50, *Information Technology (IT) Security, IDRS Security Controls*, for security patch management guidance.

10.8.2.3.1.26
(05-16-2014)

**Program
Developer/Programmer**

- (1) Program developers/programmers are responsible for the development, testing and maintenance of application programs.
- (2) At a minimum, program developers/programmers have the following responsibilities:
 - a. Develop application programs in accordance with established organizational policies and procedures;
 - b. Develop application programs in accordance with IRM 10.8.1 and IRM 10.8.6;
 - c. Adhere to IRS configuration management (CM) practices and OneSDLC requirements; and
 - d. Create installation scripts, processes, and instructions for production organizations to utilize. The developer incorporates feedback mechanisms into the installation processes as needed.

10.8.2.3.1.27
(05-16-2014)

Web Developer

- (1) Web developers have the following responsibilities:
 - a. Development of websites and applications, including creating/manipulating/implementing graphic images and formulating documentation for websites and web applications in accordance with IRM 10.8.1; and
 - b. Formulating specification requirements, producing level of effort estimates, providing informational support to security certifications, and performing web server and web application server project planning, scheduling, and testing.

Note: Refer to IRM 10.8.22, *Information Technology (IT) Security, Web Server Security Policy*, for additional guidance.

10.8.2.3.1.28
(03-31-2017)

**Resource Access
Control Facility (RACF)
Specialist**

- (1) The roles and responsibilities for the resource access control facility (RACF) specialist are located in IRM 10.8.33, *Information Technology (IT) Security, Mainframe System Security Policy*.

Note: Refer to IRM 10.8.33 for RACF specialist responsibilities.

10.8.2.3.1.29
(11-27-2019)

**Security Specialist
(SecSpec)**

- (1) SecSpecs are responsible for reviewing all activities of the SAs, NAs, DBAs, anyone responsible for the operation or administration of IT equipment, anyone involved with user administration, such as the EAA staff, and all other users to ensure they are compliant with security requirements.
- (2) SecSpecs oversee any and all user (e.g., system, database, application, etc.) administration regardless of how or who performs it.
- (3) Additionally, SecSpecs have the following responsibilities:
 - a. Ensure the site contingency plans remain up-to-date in response to new security requirements or changes in the IRS IT architecture;
 - b. Conduct and support all security reviews of IRS systems and networks;
 - c. Provide or recommend security measures and countermeasures based on the security reviews and security policies;
 - d. Upon management request, review individual user's access verifying it is the least privilege necessary to perform their job;
 - e. Inspect and monitor user files, as directed by management;
 - f. Conduct security audits, verifications and acceptance checks, while maintaining documentation on the results;
 - g. Promote security awareness and compliance;
 - h. Report security incidents including those discovered while reviewing audit logs/trails; and
 - i. Assist with developing a deviation request, such as interpreting policy to determine if a deviation is required, assisting with the risk assessment and possible mitigations.
- (4) SecSpecs review all types of audit logs/trails and observe system activity at least weekly in order to:
 - a. Ensure integrity, confidentiality and availability of information and resources;
 - b. Detect inappropriate user and system actions that could be construed as security incidents;
 - c. Investigate possible security incidents; and
 - d. Monitor user or system activities where appropriate.
- (5) SecSpecs do not perform system/security administration on any system/platform/application, etc.
- (6) SecSpecs have read-only access to system resources and shall not modify audit settings.
- (7) SecSpecs have the following responsibilities:
 - a. Be familiar with the requirements and procedures specified in IRM 10.8.1;
 - b. Notify their management of any implementation discrepancies between the requirements of IRM 10.8.1 and the actual audit logging status of systems that the SecSpecs support; and
 - c. Follow any applicable organizational-level incident reporting procedures (such as contacting management, system administrators, or the Computer Security Incident Response Center) in the event that evidence of suspicious activity is discovered in the course of reviewing security audit log information.

Note: Refer to IRM 10.8.1 for additional guidance.

- (8) SecSpecs are concerned with the security and integrity of the database and be responsible for:
- a. Obtaining database security technical training necessary to implement the requirements of this IRM. The training covers the security features specific to the DBMS products the individuals are required to support;
 - b. Ensuring that the requirements of IRM 10.8.1 and IRM 10.8.21 are met;
 - c. Ensuring that DBAs, SAs, and others having daily operational responsibilities for IRS databases comply with the security requirements of IRM 10.8.21. In general, the SecSpec is not expected to personally implement the requirements, but rather ensure that others do so; and
 - d. Reporting IRM non-compliance issues initially to DBAs and SAs for resolution, and escalate non-compliance reporting to IRS management officials (such as the SSO and system owner) as necessary to bring systems into compliance with IRM 10.8.21.

Note: Refer to IRM 10.8.21 for additional guidance.

- (9) SecSpecs are concerned with the security and integrity of Linux/Unix servers, workstations and devices, and are responsible for:
- a. Reviewing all activity of administrators and those responsible for administration of IT equipment;
 - b. Ensuring that SAs and others having daily operational responsibilities for IRS Linux/Unix servers and workstations comply with the security requirements of this IRM. The SecSpec is not expected to personally implement the requirements but ensures that others do so;
 - c. Reporting Windows IRM non-compliance issues initially to Information System Owner and SAs for resolution, and escalate non-compliance reporting to IRS management officials as necessary to bring systems into compliance with IRM 10.8.15, **Information Technology (IT) Security, General Platform Operating System Security Policy**; and
 - d. Not have operating SA privileges.

Note: Refer to IRM 10.8.15 for additional guidance.

- (10) IT SecSpecs are concerned with the security and integrity of Windows servers, workstations and devices, and are responsible for:
- a. Reviewing all activity of administrators and responsible for administration of IT equipment;
 - b. Ensuring that SAs and others having daily operational responsibilities for IRS Windows servers and workstations comply with the security requirements of this IRM. The SecSpec is not expected to personally implement the requirements but ensures that others do so;
 - c. Reporting Windows IRM non-compliance issues initially to Information System Owner and SAs for resolution, and escalate non-compliance reporting to IRS management officials as necessary to bring systems into compliance with IRM 10.8.15; and
 - d. Not have operating System Administrator privileges.

Note: Refer to IRM 10.8.15 for additional guidance.

- (11) IT SecSpecs are concerned with the security and integrity of Web application servers and are responsible for:

- a. Ensuring that the requirements of IRM 10.8.22 are met;
- b. Ensuring that SAs and others having daily operational responsibilities for IRS Web servers and Web application servers comply with the security requirements of IRM 10.8.22; and
- c. Reporting IRM non-compliance issues initially to Information System Owner and SAs for resolution, and escalate non-compliance reporting to IRS management officials as necessary to bring systems into compliance with IRM 10.8.22.

Note: Refer to IRM 10.8.22 for additional guidance.

- (12) SecSpecs support security assessments and authorization efforts; security control testing (monthly and annual), contingency testing, documentation development, POA&M weakness correction, and ongoing security vulnerability remediation efforts.

10.8.2.3.1.30
(03-31-2017)

**System Administrator
(SA)**

- (1) SAs are technicians who administer, maintain, and operate information systems. They are responsible for implementing technical security controls on computer systems and for being familiar with security technology that relates to their system.
- (2) At a minimum, SAs have the following responsibilities:
 - a. Add, remove, maintain system users and configure their access controls to provide the users necessary access with least privilege, as defined for each user in the access control system (e.g., BEARS);
 - b. Provide lists of system users for systems under their control and providing the lists to the appropriate users' managers and appropriate SecSpecs for review, update and certification;
 - c. Configure system parameters within the documented security standards, using the applicable IRMs and system life cycle documentation;
 - d. Maintain current documentation that properly defines the technical hardware and software configuration of system and network connections for systems they are responsible for;
 - e. Ensure the proper installation, testing, protection, and use of system and application software;
 - f. Install and manage application server software including development tools and libraries, software compilers, code builds, and middleware interfaces between servers and application servers and back-end storage media in accordance with IRM 10.8.6;
 - g. Install and manage servers and workstation software in accordance with the applicable IRM for the OS in use;
 - h. Start up and shut down the system;
 - i. Perform regular backups and recovery tests and other associated contingency planning responsibilities for systems for which they are responsible;
 - j. Enable, configure, and archive audit logs/trails and system logs for review by the SecSpecs for all IRS systems in accordance with IRM 10.8.1, and all other applicable configuration IRMs;
 - k. Monitor system/user access for performance and security concerns;
 - l. Establish conditions on the system so that other operational entities can perform application management activities; and
 - m. Run various utilities and tools in support of the SecSpecs.

Note: This includes managing additional access controls, configurations, or roles that technologies may require.

- (3) SAs are responsible for supporting the SecSpec's needs for read access to system resources as defined in the access control request (e.g., BEARS).
- (4) SAs support techniques that allow non-SAs to perform user administration in a controlled and limited manner while still managing access to system resources and other directories and files.
- (5) The use of non-SAs for user administration must be documented in the Computer Operations Handbook or equivalent for the system/application and in the security assessments and authorization documentation for the relevant general support system (GSS) and application.
- (6) The use of non-SAs for user administration must be established via a memorandum of agreement (MOA) and accepted by the involved AO.
- (7) Depending on the environment, the SA may perform user support for password issues. This can include (but is not limited to) resetting or issuing a new password when the user forgets the current one or locks the account.
- (8) SAs support CSIRC efforts and security incident handling.
- (9) SAs install security patches in a timely and expeditious manner based on CSIRC's criticality designation.
- (10) SAs apply patches and hot fixes as directed, following configuration management policies and procedures and contact IRS IT cybersecurity organization for further information concerning security patch management.
- (11) SAs support information system contingency plan (ISCP) and disaster recovery (DR) plan development and accuracy.

10.8.2.3.1.31
(05-16-2014)

**Systems Operations
Staff**

- (1) The role of the systems operations staff is assigned to the IRS, Enterprise Operations organization.
- (2) Systems operations staff have the following responsibilities:
 - a. Safeguard equipment, data, and magnetic media during day-to-day performance of their duties; and
 - b. Be able to perform SA duties delegated them from the SA with associated least privilege permissions to perform those functions.

10.8.2.3.1.32
(05-16-2014)

**Telecommunications
Specialist**

- (1) The role of telecommunications specialists is assigned to the IRS, User and Network Services (UNS) organization.
- (2) The IT UNS organization is responsible for providing communications services, including voice, data, video, and fax service.
- (3) The telecommunications specialists are responsible for the management of the communication systems in compliance with IT security policy and federal regulations.
- (4) The telecommunications specialists support ISCP and DR plan development, accuracy, documentation, and implementation efforts for their system(s).

- 10.8.2.3.1.33
(05-16-2014)
User Administrator (UA)
- (1) The user administrator (UA) role pertains only to organizations (e.g., Enterprise Service Desk - Enterprise Account Administration (ESD-EAA)) who provide the service.
 - (2) UAs have no more capability than appropriate to establish a user on a system or to establish a user within an application.
 - (3) UAs use the IRS approved access control (e.g., BEARS) process.
 - (4) An SA or NA establishing user access does not assume the UA role.
- 10.8.2.3.1.34
(04-29-2025)
Integrated Data Retrieval System (IDRS) Security Analyst
- (1) The roles and responsibilities for the integrated data retrieval system (IDRS) security analyst have been relocated to IRM 10.8.34, *Information Technology (IT) Security, IDRS Security Controls*.
- Note:** Refer to IRM 10.8.34 for IDRS security analyst responsibilities.
- 10.8.2.3.1.35
(04-29-2025)
Integrated Data Retrieval System (IDRS) Security Account Administrator
- (1) The roles and responsibilities for the integrated data retrieval system (IDRS) security account administrator have been relocated to IRM 10.8.34.
- Note:** Refer to IRM 10.8.34 for IDRS security account administrator responsibilities.
- 10.8.2.3.1.36
(04-29-2025)
Computer Audit Specialist (CAS)
- (1) The computer audit specialist (CAS) security role, which is specific to IRS business units (e.g., Large Business and International (LB&I)), is responsible for working with taxpayer records in which these records are formatted in a usable format for team members. These formats may be unique to the taxpayer and may involve the use of many different tools and programs.
 - (2) CAS' loads, runs, and configures software and services on machines to meet examination objectives. This may require them to add and remove device drivers and install/uninstall various programs as needed to work with the taxpayer records.
 - (3) CAS' have the ability to add, configure and remove software. This allows them to run multiple types of audits, whose software package may not be compatible with one another as a result; cannot be installed and loaded onto a particular system simultaneously.
- 10.8.2.3.1.37
(05-16-2014)
Functional Workstation Specialist
- (1) The functional workstations specialist responsibilities include, but are not limited to the following:
 - a. Have a full analytical and operational knowledge of specific software applications to resolve systemic & procedural problems and user errors thereby enabling the user to perform all tasks related to their jobs;
 - b. Have a working knowledge of operating systems, protocols, and equipment used in business customer organizations;
 - c. Have a working knowledge of methods and practices for troubleshooting, recovering, modifying, and improving application files;
 - d. Utilize extensive problem-solving skills and limited elevated permissions in order to diagnose and troubleshoot application problems in the performance of customer support;

- e. Have a working knowledge of all BOD processes including field, support functions and the Campuses;
- f. Act as a liaison between the Area/Territory Offices, Campus, and National Office;
- g. Provide both oral and written communication to all users' levels (including Area Managers, Territory Managers, Group Managers);
- h. Coordinate activities relating to the security posture of the application with responsible business units and IRS IT (UNS, EOPS, AD) staff;
- i. Forward problem descriptions to the appropriate personnel as these individuals are often the first to encounter application problems;
- j. Coordinate reporting within the business unit to ensure workstations are in compliance for consistency purposes;
- k. Ability to perform in an instructor capacity by conducting training and security awareness programs;
- l. Educate & communicate to end users security awareness and practices in the context of performing these and other tasks;
- m. Analyze and evaluate the effectiveness of system operations and make recommendations to correct deficiencies. Develops plans, goals, & objectives for long-range implementation and administration of program activity;
- n. Ensure adequate physical security controls are implemented at the workstation level;
- o. Provide technical direction to users who ensure the confidentiality, integrity, and availability of the tax systems;
- p. Consult with users to ensure they have applied patches and hot fixes as directed following configuration management policies and procedures in compliance with the IRM for purposes of application support;
- q. Escalate IT security matters to the respective party(s) as defined in local guidance; and
- r. General knowledge of disaster recovery/contingency planning terminology and concepts.

10.8.2.3.1.38
(05-16-2014)

Management/Program Analyst

- (1) The management/program analyst, in support of meeting FISMA requirements, has the following responsibilities:
 - a. Perform analytical studies affecting agency program operations;
 - b. Analyze and evaluate the effectiveness of program operations and make recommendations to correct deficiencies; and
 - c. Develop plans, goals, & objectives for long-range implementation and administration of program activity.

10.8.2.3.1.39
(04-29-2025)

System Designer

- (1) System designers (a.k.a. system developers) responsible for developing, implementing, and monitoring policies and controls to ensure data accuracy, security and legal regulatory compliance throughout the system lifecycle.
- (2) System designers assist in the:
 - a. Review and approval of products to ensure they incorporate and meet IRS security requirements; and
 - b. Planning, documentation and integration of security into a system's lifecycle from its initiation to its disposal phases.
- (3) System designers are responsible for identifying IT assets and determining their value for establishing implementation security safeguard priorities.

- (4) System designers ensure security control assessments are conducted during the different stages of a system's life cycle in accordance with IRM 10.8.1 (e.g., SA-11 Developer Security Testing and Evaluation) and NIST SP 800-160 Volume 1 Revision 1, *Engineering Trustworthy Secure Systems*, and NIST SP 800-160 Volume 2 Revision 1, *Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*.

Note: Refer to IRM 10.8.1 (e.g., SA-11 Developer Security Testing and Evaluation) for additional security control assessments guidance.

- (5) System designers consult and collaborate with the IRS Enterprise Architect and concerned system security engineer (SSE) and SSO whenever designing new system(s) and/or sub-systems functionality.

10.8.2.3.1.40
(05-16-2014)

**Technical Support Staff
(Desktop)**

- (1) The technical support staff is responsible for educating end-users in security procedures and practices in the context of performing their tasks.

10.8.2.3.1.41
(09-30-2021)

**Security Staff (Physical
Security)**

- (1) The physical security staff is responsible for developing and enforcing appropriate physical security controls, often in consultation with information security management, program and functional managers, and others. [NIST: SP 800-12]

- (2) The physical security staff the following responsibilities:

- a. Review, develop, promulgate, implement, and monitor the organization's physical security programs, for the protection of employees, equipment and property at all IRS facilities; and
- b. Review organizational implementation and monitoring of access controls (i.e., authorization, access, visitor control, transmission medium, display medium, logging) to ensure they are in accordance with NIST, Treasury and IRS physical security standards and guidance.

10.8.2.3.1.42
(09-12-2022)

**Cyber Critical
Infrastructure Protection
(CIP) Coordinator**

- (1) The CIP coordinator is designated by the CIO. In this role, the IRS cyber CIP coordinator has the following responsibilities:
- a. Act as the primary point of contact for addressing IRS CIP issues with Treasury;
 - b. Participate in CIP assessments and critical infrastructure for the IRS;
 - c. Maintain a prioritized list of critical infrastructure for the IRS;
 - d. Participate in all CIP work group meetings;
 - e. Provide coordination and collaboration among stakeholders on all IRS Cyber CIP activities; and
 - f. Determine the IRS cyber security program status relative to the plan's objectives.

10.8.2.3.2
(07-12-2010)

**Organization/Functional
Roles and
Responsibilities**

- (1) This section provides functional roles and responsibilities for personnel who have security related responsibility for the protection of information systems they operate, manage and support. These roles are defined in accordance with FISMA, NIST, OMB, TD P 85-01 and IRS policy and guidelines.

10.8.2.3.2.1
(04-29-2025)
**IRS Information
Technology
Cybersecurity
Organization**

- (1) In collaboration with the business and functional unit owner, the IRS IT cybersecurity organization has the following responsibilities:
 - a. Develop, publish, and disseminate security policy;
 - b. Develop security controls for systems and applications;
 - c. Conduct annual testing of the systems and applications;
 - d. Test and validate the effectiveness of corrective actions;
 - e. Ensure ISCP and DR requirements are addressed for all applications and systems owned by IRS IT cybersecurity organization;
 - f. Implement corrective actions and validate fixes to mitigate vulnerabilities assigned to IRS IT cybersecurity;
 - g. Create and implement configuration management plans that control changes to systems and applications during development; and
 - h. Track security flaws, require authorization of changes, and provide documentation of the configuration management plan and its implementation.
- (2) For DR and ISCP, the IRS IT cybersecurity organization has the following responsibilities:
 - a. Jointly develop the detailed content of each DR plan to include recovery of the system, the application, and the associated data, including all platforms applicable to the system/application;
 - b. Ensure requirements, priorities, recovery times, and costs of each DR plan are appropriate and achievable;
 - c. Support the exercise of the ISCP;
 - d. Ensure maintenance and update to the content of the DR plans by BU;
 - e. Support procurement activities to enhance DR capabilities to meet stated business objectives;
 - f. Ensure DR equipment located at recovery locations for the business units are maintained;
 - g. Ensure establishment of DR location(s) based on FISMA, NIST, and IRS DR policy and requirements;
 - h. Ensure offsite storage of data needed for recovery and ongoing backup of data;
 - i. Establish a schedule and notify IRS IT cybersecurity and the impacted BU of the schedule for coordinating ISCP/DR exercises and tests throughout the year;
 - j. Annually test each major system and establish DR testing priorities; and
 - k. Work with business units and IRS IT cybersecurity organization to resolve (if possible) issues identified during DR testing or document reasons/risk/impact.

Note: Refer to IRM 10.8.60, *Information Technology (IT) Security, (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance*, for additional guidance.

- (3) IRS IT cybersecurity organization has the following responsibilities:
 - a. Develop security controls for systems and applications;
 - b. Maintain and disseminate IRM 10.8.1;
 - c. Establish sufficient controls to ensure equipment is used appropriately; and

- d. Ensure evidence is preserved for potential prosecution in lieu of immediate eradication; detailed instructions from CSIRC (or possibly TIGTA) shall be given to SAs, NAs, and other key personnel on how to preserve the evidence.

Note: Refer to IRM 10.8.1 for additional guidance.

- (4) IRS IT Cybersecurity organization notifies the CSIRC of suspicious activities and complies with CSIRC directions.
 - a. IRS IT Cybersecurity organization complies with their internal configuration management requirements.
 - b. IRS IT Cybersecurity organization performs containment activities.
- (5) For interconnections and interconnection service agreements, the IRS IT cybersecurity organization has the following responsibilities:
 - a. Provide security engineering review of interconnections with external partners and the supporting agreements; and
 - b. Ensure that all appropriate ISAs (or other approved agreements) are in place before interconnections are allowed to be established and activated.

10.8.2.3.2.2
(04-29-2025)

**IRS Information
Technology (IT) User
and Network Services
(UNS) Organization**

- (1) The IRS IT UNS organization administers the firewall devices comprising the perimeter firewall environment.

Note: Refer to IRM 10.8.54, *Information Technology (IT) Security, Minimum Firewall Administration Requirements*, for additional guidance.

- (2) The IRS IT UNS organization designs, implements, and maintains the IRS network perimeter demilitarized zone (DMZ).
- (3) The IRS IT UNS organization ensures that the IRS minimum firewall requirements and policies are met.
- (4) The IRS IT UNS organization provides administration, operation and maintenance for the firewall devices comprising the perimeter firewall environment. This includes, but is not limited to:
 - a. Implementing CSIRC-approved firewall change requests (FCRs);
 - b. Troubleshooting access problems;
 - c. Applying security patches and software updates;
 - d. Refreshing hardware; and
 - e. Securing maintenance contracts.
- (5) The system owner for IRS IT UNS organization has the following responsibilities:
 - a. Notify and route information to the appropriate organizational POCs;
 - b. Notify CSIRC of any ticket needing CSIRC's attention;
 - c. Notify CSIRC for a user's problem that originated with the enterprise service desk; and
 - d. Report suspicious activity or incidents.
- (6) The IRS IT UNS organization monitors the "up/down" status of the network and firewall devices in the IRS network perimeter DMZ.

#

#

- (3) In preparation for IR and meet compliancy with Treasury TCIO M 22-12, CSIRC has the following responsibilities: [Treasury: IRP]

- a. Serve as primary coordination point for IR within the IRS;
 - i. It is crucial at the initial analysis stage for CSIRC to identify whether the incident involves PII, including paper or oral disclosures (e.g., unauthorized disclosures to individuals who lack a need to know).

Note: The term PII, as defined by OMB in Circular No. A-130 as, *“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.”* This broadly-worded definition encompasses a great deal of information. Therefore, Treasury is required to perform an assessment to determine the risk that an individual can be identified based on the information itself or when the information is combined with other information that is linked or linkable to the individual. The IRS therefore must ensure front-line personnel have a full understanding of the breadth of the OMB definition of PII. Refer to IRM 10.5.1.

- b. Oversee IR activities at the IRS level;
- c. Serve as the liaison to the TSOC for all communications and follow up activities in response to an incident;
- d. Ensure compliance with the Treasury IRP; and
- e. Report to TSOC in accordance with IRP section 4.2.3 Reporting and Escalation reporting requirements.

Note: Refer to IRM 10.8.1 and *Treasury Incident Response Plan (IRP)* for additional incident response guidance.

- (4) CSIRC is responsible for operating and maintaining a wireless intrusion detection system.

Note: Refer to IRM 10.8.55 for additional guidance.

- (5) CSIRC has the following responsibilities: [NIST: SP 800-53]

- a. Establish and manage the IRS computer security incident handling capability;
- b. Establish and maintain the policies for the IRS security incident handling capability;
- c. Have four basic functions defining the Incident Management Lifecycle:
 - Prevention
 - Detection
 - Response
 - Reporting
- d. Track and document information system security incidents on an ongoing basis;

- e. Actively and continuously monitor IT resources, to include but not limited to firewalls, wireless, network-based and host-based intrusion detection systems (IDSs) and event records, watching for suspicious cyber activities (termed, “suspicious activities,” within IRM 10.8.1);
- f. Conduct offline/passive monitoring of logs from IDSs, firewalls, Web servers, and critical hosts, watching for possible security incidents;
- g. Inform TIGTA of suspected criminal activities, following established procedures in the memorandum of understanding (MOU) with TIGTA;
- h. Perform routine vulnerability assessments (announced and unannounced);

Note: These assessments include active/passive monitoring, system and network scanning to support Security Assessments and Authorization processes, etc.

- i. Serve as front line/1st tier support for security alerts;
- j. Perform initial analyses to determine validity, applicability, impact, and risks from potential security incidents;
- k. Record all detected intrusion attempts and report such events;
- l. Ensure that forensic evidence is properly collected and retained when investigating computer and network security incidents;
- m. Promptly report incident information to appropriate authorities;
- n. Maintain an Incident Handling Contact List of personnel that are involved in security incident handling activities. The list must include contact information (phone numbers, etc.) so they can be reached in the event of a security incident;
- o. Employ automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information;
- p. Maintain all incident reports in an incident database (For electronic reporting, the original messages will be retained. For telephonic reporting, the analyst who answered the phone will prepare a summary and enter it into the database. For each incident, the database record will include the date and time the report was received, the person who submitted the report, the handling analyst, and the original message or a summary.);
- q. Develop a plan to acquire the data used for analysis;
- r. Create a plan (i.e., data acquisition plan) that prioritizes the sources, establishing the order in which the data should be acquired;
- s. Respond to government forum of incident response teams (GFIRST) surveys that are of an incidental or routine administrative nature;
- t. Not respond to GFIRST surveys inquiring as to the status of Treasury systems, whether certain remediation actions have taken place, future security budget plans, and the like;
- u. Participate in an MOA/MOU with the situational awareness management center (SAMC); and
- v. Establish an MOA/MOU with TIGTA to: establish formal custody transfer procedures for forensic evidence; and establish reporting procedures for incidents.

Note: Refer to IRM 10.8.1 for additional guidance.

(6) CSIRC has the following responsibilities:

- a. Establish and manage the IRS minimum firewall administration requirements;
- b. Oversee and approve all rule sets for the IRS network perimeter firewall environments; and

- c. Review and concur with IRS IT UNS organization DMZ efforts.

Note: Refer to IRM 10.8.54 for additional guidance.

10.8.2.3.2.4
(07-12-2010)

**Situational Awareness
Management Center
(SAMC)**

- (1) SAMC has the following responsibilities:

- a. Process physical security incidents; and
- b. Establish a MOA/MOU with CSIRC to establish notification procedures for when either organization discovers an incident affects the other; ensure information is recorded in the incident database for both incidents; and ensure shared staff meets the requirements of each organization.

Note: Refer to IRM 10.8.60 for additional guidance.

10.8.2.3.2.5
(04-29-2025)

**IRS Patch and
Vulnerability Group
(PVG)**

- (1) An IRS PVG is created to facilitate the identification and distribution of patches within the IRS. The PVG is tasked to implement the patch and vulnerability management program throughout the IRS. The PVG is the central point for vulnerability remediation efforts, such as OS and application patching and configuration changes. [NIST: SP 800-40r2]

- (2) The PVG has the following duties: [NIST: SP 800-40r2]

- a. **System Inventories:** Use existing inventories of the organization's IT resources to determine which hardware equipment, operating systems, and software applications are used within the organization. The PVG also maintains a manual inventory of IT resources not captured in the existing inventories.
- b. **Monitor for Vulnerabilities, Remediations, and Threats:** Monitor security sources for vulnerability announcements, patch and non-patch remediations, and emerging threats that correspond to the software within the PVG's system inventory.
- c. **Prioritize Vulnerability Remediation:** Prioritize the order in which the organization addresses vulnerability remediation;
- d. **Create an Organization-Specific Remediation Database:** Create a database of remediations that need to be applied organization-wide;
- e. **Conduct Generic Testing of Remediations:** Test patches and non-patch remediations on IT devices that use standardized configurations. This will avoid the need for local administrators to perform redundant testing. The PVG also works closely with local administrators to test patches and configuration changes on important systems.
- f. **Deploy Vulnerability Remediations:** Oversee vulnerability remediation;
- g. **Distribute Vulnerability and Remediation Information to Local Administrators:** Inform local administrators about vulnerabilities and remediations that correspond to software packages included within the PVG scope and that are in the organizational software inventory.
- h. **Perform Automated Deployment of Patches:** Deploy patches automatically to IT devices using enterprise patch management tools. Alternately, the PVG works closely with the group actually running the patch management tools.

Note: Automated patching tools allow an administrator to update hundreds or even thousands of systems from a single console. Deployment is fairly simple when there are homogeneous computing platforms, with standardized desktop systems and similarly config-

ured servers. Multi-platform environments, nonstandard desktop systems, legacy computers, and computers with unusual configurations may also be integrated.

- i. **Configure Automatic Update of Applications Whenever Possible and Appropriate:** Many newer applications provide a feature that checks the vendor's web site for updates. This feature can be very useful in minimizing the level of effort required to identify, distribute, and install patches. However, some organizations may not wish to implement this feature because it might interfere with their configuration management process. A recommended option would be a locally distributed automated update process, where the patches are made available from the organization's network. Applications can then be updated from the local network instead of from the Internet.
- j. **Verify Vulnerability Remediation Through Network and Host Vulnerability Scanning:** Verify that vulnerabilities have been successfully remediated.
- k. **Vulnerability Remediation Training:** Train administrators on how to apply vulnerability remediations.

Note: Refer to IRM 10.8.50 for additional guidance.

Note: NIST SP 800-40 currently has four versions. The original SP 800-40, *Procedures for Handling Security Patches* (2002), provided basic information on patching procedures and sources of patch and vulnerability information. SP 800-40 Version 2.0, *Creating a Patch and Vulnerability Management Program* (2005), built on the original by adding content on processes, metrics, and common issues. Although SP 800-40 and SP 800-40 Version 2.0 are primarily of interest from a historical perspective, they address many of the same topics that organizations are still struggling with today. The third version, SP 800-40, Revision 3, *Guide to Enterprise Patch Management Technologies* (2013), was written under the assumption that readers already understood the basics of patch management and that what they most needed help with was implementing, configuring, securing, and using enterprise patch management technologies. The latest SP 800-40 version is based on the assumption that, in the overall scope of enterprise patch management, organizations would benefit more from rethinking their patch management planning than their patch management technology.

This Page Intentionally Left Blank

Exhibit 10.8.2-1 (04-29-2025)**Roles That Require Specialized Training**

To help ensure that the appropriate number of training hours is addressed, the list includes the minimum number of security-relevant specialized training hours required per role. Individuals who serve in multiple roles are required to complete the highest of the required hours for each of the roles in which the individual serves. For example, if an individual serves in three roles with hourly requirements of 4, 4, and 8 hours respectively, the individual will have to complete, at a minimum, 8 hours of specialized training.

Note: The roles and specialized training hours listed come from TD P 85-01 Appendix H and NIST SP 800-181 Rev. 1, **Workforce Framework for Cybersecurity (NICE Framework)**.

Roles	Minimum Required Specialized Training Hours
Chief Information Officer (CIO) (National Initiative for Cybersecurity Education (NICE)) Framework role = Executive Cyber Leadership)	4
Deputy Chief Information Officer (DCIO) (NICE Framework role = Executive Cyber Leadership)	4
Senior Agency Information Security Officer (SAISO)/Chief Information Security Officer (CISO) (NICE Framework role = Executive Cyber Leadership)	8
Authorizing Official (AO) (NICE Framework role = Authorizing Official/Designating Representative)	4
System Owner (NICE Framework role = Knowledge Manager)	4
Information Owner (NICE Framework role = Knowledge Manager)	4
System Security Officer (SSO) (NICE Framework role = Information Systems Security Manager)	8
Security Control Assessor	4
System Security Manager (SSM)- Oversees the cybersecurity program of an information system(s). The SSM often works closely with the SSO.	8
Cybersecurity Policy and Guidance Personnel - Individuals responsible for developing and/ or maintaining cybersecurity policy. (NICE Framework role = Cyber Policy and Strategy Planner)	8
Incident Analyst/Handler/Responder/Investigator Individuals responsible for providing security operations center services to part or all of an organization. An individual with this role may or may not be a member of an incident response team (bureau CSIRC) (NICE Framework role = Cyber Defense Incident Responder)	8
Contracting Officer's Representative for IT Contracts - Individuals IT (NICE Framework role = Investment/Portfolio Manager)	4
Network Administrator - Individuals with the responsibility of oversight and management of a network, including implementation of security requirements. (NICE Framework role name = Network Operations Specialist)	8

Exhibit 10.8.2-1 (Cont. 1) (04-29-2025)
Roles That Require Specialized Training

System Administrator - Individuals with the responsibility of oversight and management of a system, including implementation of security requirements.	8
Database Administrator - Individuals with the responsibility of oversight and management of a database, including implementation of security requirements.	8
System Programmer/Developer (NICE Framework role = Information Systems Security Developer)	4
Quality Assurance Personnel - Individuals responsible for ensuring the quality of an information system(s) and/ or its data.	4
Change Management Personnel - Individuals with change management (patching, configuration changes, functionality changes, etc.,) responsibilities.	4
Help Desk/IT Services Personnel - Individuals part of the Help Desk or IT Services staff. (NICE Framework role name = Technical Support Specialist)	4

Exhibit 10.8.2-2 (04-29-2025)**Terms and Acronyms****A**

Access Control – The process of granting or denying specific requests: 1) For obtaining and using information and related information processing services. 2) To enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).

Accountability – The security objective 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.

ACIO – Associate CIO

ACIOCS – Associate CIO for Cybersecurity

AO – Authorizing Official

AODR – Authorizing Official Designated Representative

Asset – A major application, GSS, high impact program, physical plant, mission critical system, or a logically related group of systems.

ATO – Authorization to Operate

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

Authentication – Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

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

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

B

BEARS – Business Entitlement Access Request System

BPA – Blanket Purchase Agreement

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 personally identifiable information or (2) a person accesses or potentially accesses personally identifiable information for an unauthorized purpose (i.e., a purpose unrelated to their official duties/functions).
INFORMATIONAL: A breach is a type of incident.

BSP – Business System Planner

C

CAO – Chief Acquisition Officer

CAS – Computer Audit Specialist

Exhibit 10.8.2-2 (Cont. 1) (04-29-2025)**Terms and Acronyms**

CCB – Configuration Control Board

CDO – Chief Data Officer

Certificate – A digital representation of information which at least: 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.

CFO – Chief Financial Officer

CIO – Chief Information Officer

CIP – Critical Infrastructure Protection

CISA – Cybersecurity and Infrastructure Security Agency

CISO – Chief Information Security Officer

CM – Configuration Management

CNSI – Classified National Security Information

CNSS – Committee on National Security Systems

Confidentiality – Preserving authorized restrictions on access and disclosure, (including means for protecting personal privacy and proprietary information) from unauthorized individuals, entities, or processes.

Contingency Plan – A plan that is maintained for disaster response, backup operations, and post-disaster recovery to ensure the availability of critical resources and to facilitate the continuity of operations in an emergency situation.

Controlled Unclassified Information (CUI) – Information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information (see paragraph (e) of this section) or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify. Note: The CUI categories and subcategories are listed in the *CUI Registry*.

COR – Contracting Officers Representative

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

CPO – Chief Procurement Officer

CSIRC – Computer Security Incident Response Center

Cyber Event – Any observance occurrence in a network or system that may indicate a cyber incident has occurred.

Exhibit 10.8.2-2 (Cont. 2) (04-29-2025)**Terms and Acronyms****D**

DASPTR – Deputy Assistant Secretary for Privacy, Transparency, and Records

DBA – Database Administrator

DBMS – Database Management System

DHS – Department of Homeland Security

Demilitarized Zone (DMZ) – A host or network segment inserted as a “neutral zone” between an organization’s private network and the Internet.

DR – Disaster Recovery

E

EFO – Enterprise Field Operations

EO – Executive Order

Encryption – The conversion of data into a form, called a ciphertext, which cannot be easily understood by unauthorized people, for the purposes of security or privacy.

Ensure – To make certain that something is done. In some instances, the individual/role whose responsibility is to ensure something is accomplished does not mean they perform the task but rather they are responsible for making sure the task is performed.

F

FCR – Firewall Change Request

Federal Information Security Modernization Act of 2014 (FISMA) – Directs federal agencies to develop, document, and implement agency- wide programs to provide security for the information and systems that support the agency’s operations and assets. This includes the security authorization and accreditation (SA&A) of IT systems that support digital authentication.

FIPS – Federal Information Processing Standard

G

GFIRST – Government Forum of Incident Response Teams

GSA – General Service Administration

GSS – General Support System

H, I

Identification – The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.

IDRS – Integrated Data Retrieval System

IDS – Intrusion Detection System

Exhibit 10.8.2-2 (Cont. 3) (04-29-2025)**Terms and Acronyms**

Impact – The effect on organizational operations, organizational assets, individuals, other organizations, or the Nation (including the national security interests of the United States) of a loss of confidentiality, integrity, or availability of information or an information system.

Impact Level – 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 information system availability.

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

Incident Handling – The remediation or mitigation of violations of security policies and recommended practices.

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

Information System Security Officer (ISSO) – See System Security Officer (SSO).

Information Security Continuous Monitoring (ISCM) – Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Note: The terms “continuous” and “ongoing” in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information.

Information Security Continuous Monitoring (ISCM) Program – A program established to collect information in accordance with pre-established metrics, utilizing information readily available in part through implemented security controls.

Information Technology (IT) – Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related resources.

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

Integrity – Guarding against improper modification or destruction of information; includes ensuring information non-repudiation and authenticity.

Exhibit 10.8.2-2 (Cont. 4) (04-29-2025)**Terms and Acronyms**

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

IOC – Indicators of Compromise

IPS – Identity Protection Service

IR – Incident Response

IRB – Investment Review Board

IRB – Investment Review Board

IRP – Incident Response Plan

J, K–

Key Management – The activities involving the handling of cryptographic keys and other related key information during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.

L

LB&I – Large Business and International

Least Privilege – A security principle that a system should restrict the access privileges of users (or processes acting on behalf of users) to the minimum necessary to accomplish assigned tasks.

M

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 they hold, however, require special management oversight and shall be treated as major. Adequate security for other applications shall be provided by security of the systems in which they operate.

Major Incident – A major incident is EITHER: [Treasury: IRP]

I. Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. Agencies should determine the level of impact of the incident by using the existing incident management process established in NIST SP 800-61, *Computer Security Incident Handling Guide*,

OR,

II. A breach that involves PII that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people. Or an unauthorized modification or unauthorized deletion of unauthorized exfiltration of or unauthorized access to the PII of 100,000 or more people constitutes a “major incident.”

OR

Exhibit 10.8.2-2 (Cont. 5) (04-29-2025)**Terms and Acronyms**

III. Any incident resulting from Advanced Persistent Threat (APT) actors, with attribution from a trusted commercial or external government intelligence source.

MD5 – A widely used cryptographic hash function producing a 16-byte hash value, typically expressed in text format as a 32-digit hexadecimal number. MD5 is commonly used to verify data integrity.

Memorandum of Agreement (MOA) – Used to document agreements and execute or deliver support with or without reimbursement between any two or more parties.

Memorandum of Understanding (MOU) – Used to document a mutual understanding between any two or more parties that do not contain an expectation of payment, and under which the parties do not rely on each other to execute or deliver on any responsibilities.

N

NA – Network Administrators

NICE – National Initiative for Cybersecurity Education

NIST – National Institute of Standards and Technology

NOM – Network Operations Management

Non-repudiation – Protection against an individual who falsely denies having performed a certain action and provides the capability to determine whether an individual took a certain action, such as creating information, sending a message, approving information, or receiving a message.

Notable Cyber Event – Any deviation from the norm or observable occurrence in a network or system that could have led to a cyber incident but was otherwise mitigated and the source or threat vector poses an ongoing risk to the Department.

O

OMB – Office of Management and Budget

P

PGLD – Privacy, Governmental Liaison and Disclosure

PIIRMG – Personally Identifiable Information Risk Management Group

Personally Identifiable Information (PII) – Any information about an individual maintained by an agency, including:

1. 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, such as name, social security number, date and place of birth, mother's maiden name, or biometric records.
 - a. 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.
 - b. 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.
2. Information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.
 - a. Linked information is information about or related to an individual that is logically associated with

Exhibit 10.8.2-2 (Cont. 6) (04-29-2025)**Terms and Acronyms**

other information about the individual.

b. 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.

3. 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.

Plan of Action and Milestones (POA&M) – A tool that identifies tasks that need 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.

POC – Point of Contact

Privacy Officer – The senior agency official for privacy is the senior official or executive with agency-wide responsibility and accountability for ensuring compliance with applicable privacy requirements and managing privacy risk.

Private Key – A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.

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 IT 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.

Public Key – A mathematical key that has public availability and that applications use to encrypt data or to verify signatures created with its corresponding private key.

PVG – Patch and Vulnerability Group

Q, R

RACF – Resource Access Control Facility

RBD – Risk-Based Decision

Remediation – Actions taken to correct known deficiencies and weaknesses once a vulnerability has been identified. The act of mitigating a vulnerability or a threat.

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 section, 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 is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Risk Assessment – The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the

Exhibit 10.8.2-2 (Cont. 7) (04-29-2025)**Terms and Acronyms**

Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

RMF – Risk Management Framework

S

SA – System Administrator

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

SAISO – Senior Agency Information Security Officer

SAMC – Situational Awareness Management Center

SCA – Security Control Assessment

Scanning – Sending packets or requests to another system to gain information to be used in a subsequent attack.

SecSpec – Security Specialist

Security Assessment and Authorization (SA&A) – A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the requirements for the system.

Security Controls – The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the CIA of the system and its information.

Security Requirements – Requirements levied on an information system that are derived from laws, EOs, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

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 shall be conducted in conjunction with, or prior to the self-assessment. A self-assessment does not eliminate the need for a risk assessment.

Sensitive But Unclassified (SBU) Information – Originated with the Computer Security Act of 1987. It is defined as “any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (USC) (the Privacy Act) but which has not 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.”

Sensitive Information – See controlled unclassified information (CUI).

Significant Cyber Incident – A cyber incident that is (or group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people.

Exhibit 10.8.2-2 (Cont. 8) (04-29-2025)**Terms and Acronyms**

Note, all major incidents are also deemed significant cyber incidents. However, only when a breach of PII that constitutes a “major incident” is the result of a cyber incident will it meet the definition of a “significant cyber incident” and trigger the coordination mechanisms outlined in NSPD-7.

SOP – Standard Operating Procedure

SP – Special Publication

SPMO – Security Program Management Officer

SRM – Security Risk Management

SSE – System Security Engineer

SSM -- System Security Manager

SSO – System Security Officer

Suspected Incident – An occurrence or alert that is under investigation is a potential incident but has yet to be confirmed.

Suspected Breach – An occurrence or alert that is under investigation as a potential breach but has yet to be confirmed.

System – Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions. Note: Systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

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

T

TCSIRC – Treasury Computer Security Incident Response Center

TD P – Treasury Directive Publication

Threat – Any circumstance or event with the potential to adversely impact agency operations (including mission, functions, image, or reputation), agency assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

TIGTA – Treasury Inspector General for Tax Administration

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.

TS-SCI – Top Secret Sensitive Compartmented Information

TSOC – Treasury Shared Services Security Operations Center

Exhibit 10.8.2-2 (Cont. 9) (04-29-2025)**Terms and Acronyms****U, V**

UA – User Administrator

UNS – User and Network Services

Vulnerability – A known weakness in a system, system security procedures, internal controls, or implementation by which an actor or event may intentionally exploit or accidentally trigger the weakness to access, modify, or disrupt normal operations of a system-resulting in a security incident or a violation of the system’s security policy.

Vulnerability Assessment – Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Exhibit 10.8.2-3 (05-01-2023)**Related Resources****Department of the Treasury Publications**

- TD P 85-01: TD P 85-01 Version 3.1.3, “*Treasury Information Technology Security Programs*,” issued February 28, 2022.
- TD 85-02: TD 85-02, “*Treasury Software Piracy Policy*,” issued March 23, 2016.
- TD 87-04: TD 87-04, “*Personal Use of Government Information Technology Resources*,” issued January 27, 2012.
- ISCM: Department of the Treasury, Version 1.0, “*Treasury Information Security Continuous Monitoring (ISCM) Framework*,” issued February 2, 2015.
- IRP: Department of the Treasury, Version 6.0, “*Departmental Incident Response Plan (IRP)*,” issued October 28, 2024.

IRS Publications

- IRM 1.1.32, *Organization and Staffing, Office of the Chief Procurement Officer*
- IRM 1.4.1, *Resource Guide for Managers, Management Roles and Responsibilities*
- IRM 10.2.14, *Physical Security Program, Methods of Providing Protection*
- IRM 10.5.1, *Privacy and Information Protection, Privacy Policy*
- IRM 10.8.1, *Information Technology (IT) Security, Security Policy*
- IRM 10.8.5, *Information Technology (IT) Security, Domain Name System (DNS) Security Policy*
- IRM 10.8.6, *Information Technology (IT) Security, Application Security and Development*
- IRM 10.8.11, *Information Technology (IT) Security, Application Security Policy*
- IRM 10.8.12, *Information Technology (IT) Security, Container Platform 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*
- IRM 10.8.21, *Information Technology (IT) Security, Database Security Policy*
- IRM 10.8.22, *Information Technology (IT) Security, Web Server Security Policy*
- IRM 10.8.23, *Information Technology (IT) Security, Application 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 10.8.27, *Information Technology (IT) Security, Personal Use Of Government Furnished Information Technology and Resources*
- IRM 10.8.33, *Information Technology (IT) Security, Mainframe System Security Policy*
- IRM 10.8.34, *Information Technology (IT) Security, IDRS Security Controls*
- IRM 10.8.50, *Information Technology (IT) Security, Service-wide 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 10.8.55, *Information Technology (IT) Security, Network Security Policy*
- IRM 10.8.60, *Information Technology (IT) Security, (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance*
- IRM 10.8.62, *Information Technology (IT) Security, Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Process*
- IRM 10.8.63, *Information Technology (IT) Security, Central Log Server Security Policy*
- IRM 10.9.1, *Classified National Security Information, (CNSI)*

Note: The IRS’ Office of Service-wide Policy, Directives and Electronic Research (SPDER), in partnership with LEXIS-NEXIS have made all IRMs available to all IRS employees. IRS IRMs are available on the *IMD IRM Numerical Index* site.

Exhibit 10.8.2-3 (Cont. 1) (05-01-2023)**Related Resources****National Institute of Standards and Technology (NIST) Publications**

- FIPS 199: Federal Information Processing Standard Publication 199, “*Standards for Security Categorization of Federal Information and Information*,” issued February 2004.
- SP 800-12: NIST Special Publication 800-12 Revision 1, “*An Introduction to Information Security*,” issued June 22, 2017.
- SP 800-18: NIST Special Publication 800-18 Revision 1, “*Guide for Developing Security Plans for Federal Information Systems*,” issued February 24, 2006.
- SP 800-34: NIST Special Publication 800-34 Revision 1, “*Contingency Planning Guide for Federal Information Systems*,” issued November 11, 2010.
- SP 800-37: NIST Special Publication 800-37 Revision 2, “*Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*,” issued December 20, 2018.
- SP 800-39: NIST Special Publication 800-39, “*Managing Information Security Risk: Organization, Mission, and Information System View*,” issued March 1, 2011.
- SP 800-40r2: NIST Special Publication 800-40 Revision 2, “*Creating a Patch and Vulnerability Management Program*,” issued November 16, 2005.
- SP 800-40r3: NIST Special Publication 800-40 Revision 3, “*Guide to Enterprise Patch Management Technologies*,” issued July 22, 2013.
- SP 800-40r4: NIST Special Publication 800-40 Revision 4, “*Guide to Enterprise Patch Management Technologies: Preventive Maintenance for Technology*,” issued July 22, 2013.
- SP 800-53: NIST Special Publication 800-53 Revision 5.1.1, “*Security and Privacy Controls for Federal Information Systems and Organizations*,” issued November 7, 2023.
- SP 800-60r1vI: NIST Special Publication 800-60 Revision 1 Volume I, “*Guide for Mapping Types of Information and Information Systems to Security Categories*,” issued August 1, 2008.
- SP 800-60r1vII: NIST Special Publication 800-60 Revision 1 Volume II, “*Appendices for Mapping Types of Information and Information Systems to Security Categories*,” issued August 1, 2008.
- SP 800-100: NIST Special Publication 800-100, “*Information Security Handbook: A Guide for Managers*,” issued March 7, 2007.
- SP 800-137: NIST Special Publication 800-137, “*Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*,” issued September 30, 2011.
- SP 800-160v1r1: NIST Special Publication 800-160 Volume 1 Revision 1, “*Engineering Trustworthy Secure Systems*,” issued November 16, 2022.
- SP 800-160v2r1: NIST Special Publication 800-160 Volume 2 Revision 1, “*Developing Cyber-Resilient Systems: A Systems Security Engineering Approach*,” issued December 9, 2021.
- SP 800-181: NIST Special Publication 800-181 Revision 1, “*Workforce Framework for Cybersecurity (NICE Framework)*,” issued November 16, 2020.

Note: NIST publications are available on the *NIST publications* site.

Other References

- CNSSI 4009, “*Committee on National Security Systems (CNSSI) Glossary*,” issued March 2, 2022.
- Federal: FAR: Title 48, “*Federal Acquisition Regulation (FAR) System Chapter 1*,” issued September 30, 2024.
- EO: 13833: Executive Order 13833, “*Enhancing the Effectiveness of Agency Chief Information Officers*,” issued May 15, 2018.
- EO: 13103: Executive Order 13103, “*Computer Software Piracy*,” issued September 30, 1988.
- OMB Memorandum for Chief Acquisition Officers - Revisions to the Federal Acquisition Certification for Contracting Officer’s Representatives (FAC-COR), issued September 6, 2011
- OMB: M-16-14: OMB Memorandum 16-14, “*Category Management Policy 16-2: Providing Comprehensive Identity Protection Services, Identity Monitoring, and Data Breach Response*,” issued July 1, 2016.

Exhibit 10.8.2-3 (Cont. 2) (05-01-2023)**Related Resources**

- OMB: M-20-04: OMB Memorandum 20-04, “Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements,” issued November 19, 2019.
- OMB: M-21-31: OMB Memorandum 21-31, “Improving the Federal Governments Investigative and Remediation Capabilities Related to Cybersecurity Incidents,” issued August 27, 2021.
- OMB: A-130: OMB Circular No. A-130, “Management Information as a Strategic Resource,” issued July 27, 2016.
- Federal: Privacy Act: Public Law 93-579 (S. 3418), “Privacy Act of 1974,” issued December 31, 1974.
- Federal: Taxpayer Browsing Protection Act: Public Law 105-35, “Taxpayer Browsing Protection Act of 1997,” issued August 5, 1997.
- Federal: Chief Financial Officers Act: Public Law 101-576, “Chief Financial Officers Act of 1990,” issued November 15, 1990.
- Federal: FISMA: Public Law 113-283 (H.R. 2521), “Federal Information Security Modernization Act (FISMA) of 2014,” issued December 18, 2014.
- Federal: Consolidated Appropriations Act, Section: Public Law 114-113 (H.R. 2029), “Consolidated Appropriations Act, 2016,” issued December 18, 2015.
- Federal: Foundations for Evidence-Based Policymaking Act: Public Law 115-435 (H.R. 4174), “Foundations for Evidence-Based Policymaking Act of 2018” issued January 14, 2019.
- Federal: Taxpayer First Act: Public Law 116-25 (H.R. 3151), “Taxpayer First Act,” issued July 1, 2019.
- U.S. Code Title 5, “Government Organization and Employees”.
- U.S. Code Title 31, “Money and Finance”.
- U.S. Code Title 44, Chapter 35, “Public Printing and Documents”.

Note: Executive Orders and OMB Memoranda are available on *The White House Information and Guidance* web site.

Note: Public Laws are available on the *Congress Statutes at Large and Public Laws* web site.

Note: United States Codes are available on the *U.S. House of Representatives United States Code* web site.

