



# MANUAL TRANSMITTAL

Department of the Treasury  
Internal Revenue Service

10.8.2

NOVEMBER 7, 2023

## EFFECTIVE DATE

(11-07-2023)

## PURPOSE

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

## MATERIAL CHANGES

- (1) IRM updated to align with IRM 1.11.2 , **Internal Management Documents System, Internal Revenue Manual (IRM) Process** Internal Controls.
- (2) The following sections were added: 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, and 10.8.2.1.7 Related Resources.
- (3) 10.8.2.1.1.1 (1) moved to 10.8.2.1.5 Program Controls.
- (4) 10.8.2.1.1.1 (2) moved to 10.8.2.1.3 Roles and Responsibilities.
- (5) 10.8.2.1.1.1 (3) moved to 10.8.2.1.3 Roles and Responsibilities.
- (6) 10.8.2.1.1.1 (4) moved to 10.8.2.1.5 Program Controls.
- (7) 10.8.2.1.1.2 (1) moved to 10.8.2.2 IT Security Roles and Responsibilities.
- (8) Section 10.8.2.1.8 Risk Acceptance and Risk-Based Decisions moved renumbered 10.8.2.2.
- (9) Section 10.8.2.2 renamed IT Security Roles and Responsibilities.
- (10) Exhibit 10.8.2-4 renamed Related Resources.
- (11) Interim Guidance Memorandum IT-10-0223-0002, Interim Guidance (IG) - Senior Agency Information Security Officer (SAISO)/Chief Information Security Officer (CISO) and Authorizing Official (AO) Responsibilities dated June 1, 2023 incorporated into the IRM. 10.8.2.3.1.3 Senior Agency Information Security Officer (SAISO)/Chief Information Security Officer (CISO) and 10.8.2.3.1.7 Authorizing Official (AO) sections updated.

## EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 10.8.2, dated September 12, 2022, and all prior versions of IRM 10.8.2. This IRM incorporates Interim Guidance Memorandum IT-10-0223-0002, Interim Guidance (IG) - Senior Agency Information Security Officer (SAISO)/Chief Information Security Officer (CISO) and Authorizing Official (AO) Responsibilities dated June 1, 2023. This IRM supplements IRM 10.8.1, *Information Technology (IT) Security Policy and Guidance*.

**AUDIENCE**

This IRM applies to all IRS employees, contractors and vendors who are responsible for ensuring adequate security is provided for IRS information and information systems.

Kaschit Pandya  
Acting, 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
- 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 Senior Agency Information Security Officer (SAISO)/Chief Information Security Officer (CISO)
      - 10.8.2.3.1.3.1 Security Control Assessor
      - 10.8.2.3.1.3.2 Risk Executive (Function)
      - 10.8.2.3.1.3.3 Common Control Provider
    - 10.8.2.3.1.4 Senior Management/Executives
    - 10.8.2.3.1.5 Information System Owner/Business and Functional Unit Owner
      - 10.8.2.3.1.5.1 Business System Planner (BSP)
        - 10.8.2.3.1.5.1.1 Security Program Management Officer (SPMO)
    - 10.8.2.3.1.6 Information Owner
    - 10.8.2.3.1.7 Authorizing Official (AO)
      - 10.8.2.3.1.7.1 Authorizing Official Designated Representative
    - 10.8.2.3.1.8 Information System Security Officer (ISSO)
    - 10.8.2.3.1.9 Manager
    - 10.8.2.3.1.10 Contracting Officer
      - 10.8.2.3.1.10.1 Contracting Officers Representatives (COR)
    - 10.8.2.3.1.11 Enterprise Architect
    - 10.8.2.3.1.12 Information System Security Engineer
    - 10.8.2.3.1.13 Chief Financial Officer (CFO)
    - 10.8.2.3.1.14 Privacy Officer
      - 10.8.2.3.1.14.1 IRS Privacy Offices
    - 10.8.2.3.1.15 Physical Security Officer
    - 10.8.2.3.1.16 Personnel Security Officer

- 
- 10.8.2.3.1.17 Employee
  - 10.8.2.3.1.18 Contractor
  - 10.8.2.3.1.19 Database Administrator (DBA)
  - 10.8.2.3.1.20 Encryption Recovery Agent
  - 10.8.2.3.1.21 Network Administrator
  - 10.8.2.3.1.22 Program Developer/Programmer
  - 10.8.2.3.1.23 Web Developer
  - 10.8.2.3.1.24 Resource Access Control Facility (RACF) Specialist
  - 10.8.2.3.1.25 Security Specialist (SecSpec)
  - 10.8.2.3.1.26 System Administrator (SA)
  - 10.8.2.3.1.27 Systems Operations Staff
  - 10.8.2.3.1.28 Telecommunications Specialist
  - 10.8.2.3.1.29 User Administrator (UA)
  - 10.8.2.3.1.30 Integrated Data Retrieval System (IDRS) Security Analyst
  - 10.8.2.3.1.31 Integrated Data Retrieval System (IDRS) Security Account Administrator
  - 10.8.2.3.1.32 Computer Audit Specialist
  - 10.8.2.3.1.33 Functional Workstation Specialist
  - 10.8.2.3.1.34 Management/Program Analyst
  - 10.8.2.3.1.35 System Designer
  - 10.8.2.3.1.36 Technical Support Staff (Desktop)
  - 10.8.2.3.1.37 Security Staff (Physical Security)
  - 10.8.2.3.1.38 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 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 Incident, Breach, and Event Definitions
- 10.8.2-3 Terms and Acronyms
- 10.8.2-4 Related Resources

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

- (1) **Overview:** This Internal Revenue Manual (IRM) lays the foundation for roles and responsibilities within the Internal Revenue Service (IRS).
- (2) **Purpose of the Program:** Develop and publish policies to protect the IRS against potential IT threats and vulnerabilities and 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, Threat Response and Remediation, an organization within Cybersecurity.
- (6) **Program Goals:** To protect the confidentiality, integrity, and availability of data processed on IRS systems.

10.8.2.1.1  
(09-12-2022)  
**Background**

- (1) Department of Treasury Directive Publication (TD P) 85-01 and federal regulations require that senior management/executive officials establish an IT security program, which includes the identification of IT security roles and responsibilities.
  - a. This IRM establishes the roles and responsibilities for the Internal Revenue Service (IRS) organizations and the employees relevant to sensitive information and systems.
- (2) IRM 10.8.2 has been aligned to the roles and responsibilities described in NIST Special Publication (SP) 800-100, *Information Security Handbook: A Guide for Managers* and SP 800-37 Rev 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- (3) IRM 10.8.2 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Information Technology Cybersecurity.

10.8.2.1.2  
(09-12-2022)  
**Authority**

- (1) All IRS information systems and applications shall be compliant 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) TD P 85-01 and federal regulations require that 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  
(11-07-2023)  
**Roles and Responsibilities**

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

- a. Refer to IRM 10.5.1, *Privacy and Information Protection, Privacy Policy*, for a detailed description of Privacy Roles and Responsibilities.
- (3) 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.X series, additional applicable policy suites of IRMs, applicable business unit Guidelines, Standards and Procedures (GSP), and Standard Operating Procedures (SOP) shall be carefully reviewed for an individual to comprehensively understand their role and specific responsibilities in their environmental context. IRMs in the 10.8.X 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 shall be implicitly followed along with those stated in this IRM.

10.8.2.1.4  
(11-07-2023)  
**Program Management  
and Review**

- (1) The IRS Cybersecurity Program establishes a framework of security controls to ensure the inclusion of security in the daily operations and management of IRS IT resources. This framework of security controls is provided through the issuance of security policies via the IRM 10.8.x series and the development of technology specific security requirement checklists. Stakeholders are notified when revisions to the security policies and security requirement checklists are made.

10.8.2.1.5  
(11-07-2023)  
**Program Controls**

- (1) Each IRM in the 10.8.x series is assigned an author who reviews their IRM annually to ensure accuracy. The IRM authors continuously monitor federal guidance (e.g., OMB, CISA, NIST, DISA) for potential revisions to security policies and security requirement checklists. Revisions to security policies and checklists are reviewed by the security policy team, in collaboration with applicable stakeholders, for potential impact to the IRS operational environment.
- (2) Security Policy provides a report identifying security policies and security requirement checklists that have recently been revised or are in the process of being revised.
- (3) This IRM applies to all IRS information and information systems, which include IRS production, development, test, and contractor systems. For information systems that store, process, or transmit classified information, refer to IRM 10.9.1, *Classified National Security Information (NSI)*, for additional guidance for protecting classified information.
- (4) In the event there is a discrepancy between this policy and IRM 10.8.1, IRM 10.8.1 has precedence, unless the security controls/requirements in this policy are more restrictive or otherwise noted.

10.8.2.1.6  
(11-07-2023)  
**Terms and Acronyms**

- (1) Refer to Exhibit 10.8.2-3 for a list of terms, acronyms, and definitions.

10.8.2.1.7  
(11-07-2023)  
**Related Resources**

- (1) Refer to Exhibit 10.8.2-4 for a list of related resources and references.

10.8.2.2  
(09-12-2022)  
**Risk Acceptance and Risk-Based Decisions**

- (1) Any exception to this policy requires that the Authorizing Official (AO) make a Risk-Based Decision.
- (2) Users shall submit RBD requests in accordance with Cybersecurity’s Security Risk Management (SRM) Risk Acceptance Process within the Risk Based Decision Standard Operating Procedures (SOP).

#  
#  
#

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

10.8.2.3  
(09-12-2022)  
**IT Security Roles and Responsibilities**

- (1) This IRM establishes the IT Security responsibilities for roles within the IRS.
  - a. In accordance with IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*, the IRS shall 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.

10.8.2.3.1  
(09-12-2022)  
**Key Governance and Related Roles & Responsibilities**

- (1) In accordance with NIST SP 800–100, 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.
- (2) This section provides 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  
(09-12-2022)  
**Agency Head**

- (1) FISMA requires the head of each federal agency to provide information security protections commensurate with the risk and magnitude of the harm that may result from unauthorized access, use, disclosure, disruption, modification, or destruction of its information and information systems. The protection should apply not only within the agency, but also within contractor or other organizations working on behalf of the agency.
  - a. 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 shall:
  - a. Designate a CIO;

- b. Ensure high priority is given to effective information security awareness, security awareness training, and role-based training for the workforce.
- (3) In accordance with TD P 85-01, the Agency Head shall:
- a. Ensure that a Cybersecurity Program is developed within their organizations in accordance with Treasury policy;
  - b. Ensure the IRS practices its Cybersecurity Program throughout the life cycle of each IRS system;
  - c. Ensure an IRS-wide report on the Cybersecurity Program and any internal annual compliance reviews is submitted annually to the Treasury Associate CIO for Cybersecurity (ACIOCS);
  - d. Ensure that a system inventory is maintained following Treasury FISMA inventory requirements;
  - e. Ensure IRS employees/contractors complete annual cybersecurity awareness training and specialized training (as required);
  - f. Ensure each information system is assigned an AO and that no information systems are operated in production environments without an assigned AO; and
  - g. Perform any additional responsibilities set forth in Federal guidance and policies, including applicable Committee on National Security Systems (CNSS) Policies and Directives.

**Note:** For information systems that store, process, or transmit classified information refer to IRM 10.9.1 for additional guidance for protecting classified information.

- (4) In accordance with FISMA, the Agency Head shall be responsible for:
- 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. Ensuring information security management processes are integrated with agency strategic and operational planning processes;
  - d. Ensuring that the agency has trained personnel sufficient to assist the agency in complying with the requirements of FISMA Section 3544 §, this policy and related policies, procedures, standards, and guidelines;
  - e. Establishing the organizational commitment and the actions required to effectively manage security and privacy risk and protect the mission and business functions being carried out by the organization;
  - f. Establishing security and privacy accountability and providing active support and oversight of monitoring and improvement for the security and privacy programs; and
  - g. Ensuring policies are disseminated to all employees.
- (5) In accordance with FISMA, the Agency Head shall:







- a. Designate a SAISO/CISO, who shall carry 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. Ensure information security and privacy considerations are integrated into programming, planning and budgeting cycles, enterprise architectures and acquisition/system development life cycles;
  - d. Ensure information systems are covered by an approved security plan and are authorized to operate;
  - e. Ensure security authorizations are accomplished in an efficient, cost-effective and timely manner;
  - f. Ensure centralized capability for reporting of all security-related activities;
  - g. Determine 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;
  - h. For information systems that process PII, coordinate any determination about the allocation of resources dedicated to the protection of those systems with the Chief, Privacy Officer;
  - i. Manage the identification, development, implementation, and assessment of common security controls;
  - j. Ensure compliance with applicable information security requirements;
  - k. Ensure that personnel with significant responsibilities for system and program security plans and assessments are trained;
  - l. Assist senior management/executive officials with their responsibilities for system and program security plans and assessments;
  - m. Report annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions;
  - n. Encourage the maximum reuse and sharing of security-related information including: 1) threat and vulnerability assessments; 2) risk assessments; 3) results from common security control assessments; and 4) any other general information that may be of assistance to information system owners and their supporting security staffs;
  - o. Determine the appropriate allocation of resources dedicated to the protection of the agency's information systems based on organizational priorities; and
  - p. In certain instances, operate as the AO for agency-wide General Support Systems (GSS) or as co-AO with other senior management/executive officials for selected agency systems.
- (8) In accordance with the Department of Treasury's Software Piracy Policy, the CIO shall:
- 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 enterprise list of Treasury Department authorized and supported software. The list shall indicate by Bureaus and Offices, terms of licenses, authorized number of users, and physical location of software;

- d. Perform spot audits. Periodic audit checks shall be done to ensure Bureaus and Offices are in compliance with software license agreements; and
  - e. Establish centralized software acquisition whenever possible.
- (9) In addition, the CIO shall:
- a. Provide leadership and high level direction in the management of projects and plans involving highly complex, mission critical information systems and business systems modernization projects in support of modernizing the nation's tax system;
  - b. Ensure the organization's core IT competencies are aligned to provide maximum value in support of agency business processes, and ensures overall strategies are established and engaged to support long-term enterprise-wide information needs and modernization projects;
  - c. Define objectives and make decisions which impact the cost, schedule, supportability and performance modernization projects;
  - d. Provide focus for technology management within the IRS by developing integrated enterprise-wide technology policies;
  - e. Establish and maintain strong relationships with stakeholders such as oversight groups, IRS business leaders and external stakeholders, etc., to facilitate the exchange of information in support of program goals and requirements;
  - f. Provide oversight and guidance to key contractors to ensure successful performance of contracts;
  - g. Provide executive leadership in IT strategic and operational planning to achieve business goals by fostering innovation, prioritizing complex IT initiatives and directing the evaluation, deployment and management of current and future IT systems across the organization;
  - h. Serve as the external spokesman for the IRS on technology matters to the Administration, Congress and external oversight bodies;
  - i. Influence strategic business decisions regarding the use of technology and assesses the impact of emerging technology to strategic business needs;
  - j. Drive the vision for all enterprise-wide IT activities including planning, budgeting, acquisition, allocation of computer services and communication services;
  - k. Develop and implement IT initiatives that will advance operational efficiencies, improve enterprise-wide decision making and communication, increase revenues, drive cost efficiencies and strengthen financial reporting and controls;
  - l. Develop and implement an IRS-wide time server, in accordance with IRM 10.8.1; and
  - m. Ensure IRS Information Technology organization notifies the CSIRC of suspicious activities and complies with CSIRC directions.
    - i. IRS Information Technology organization shall comply with their internal configuration management requirements.
    - ii. IRS Information Technology organization shall perform containment activities.
- (10) The CIO, as tasked by FISMA, shall administer training and oversee personnel with significant information security responsibilities. To accomplish this, the CIO shall work with the SAISO/CISO to:

- 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 specialized cybersecurity training is completed annually by the employees/contractors with significant cybersecurity responsibilities;
  - e. Ensure cybersecurity awareness training is provided annually to information system users in accordance with applicable guidance;
    - i. All users of information systems shall be sufficiently trained in their security responsibilities and other information security basics and literacy through awareness training.
  - f. 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
  - g. Ensure that effective tracking and reporting mechanisms are in place.
- (11) In accordance with NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, and Treasury's Information Security Continuous Monitoring (ISCM) Framework, the CIO shall perform the following Information Security Continuous Monitoring (ISCM) responsibilities:
- 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;
  - d. Maintain high-level communications and working group relationships among organizational entities;
  - e. Ensure ISCM implementation and associated activities are accomplished in a timely and cost-effective manner;
  - f. Ensure that there is centralized reporting of all security-related activities; and
  - g. Ensure the maximum reuse and sharing of security-related information, especially in the context of risk correlation across the organization.

10.8.2.3.1.3  
(05-01-2023)

**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 Information System Security Officers (ISSOs). (NIST SP 800-37)

**Note:** At the IRS, the Associate CIO (ACIO), IRS Information Technology Cybersecurity organization is the SAISO/CISO.

- (2) The SAISO/CISO shall coordinate with the Chief, Privacy Officer to ensure coordination between privacy and information security programs. (OMB A-130 Appendix I 3(b)(11))
- (3) In accordance with TD P 85-01, the SAISO/CISO shall:

- a. Serves as the central point of contact for the IRS's overall cybersecurity program;  
**Note:** The IRS SAISO/CISO typically advises on cybersecurity program matters to the IRS CIO.
- b. Be a Federal Employee;
- c. Develop and manage the IRS cybersecurity program in accordance with Treasury and IRS policies and standards;
- d. Monitor and evaluate the status of the IRS's cybersecurity posture;
- e. Prepare and distribute IRS policies, security standards, and additional guidance, as necessary, to implement and manage the IRS Cybersecurity Program;
- f. Ensure parameters are defined and documented for system security controls where parameters are required and are not defined by Federal or Treasury standards, policy, or compulsory guidance;
- g. Oversee the execution of the IRS's System Security Assessment and Authorization (SA&A) process by ensuring at a minimum:
  - i. All IRS information systems, including contractor systems, complete a security authorization process in accordance with Federal, Departmental, and IRS requirements.
  - ii. SA&A documents, include but not limited to system security plans, security assessment reports, and POA&Ms, are developed implemented, and reviewed in accordance with applicable Federal, Treasury, and IRS security standards to ensure security requirements are adequately addressed.
  - iii. Continuous monitoring, to include technical control testing, system security assessments, and updated risk analyses, are conducted in accordance with IRS and Treasury policies and applicable guidance.
  - iv. Results of periodic testing are reviewed as part of the continuous monitoring of system authorization activities.
  - v. IRS SA&As are conducted and maintained in accordance with Treasury and IRS defined policies and frequencies.
    - a. Ensure the re-accreditation/reauthorization and risk analyses are conducted every 3 years or when major changes occur for IT systems/application processing sensitive information. (IRS-defined)
    - b. Refer to IRM 10.8.1 for additional requirements.
- h. Ensure that cybersecurity requirements are fully addressed in IRS IT business cases and budget submissions;  
**Note:** This is to ensure that IT security requirements are addressed and adequately resourced.
- i. Establish and maintain a process to track, for all cybersecurity weaknesses reported under self-assessments, external reviews, continuous monitoring activities, and other internal or external assessments, IRS POA&Ms that include milestones, schedules, points of contact, allocation of resources, and status for implementation of any corrective actions;
- j. Ensure the IRS CIO is informed of overall security status and risk posture;
- k. Ensure that the security aspects and day-to-day security operations of the information system, including physical security, personnel security, incident handling, and security training and awareness, are managed, and that summary security metrics are reported to the Treasury CIO or Treasury Associate CIO for Cybersecurity (ACIOS) as requested;

- l. Develop and maintain CSIRC policy and procedures for reporting, investigating, and resolving all cybersecurity incidents involving IRS information systems;
- m. Validate that an ISSO is assigned for each IRS information system;
- n. Provide timely responses to ACIOCS and Treasury cybersecurity data calls as requested;
- o. Prepare and distribute IRS policies, security standards, and additional guidance, as necessary, to implement and manage the IRS cybersecurity program;
- p. Maintain an inventory of the IRS's information systems and relevant security information for those systems;
- q. Establish and monitor the IRS's information security continuous monitoring program, including ensuring that information systems are monitored and that issues identified are escalated for appropriate action;
- r. Develop methods and techniques to support situation awareness as to the security risk posture of systems and networks across the IRS;
- s. Support continuing IRS operations by ensuring that requirements are in place for information systems to recover from a contingency event by following information system contingency plans and procedures that:
  - i. Are developed, maintained, and tested/exercised in accordance with Federal, Departmental, and IRS standards.
  - ii. Are reviewed and approved by appropriate IRS and system authorities.
- t. Conduct and coordinate information security audits at IRS and contractor facilities. Review security clauses in contracts and statements of work;
- u. Ensure that information system and service contracts and related documents contain security clauses ensuring adequate protection of Treasury information and systems;
- v. Ensure IRS personnel, contractors, and others working on behalf of the IRS receive information security awareness training and that records are maintained to demonstrate individual completion of awareness training;
- w. Ensure IRS personnel, contractors, and others with significant security responsibilities receive role-based training in accordance with Treasury and IRS policies and that records are maintained to demonstrate completion of sufficient hours of role-based training each year;
- x. Complete mandatory annual specialized information security training; and
- y. Review, in consultation with the IRS CIO, any requested IRS-wide exceptions to policy, and sign approved exceptions.

**Note:** In the IRS exceptions are called RBDs.

- i. An approved and signed exception must be held by the IRS with a copy submitted to the Department CIO via the Department CISO.
- ii IRS-wide exceptions to Treasury requirements shall be managed differently than information system tailoring. Documentation of exception requests to Treasury requirements must include operation justification, risk acceptance, and risk mitigation measures.
- iii Such requests must be submitted to and approved by the IRS CIO, in consultation with the IRS SAISO/CISO.
- iv An approved exception must be signed by the individuals in these roles and held by the IRS, with a copy submitted to the Department CIO via the Department CISO.

- (4) In accordance with OMB M-20-04, the SAISO/CISO shall have TS-SCI access.



quirements throughout the life cycle of each agency information system to ensure compliance with applicable requirements;

- g. Facilitate development of subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems;
- h. Coordinate the development, review, and acceptance of system security plans with information system owners, ISSOs, and the AO;
- i. Coordinate the identification, implementation, and assessment of the common security controls;
- 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. Develop and review procedures for monitoring and reacting to system security alarms, warning messages, and reports, and implement said procedures;

**Note:** This duty may be delegated to ISSOs.

- m. Oversee a program of disaster recovery readiness and evaluation;
- n. 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;
- o. 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
- p. Assist senior management/executive officials concerning their responsibilities.

(7) In accordance with NIST, the SAISO/CISO shall:

- a. Ensure that IT system SA&A (i.e., Certification & Accreditation reports and risk analyses) are conducted by each AO;
- b. Ensure that security plans are reviewed and submitted to the AO for approval at least annually or upon significant changes to the system, whichever is sooner;
- c. Review IRS business cases and budget submissions to ensure that IT security requirements are addressed and adequately resourced;
- d. Conduct security audits, verifications and acceptance checks and maintain documentation on the results;
- e. Manage and Maintain agency POA&Ms for all IT security weaknesses, tracking milestones, and resource allocation of resources for remediation, and provide a quarterly status to Department of Treasury through the IRS CIO;
- f. Ensure the CIO is informed of technical risks and vulnerabilities, to include those accepted by AOs;
- g. Ensure that IRS security status and other relevant data is provided to the CIO for situational awareness and related purposes;
- h. Prepare and submit a written report for all technical security exceptions. The report shall outline the risks and vulnerabilities and/or advantages that could result from granting the exception or from implementing any alternative. Maintain a file of all approved IT facility security-related exceptions;

- i. Coordinate the implementation of logical access controls into operating systems, Relational Database Management Systems (RDBMS), remote terminals and IT applications;
  - j. Provide IT and facility technical and non-technical (e.g., physical and personnel security) certification support to any Information System Owner;
  - k. Ensure that re-accreditation/reauthorization and risk analyses are conducted at least every 3 years or when major changes occur for IT systems/application processing sensitive information;
  - l. Ensure that a Security Control Assessment (SCA) is performed for each non-national security system when conducting a SA&A (for policy pertaining to national security system Refer to IRM 10.9.1);
  - m. Ensure that contingency plans for IT systems processing sensitive information are developed, maintained and tested;
  - n. Develop each certification letter citing risks and mitigations along with Authority to Operate (ATO) or recommendation to the AO;
  - o. Be a voting member on the Configuration Control Board (CCB) for the IRS' IT architecture;
  - p. Review contract vehicles to ensure they address appropriate security measures; and
  - q. Define and implement performance metrics to evaluate the effectiveness of their IT security programs.
- (8) The SAISO/CISO shall maintain an inventory of major applications and GSSs.
- a. Refer to IRM 10.8.1 for additional requirements and guidance.
- (9) The ACIO Cybersecurity shall:
- a. Maintain and provide updates to IRM 10.8.1, in accordance with IRM 10.8.2 and other applicable IRS policies; and
  - b. Develop GSP documentation, consistent with the requirements of this IRM, to describe platform-specific files, permissions, and other configuration settings necessary to comply with IRM 10.8.1.
  - c. Refer to IRM 10.8.1 for additional requirements and guidance.
- (10) The ACIO Cybersecurity, in conjunction with IRM 10.8.27, *Information Technology (IT) Security, Internal Revenue Service Policy on Limited Personal Use of Government Information Technology Resources*, shall develop and disseminate policy appropriate to personal use of Government IT resources as necessary.
- (11) The SAISO/CISO has the responsibility for the organization's information security awareness and training program. In this role, the SAISO/CISO shall:
- a. Ensure that security awareness, security awareness training, and role-based training material developed or purchased is appropriate and timely for the intended audiences;
  - b. Ensure that security awareness, security awareness training, and role-based training material is effectively deployed to reach the intended audiences;
  - c. Ensure that employees, users, those receiving role-based training, and managers have an effective way to provide feedback on the security awareness, security awareness training, and role-based training material and its presentation;
  - d. Ensure that security awareness, security awareness training, and role-based training material is reviewed periodically and updated when necessary; and



#  
#  
#  
#  
#  
#

- (4) In accordance with NIST, the security control assessor shall:
- a. Provide corrective actions to reduce or eliminate vulnerabilities in the information system;
  - b. Be independent from the persons directly responsible for the development of the information system and the day-to-day operation of the system;
  - c. Be independent of those individuals responsible for correcting security deficiencies identified during the security certification; and
  - d. Assess the implemented controls using the assessment procedures specified in the security and privacy assessment plans.
- (5) Refer to the Senior Agency Information Security Officer (SAISO)/Chief Information Security Officer (CISO) section of this IRM for additional roles and responsibilities.

10.8.2.3.1.3.2  
(11-27-2019)  
**Risk Executive  
(Function)**

#  
#  
#  
#  
#

10.8.2.3.1.3.3  
(09-30-2021)  
**Common Control  
Provider**

- (1) In accordance with NIST SP 800-37, the IRS shall appoint a common control provider. The common control provider shall be an IRS official or group responsible for the planning, , implementation, assessment, authorization, and maintenance of common controls (i.e., security controls inherited by information systems).

**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) Common control providers shall be responsible for:
- a. Documenting common controls to be utilized in a System Security Plan (SSP);
  - b. Ensuring that required assessments of common controls are carried out by qualified assessors with an appropriate level of independence;
  - c. Documenting assessment findings in a security assessment report;
  - d. Producing a POA&M for all controls having weaknesses or deficiencies; and
  - e. Making available security plans, security assessment reports, and POA&Ms for common controls (or a summary of such information) to information system owners inheriting those controls after the information is reviewed and approved by the senior management/executive official or other with oversight responsibility for those controls.

- (3) In accordance with NIST SP 800-137, the Common Control Provider shall perform the following ISCM responsibilities:
- 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/ information system owners, and other senior leaders in accordance with organizational policy/procedures.

10.8.2.3.1.4  
(09-05-2012)

**Senior  
Management/Executives**

- (1) OMB Circular A-130, states executive agencies within the federal government shall:
- 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.
- (2) FISMA, OMB, Department of Treasury, and FISMA guidance specify that senior management/executive officials are subordinate to the Commissioner and shall be 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.
- (3) The AO for a GSS or application shall be a senior management/executive official.
- (4) Senior management/executive officials shall be responsible for balancing the mission and business priorities versus any security risks that might be applicable and formally authorizing the operation of an information system (this is known as security accreditation).





- m. Provide orderly, disciplined, and timely updates to the security plan, security assessment report, POA&M on an ongoing basis, supports the concept of a near real-time risk management and ongoing authorization;
  - n. Ensure all security weaknesses and deficiencies identified during the security control assessment are documented in the security assessment report to maintain an effective audit trail. Organizations develop specific plans of action and milestones based on the results of the security control assessment and in accordance with applicable laws, EOs, directives, policies, standards, guidance, or regulations;
  - o. Ensure a strategy is developed for the continuous monitoring of security control effectiveness and any proposed or actual changes to the information system and its environment of operation;
  - p. Ensure security controls that are modified, enhanced, or added during the continuous monitoring process are reassessed by the assessor to ensure that appropriate corrective actions are taken to eliminate weaknesses or deficiencies or to mitigate the identified risk;
  - q. Identify security control weaknesses or deficiencies (i.e., the direct or indirect effect the weaknesses or deficiencies may have on the overall security state of the information system and hence on the risk exposure of the organization);
  - r. Ensure security control assessments are conducted in parallel with the development and implementation phases of the system development life cycle facilitates the early identification of weaknesses and deficiencies and provides the most cost-effective method for initiating corrective actions;
  - s. Provide specific recommendations on how to correct weaknesses or deficiencies in the controls;
  - t. Ensure any weaknesses or deficiencies in the security controls noted during the assessment are corrected;
  - u. Report the security status of the information system (including the effectiveness of security controls employed within and inherited by the system) to the Authorizing Official and other appropriate organizational officials on an ongoing basis in accordance with the monitoring strategy;
  - v. Ensure system-level POA&Ms are established and corrective actions are implemented in accordance with the Treasury standard for POA&Ms;  
**Note:** This includes taking appropriate steps to update the risk assessment and to reduce or eliminate vulnerabilities after receiving the security assessment results from the Security Control Assessor.
  - w. Define how changes to the information system shall be monitored, how security impact analyses shall be conducted, and the security status reporting requirements including recipients of the status reports;
  - x. Develop a strategy for the continuous monitoring of security control effectiveness and any proposed/actual changes to the information systems and its environment of operation; and
  - y. 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.
- (5) Information System Owners are responsible for the information security of their Contractor Systems. In accordance with FISMA, Information System Owners shall:
- a. Conduct an annual FISMA Contractor Review of the contractor's facility and systems;

- b. Perform continuous monitoring and create and maintain a POA&M of their FISMA Contractor Systems in accordance with NIST SP 800-37 and 800-53 Rev 5, *Security and Privacy Controls for Federal Information Systems and Organizations* guidance; and
  - c. Provide funding to conduct the annual FISMA Contractor reviews.
- (6) For DR / Business Resumption (BR), the Information System Owner shall cooperate with the other business units and the area/site managers to develop, maintain, and validate effective, comprehensive plans. At a minimum, the Information System Owner shall coordinate with other appropriate business units and shall be responsible to:
- a. Fully describe and document the information system in Information System Contingency Plan (ISCP);
  - b. Acquire and transport replacement equipment required to restore operations;
  - c. Acquire space for processing operation to include occupation of an alternate processing facility when necessary;
  - d. Estimate supplies and office equipment needed to support a computer processing operation occupying an alternate processing facility when appropriate; and
  - e. Support expeditious acquisition and transportation of replacement equipment required to restore operations.
  - f. Refer to IRM 10.8.60, *Information Technology (IT) Security, IT Service Continuity Management (ITSCM)*, and IRM 10.8.62, *Information Technology (IT) Security, Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Process*, for additional information on IT Disaster Recovery roles & responsibilities.
- (7) For DR, the Information System Owner shall:
- a. Coordinate with other appropriate business units;
  - b. Determine recovery needs and time frames needed for business restoration through comprehensive Business Impact Analysis (BIA) evaluations;
  - c. Develop DR requirements during the development phase of all new systems and throughout any production system upgrades;
  - d. Provide the funding for the DR equipment/space/storage needed to meet the recovery goals (set by the business);
  - e. Fully describe and document the details of the information system in the ISCP that is required by FISMA for each major system;
  - f. Support the development of processing priorities for completion of work following emergencies that degrade computer processing capabilities;
  - g. Work jointly with IRS Information Technology Operations and SRM to ensure ISCPs and DR Plans for all applications and systems are tested annually;
  - h. Work jointly with IRS Information Technology Operations and SRM in the development and testing of DR plans to ensure availability of data from the recovered system and business continuity;
  - i. Work jointly in the testing of the DR plans to ensure availability of data from the recovered system; and
  - j. Work with SRM regarding enterprise priorities.
  - k. Refer to IRM 10.8.60, for additional information on IT Disaster Recovery.
- (8) For each IRS system within their area of responsibility, the Information System Owner shall comply with audit and accountability guidance in accordance with IRM 10.8.1.

- (9) The Information System Owner of the database shall:
- a. Ensure that Database Management System (DBMS) environments comply with the security change management requirements listed in IRM 10.8.1;
  - b. Ensure that changes to DBMSs are documented and tracked using the appropriate change management process;
  - c. Ensure that development servers are properly configured and managed in accordance with the requirements in IRM 10.8.21 *Information Technology (IT) Security, Database Security Policy*;
  - d. Work with Program Developer/Programmers to ensure proper configuration of application server software, on the operating system(s) are in accordance with IRM 10.8.21;
  - e. Advise the Security Specialist of any technical, operational, or security problems and recommended solutions; and
  - f. Ensure Database Administrators (DBAs) do not have unnecessary operating System Administrator privileges. DBAs shall have the least level of elevated operating system privileges required to perform DBA-related duties.
  - g. Refer to IRM 10.8.21 for additional requirements.
- (10) The Information System Owner shall:
- a. Assist Program Developer/Programmers to ensure proper configuration of application server software, on the operating system(s) are in accordance with IRM 10.8.6 *Information Technology (IT) Security, Application Security and Development*;
  - b. Advise the Security Specialist of any technical, operational, or security problems and recommended solutions for secure application development; and
  - c. Not have operating system Administrator privileges.
  - d. Refer to IRM 10.8.6, for additional requirements.
- (11) The Information System Owner shall be responsible for the following:
- a. Assist SAs and other stakeholders to ensure proper configuration of Linux/Unix based operating systems in accordance with IRM 10.8.15, *Information Technology (IT) Security, General Platform Operating System Security Policy*; and
  - b. Advise the Security Specialist of any technical, operational, or security problems and recommend solutions for the Linux/Unix environment.
  - c. Refer to IRM 10.8.15, for additional requirements.
- (12) Information System Owners shall be responsible for the following:
- a. Assist System Administrators (SA) and other stakeholders to ensure proper configuration of Windows based operating systems in accordance with IRM 10.8.15; and
  - b. Advise the Security Specialist of any technical, operational, or security problems and recommend solutions for the Windows environment.
  - c. Refer to IRM 10.8.15, for additional requirements.
- (13) The Information System Owner shall be responsible for the following:
- a. Ensure that Web servers and Web application servers are properly configured and managed in accordance with the requirements of associated IRM.

- b. Work with SAs and other stakeholders to ensure proper configuration of Web servers and web application server software on the operating system in accordance with associated IRM; and
  - c. Coordinate placement of information and scripts on the Web server and Web application servers with appropriate authorities.
  - d. Refer to IRM 10.8.22, *Information Technology (IT) Security Web Server Policy*, for additional requirements.
- (14) Information System Owners that maintain systems, networks, IRS applications, and Commercial-off-the-Shelf (COTS) shall:
- a. Develop implementation policies and procedures for managing security patches to the systems and applications for which they are responsible;
  - b. Review various sources for security-related patches specific to their systems and applications;
  - c. Notify CSIRC prior to the working on each set of their pending patch activities. Notification shall be via the Patch and Vulnerability Group (PVG) member;
  - d. Provide application names and implementation counts to the CSIRC for the Business Impact Analysis during the assignment of severity levels;
  - e. Maintain hardware/software inventories;
  - f. Coordinate their patch activities with other Information System Owners;
  - g. Coordinate their patch activities with the CSIRC;
  - h. Provide multiple representations to the PVG based on key stakeholder organizations involved in the Enterprise Life Cycle (ELC) and operations;
  - i. Acknowledge receipt of the IRS PVG Advisories per the Acknowledgment of Receipt schedule;
  - j. In the event an applicable patch is not applied, the Business and Functional Unit Owner shall document this weakness in a POA&M associated with the SA&A package; and
  - k. Information System Owners shall be represented on the PVG.
  - l. Refer to IRM 10.8.50, *Information Technology (IT) Security Service-wide Security Patch Management*, for additional guidance.
- (15) Information System Owners that own or operate a perimeter firewall environment shall comply with the security requirements in IRM 10.8.54, *Information Technology (IT) Security, Minimum Firewall Administration Requirements*.
- (16) In accordance with NIST SP 800-137, the Information System Owner shall perform the following ISCM responsibilities:
- 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.

10.8.2.3.1.5.1  
(07-12-2010)  
**Business System  
Planner (BSP)**

- (1) The Business System Planner (BSP) shall perform duties outlined for Senior Management/Executives.

10.8.2.3.1.5.1.1  
(05-16-2014)  
**Security Program  
Management Officer  
(SPMO)**

- (1) The Security Program Management Officers (SPMOs) have been established within the Business Units and IRS Information Technology 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 shall support the BSP functions, System Owners, FISMA activities and shall provide other security-related support for other security activities.
- (3) The SPMO shall provide ISSOs for the systems owned by their respective Business Unit.
  - a. When there is no ISSO assigned for a system, the SPMO shall assume the role of the ISSO.
- (4) In support of FISMA, the SPMO shall:
  - 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 POC concurrence;
 

**Note:** POA&Ms shall be approved by the AO (e.g., as a part of the accreditation process or prior to establishing in TFIMS), and shall be 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) For weaknesses and POA&Ms, the SPMO shall:
  - a. Identify and track, with ISSO 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;





- d. Approves plans (e.g., system security, privacy, assessment), memorandums of agreement or understanding, and plans of action and milestones;
- e. Determines whether significant changes in the information systems or environments of operation require reauthorization;
- f. Coordinates 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, which includes carrying out many of the activities related to the execution of the Risk Management Framework (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. Is responsible and accountable for ensuring that authorization activities and functions that are delegated to authorizing official designated representatives are carried out as specified;
- (4) In accordance with NIST SP 800-37, the AO shall ensure the following Risk Management Framework (RMF) tasks are accomplished:

**Note:** The AO is identified as having “Primary Responsibility” for these RMF tasks. 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 authorizing official and cannot be delegated to other officials within the organization. (Task R-4)

- 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 plans of action and milestones; and
  - k. Review the security and privacy posture of the system on an ongoing basis to determine whether the risk remains acceptable.
- (5) In accordance with NIST SP 800-137 and Treasury's Information Security Continuous Monitoring (ISCM) Framework, the AO shall perform the following ISCM responsibilities:
- 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. Ensure ISCM is performed in accordance with current policy;
  - d. Review security status reports and critical security documents and determines if the risk to the organization from operation of the information system remains acceptable;
  - e. In consultation with the ISSO, determine whether significant information system changes require system reauthorization;
  - f. Make authorization decisions for information systems under AO's purview on an ongoing basis; and
  - g. Formally acknowledge that an information system and/or common controls are being managed by an ongoing authorization process in accordance with the ISCM Framework and accept the responsibility for performing all necessary activities associated with that process.
- (6) In accordance with NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, the AO shall:
- a. Be identified in the system security plan for each system;
  - b. Be assigned in writing; and
  - c. Have their contact information contained in the system security plan.

#### 10.8.2.3.1.7.1

(09-12-2022)

#### **Authorizing Official Designated Representative**

- (1) The Authorizing Official Designated Representative shall be an officially designated organization official that acts on behalf of the AO to coordinate and conduct the required day-to-day activities associated with the security authorization process.
- (2) The Authorizing Official Designated Representatives shall coordinate their activities with the CIO, SAISO/CISO, Risk Executive (function), information system and common control providers, information system security officers, security control assessors, and other interested parties during the security authorization process.
- (3) The Authorizing Official Designated Representative shall be empowered by the AO to make certain decisions with regard to the planning and resourcing security authorization process, such as:
  - 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.



- (2) The ISSO, while working in collaboration with the information system owner, shall be responsible to the AO, information system owner, or SAISO/CISO for ensuring that the appropriate operational security posture (i.e., physical and environmental protection, personnel security, incident handling, and security training and awareness) is maintained for an information system or program.
- (3) As the principal advisor to the AO, Information System Owner, or SAISO/CISO on all matters, technical and otherwise, involving the security of an information system, the ISSO shall provide:
  - a. Analysis of security findings, issues, and plans;
  - b. Interpretation and clarification of security policy, guidance and new or changing IRM requirements;
  - c. Recommendation for action(s) to resolve or mitigate known weaknesses, or for preventive measures and safeguards for potential threats;
  - d. Status monitoring for POA&Ms, and other applicable action plans designed to resolve known weaknesses or prevent potential threats;
  - e. Guidance in resolving known system weaknesses according to available enterprise-level plans or solutions; and
  - f. Situational Awareness through notification of enterprise security issues, solutions, projects and plans that may impact the system(s) under their purview.
- (4) The ISSO or Chief, Privacy Officer shall have the detailed knowledge and expertise required to manage the security or privacy aspects of an information system.
- (5) In accordance with NIST, the ISSO shall:
  - a. Be responsible for ensuring the security of the system is in compliance with the requirements throughout the system life cycle (from design through disposal);
  - b. Be appointed in writing;
  - c. Accomplish duties through planning, analysis, development, implementation, maintenance, and enhancement of IRS Information Technology Cybersecurity information systems security programs, policies, procedures, and tools consistent with Department of Treasury, FISMA, and NIST guidelines;
  - d. Actively support the development and maintenance of the system security plan, to include coordinating system changes with the information system owner and assessing the security impact of those changes;
  - e. Perform and/or provide oversight and guidance for day-to-day security activities for assigned systems;
  - f. Develop or assist in development of system security policy;

**Note:** This includes, but is not limited to, contributing analysis and recommendations.

  - g. Coordinate changes to the system with the system owner and the information owner, as needed;

- h. Assess security or privacy impact of system changes;
- i. Is primarily responsible for addressing security concerns related to the Configuration Management (CM) program and for providing expertise and decision support to the Configuration Control Review Board (CCRB); and
- j. Be a voting member on the CCB for the systems and applications for which they are assigned.

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

- (6) For their respective Business Unit, the ISSO shall also:
  - a. Support the AO in the management of an enterprise risk management capability that incorporates the specific GSS or application;
  - b. Ensure current security plans, ISCP, and disaster recovery plans exist;
  - c. Ensure DR planning and testing occurs;
  - d. Ensure BR planning and testing occurs;
  - e. Participate, as needed, in testing of corrective action effectiveness, system security controls, and any other security testing;
  - f. Participate in Cybersecurity Operations Compliance Reviews and Contractor Site Reviews as they relate to assigned systems;
  - g. Provide an early warning to appropriate personnel, assisting with (or in) the tasks necessary to plan, allocate resources, and conduct any required security re-certification and accreditation;
  - h. Assist in identification of IT and security resources which support critical operations;
  - i. Support the activities relating to the security posture of the GSS or application;
  - j. Alert the AO to system-relevant security threats and/or vulnerabilities as they are discovered; provide recommendations for mitigation or resolution as appropriate;
  - k. Recommend (dis)approval of deviations from policy and/or security input to risk-based decisions for the systems or applications for which they are responsible;
  - l. Analyze the proposed changes to the systems and applications (including hardware, software, and surrounding environment) to provide system-specific input to the determination of need for re-certification; and
  - m. Analyze, interpret and/or clarify Security Assessment and Authorization packages with requirements and results for the AO.
- (7) The ISSO shall support the SPMO in FISMA activities.
- (8) In accordance with NIST SP 800-137 and Treasury's Information Security Continuous Monitoring (ISCM) Framework, the ISSO shall perform the following ISCM responsibilities:
  - a. Support the organization's ISCM program by assisting the ISSO in completing ISCM responsibilities and by participating in the configuration management process;
  - b. Establish and maintain processes and procedures in support of system-level implementation of the Treasury ISCM Framework;
  - c. Oversee and coordinate day-to-day Operational ISCM activities associated with ensuring system security as described in NIST SP 800-137 and Section 5 - ISCM Operational Security of the Treasury ISCM Framework;
  - d. Review ISCM reports from Common Control Providers to verify that the common controls continue to provide adequate protection for the information system; and

- e. Update critical security documents based on the results of ISCM.

10.8.2.3.1.9  
(09-12-2022)  
**Manager**

- (1) In accordance with TD P 85-01, the Manager shall:
  - a. Determine employee access requirements for Federal employees who report to them based on assigned job functions;
  - b. Ensure that subordinates comply with this policy and pursue appropriate action for non-compliance based on existing IRS policy;
  - c. Review and authorize privileges for employees/contractors and review user security agreements on at least an annual basis to verify the continuing need for access, the appropriate level of privileges, and the accuracy of information contained in the agreement (e.g., systems authorized for access and type);
  - d. Notify information system owner to revoke access privileges in a timely manner when a user under their supervision or oversight no longer requires access privileges, requires a change in access privileges, or fails to comply with stated policies or procedures; and
  - e. Ensure annual and specialized cybersecurity training is completed for those personnel with roles or responsibilities identified in Exhibit 10.8.2-1.

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

- (3) In accordance with NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, managers shall:
  - a. Work with the CIO and SAISO/CISO to meet shared responsibilities;
  - b. Serve in the role of system owner and/or information owner, where applicable;
  - c. Include appropriate security training in the Career Learning Plans (CLP) for those with significant security responsibilities;
  - d. Promote the professional development and certification of the information security program staff, full-time or part-time information security officers, and others with significant responsibilities for information security;
  - e. Ensure that all users (including contractors) of their systems (i.e., general support systems and major applications) are appropriately trained in how to fulfill their information security responsibilities before allowing them access;
  - f. Ensure that users (including contractors) understand specific rules of each system and application they use; and

## 10.8 Information Technology (IT) Security

- g. Work to reduce errors and omissions by users due to lack of awareness, awareness training, and/or specialized role-based training.
- (4) Managers shall be responsible for complying with information security awareness, awareness training, and role-based training requirements established for their employees, users, and those who have been identified as having significant responsibilities for information security. In accordance with IRM 1.4.1 *Resource Guide for Managers, Management Roles and Responsibilities*. Managers are also referred to as Front Line Managers.
- (5) In addition to the guidance provided in IRM 1.4.X series *Resource Guide for Managers*, Manager's shall:
  - a. Enforce the clean desk policy (refer to IRM 10.2.14, *Physical Security Program, Methods of Providing Protection* for further information);
  - b. Ensure employees complete their annual UNAX Awareness certification;
  - c. Be responsible for notifying via the access control system (e.g., Business Entitlement Access Request System (BEARS)) and following up with the responsible organization of the system user status changes (e.g., terminations, transfers); and
  - d. Receive cybersecurity awareness training. Detailed training requirements for management are stated in IRM 10.8.1.
- (6) Managers shall:
  - 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 policy. These requirements are part of the employees' mandatory annual cybersecurity awareness training; and
  - b. Ensure IT resources are being used appropriately and shall take corrective action, as needed.
  - c. Refer to IRM 10.8.27 for additional requirements.

10.8.2.3.1.10  
(09-30-2021)  
**Contracting Officer**

- (1) In accordance with TD P 85-01, Contract Offices and Procurement Offices shall:
  - a. Ensure appropriate cybersecurity terms and conditions are addressed in all IT procurements and other procurements as appropriate; and
  - b. Ensure that contract vehicles address mandatory Federal and Departmental cybersecurity requirements.
- (2) The Contracting Officer shall be responsible for managing contracts/ acquisitions and overseeing their implementation, in accordance with IRM 1.1.32, *Organization and Office of the Chief Procurement Officer*.

#  
#  
#  
#  
#  
#  
#  
#  
#  
#

10.8.2.3.1.10.1  
(09-05-2012)  
**Contracting Officers  
Representatives (COR)**

(1) The Contracting Officers Representative (COR) shall be a qualified employee appointed by the Contracting Officer to act as its technical representative in managing the technical aspects of a particular contract.

(2) In accordance with TD P 85-01, the COR shall:

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

(3) In accordance with NIST SP 800-16, the COR shall:

- a. Identify security requirements to be included in statements of work and other appropriate procurement documents (e.g., procurement requests, purchase orders, task orders, and proposal evaluation summaries) as required by the Federal regulations;
- b. Develop security requirements specific to an information technology acquisition for inclusion in procurement documents (e.g., ensures that required controls are adequate and appropriate) as required by the Federal regulations;
- c. Evaluate proposals to determine if proposed security solutions effectively address agency requirements as detailed in solicitation documents and are in compliance with Federal regulations;
- d. Develop security requirements for hardware, software, and services acquisitions specific to the IT security program (e.g., purchase of virus-scanning software or security reviews) and for inclusion in general IT acquisition guidance;
- e. Interpret and/or approve security requirements relative to the capabilities of new information technologies, revise IT acquisition guidance as appropriate, and issue changes;
- f. Identify areas within the acquisition process where IT security work steps are required;
- g. Develop security work steps for inclusion in the acquisition process, (e.g., requiring an IT Security Officer review of statements of work);
- h. Evaluate procurement activities to ensure that IT security work steps are being effectively performed;
- i. Identify general and system-specific IT security specifications which pertain to a particular system acquisition being planned;
- j. Develop security-related portions of acquisition documents;
- k. Ensure that security-related portions of the system acquisition documents meet all identified security needs;
- l. Ensure that IT security requirements are appropriately identified in acquisition documents;
- m. Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents;

- n. Monitor contract performance and review deliverables for conformance with contract requirements related to IT security and privacy; and
- o. Take action as needed to ensure that accepted products meet contract requirements.

(4) Additionally, the COR shall:

- a. Ensure that security requirements for hardware, software, and services acquisitions are in compliance with the IT security program;
- b. Develop the system termination plan to ensure that IT security breaches are avoided during shutdown and long-term protection of archived resources is achieved;
- c. Ensure hardware, software, data, and facility resources are archived, sanitized, or disposed of in a manner consistent with the system termination plan;
- d. Ensure IT resources are being used appropriately and shall take corrective action, as needed;
- e. Determine if contractors require IT access in the accomplishment of their mission;
- f. Ensure contractors are informed of appropriate uses of Government IT resources as a part of their introductory training, orientation, or the initial implementation of this policy;
- g. Ensure that contractors comply with this policy and pursue appropriate action for noncompliance;
- h. Review and authorize access privileges for contractors and reviewing user security agreements on at least an annual basis to verify the continuing need for access, the appropriate level of privileges, and the accuracy of information contained in the agreement;
- i. Notify system owners to revoke access privileges in a timely manner when a contractor under his/her supervision or oversight no longer requires access privileges, requires a change in access privileges, or fails to comply with stated policies or procedures;
- j. Ensure contracts for Information Systems contain FISMA security language; and
- k. Ensure reviews are conducted on contractor facilities and systems annually, in accordance with FISMA and applicable NIST guidance such as NIST SP 800-53.

10.8.2.3.1.11  
(09-30-2021)

**Enterprise Architect**

- (1) The OMB Circular A-130, *Managing Information as a Strategic Resource* requires agencies to ensure consistency with Federal, agency, and bureau Enterprise Architectures and to demonstrate consistency through compliance with agency business requirements and standards. The Enterprise Architect is a highly experienced IT architect who has a broad and deep understanding of the agency's overall business strategy and general IT trends and directions.

(2) In accordance with OMB Circular A-130, the Enterprise Architect shall:

- a. Lead agency enterprise architecture development and implementation efforts;
- b. Collaborate with lines of business within the agency to ensure proper integration of lines of business into enterprise architecture;
- c. Participate in agency strategic planning and performance planning activities to ensure proper integration of enterprise architecture;
- d. Facilitate integration of information security into all layers of enterprise architecture to ensure agency implementation of secure solutions; and

- e. Work closely with the program managers, the SAISO/CISO, and the business owners to ensure that all technical architecture requirements are adequately addressed by applying Federal Enterprise Architecture (FEA) and the Security and Privacy Profile (SPP).

(3) In accordance with NIST 800-137, the Enterprise Architect shall:

- 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 System Development Life Cycle (SDLC), acquisition processes, security and privacy (including supply chain) risk management, and systems engineering processes.

10.8.2.3.1.12  
(09-30-2021)  
**Information System  
Security Engineer**

- (1) The Information System Security Engineer is the individual responsible for conducting information system security engineering activities.
- (2) In accordance with NIST SP 800-37, SP 800-160 Vol.1, *Systems Security Engineering, Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, and SP 800-64, Information system security engineers shall:
  - a. Employ best practices when implementing security controls within an information system including software engineering methodologies, security engineering principles, and secure coding techniques; and
  - b. Coordinate their activities with AO designated representatives, chief information officers, senior agency information security officers/chief information security officer, information system and common control providers, and information system security officers.
- (3) In accordance with NIST SP 800-137 and Treasury's Information Security Continuous Monitoring (ISCM) Framework, the Information System Security Engineer shall perform the following ISCM responsibilities:
  - a. Capture and refine information security requirements and ensure that the requirements are effectively integrated into information technology component products and information systems through purposeful security architecting, design, development, and configuration;
  - b. Collaborate with system development teams to design and develop organizational information systems or upgrade legacy systems;
  - c. Employ best practices when implementing security controls within an information 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 information security architects, CISOs, System Owners, common control providers, and ISSOs.

10.8.2.3.1.13  
(07-12-2010)  
**Chief Financial Officer  
(CFO)**

- (1) To provide a sound leadership structure linked to OMB's financial management responsibilities, the Chief Financial Officers (CFO) Act of 1991 creates chief financial officer positions in 23 major agencies. 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.
- (2) In accordance with the CFO Act, the CFO shall:
  - a. Review cost goals of each major information security investment;
  - b. Report financial management information to OMB as part of the President's budget;
  - c. Comply with legislative and OMB-defined responsibilities as they relate to IT capital investments;
  - d. Review systems that impact financial management activities; and
  - e. Forward investment assessments to the IRB.

10.8.2.3.1.14  
(09-12-2022)  
**Privacy Officer**

- (1) The role of the Privacy Officer and/or Chief Privacy Officer is defined in accordance with the Consolidated Appropriations Act, 2005 (H.R 4818) and the E-Government Act of 2002. This role within the IRS is assigned to the Chief Privacy Officer of Privacy, Governmental Liaison and Disclosure (PGLD).

#  
#  
#  
#

- (2) In accordance with NIST, the Privacy Officer shall be responsible for:
  - a. Coordinating with the senior agency information security officer to ensure coordination of privacy and information security activities;
  - b. Reviewing and approving the categorization of information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information;
  - c. Designating which privacy controls will be treated as program management, common, system-specific, and hybrid privacy controls;
  - d. Identifying 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. Reviewing and approving privacy plans for information systems prior to authorization, reauthorization, or ongoing authorization;
  - f. Reviewing 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. Conducting and documenting the results of privacy control assessments to verify the continued effectiveness of all privacy controls selected and implemented at the agency; and





10.8.2.3.1.15  
(09-30-2021)

**Physical Security Officer**

- (1) In accordance with NIST SP 800-100, *Information Security Handbook – A Guide for Managers*, the responsibilities of Physical Security rests with the Physical Security Officer or designated official with physical security responsibilities. Within the IRS, the Chief, FMSS, serves as the senior official with responsibility for ensuring physical security requirements are established and achieved.
- (2) 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 should work to ensure this coordination of complementary controls. (NIST SP 800-100)
- (3) The physical security officer is responsible for the overall 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 should work to ensure this coordination of complementary controls. (NIST SP 800-100)
- (4) 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.
- (5) Refer to Physical Security Program 10.2.x IRMs for additional information on Physical Security Officer roles & responsibilities.
- (6) Refer to the PE - Physical and Environmental Protection sections within IRM 10.8.1 for physical security control guidance.

10.8.2.3.1.16  
(07-12-2010)

**Personnel Security Officer**

- (1) The Personnel Security Officer manages and implements safeguards and security access authorization functions. The Personnel Security Officer is the first point of contact in helping managers determine if a security background investigation is necessary for a particular position. The Personnel Security Officer may also be responsible for providing security-related exit procedures when employees leave an organization.
- (2) The Director of Personnel Security and Investigations shall be responsible for the overall implementation and management of personnel security controls across the IRS, including integration with specific information security controls.
- (3) The Director of Personnel Security and Investigations shall:



- (4) IRS Employees shall:
- 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 information technology resources to the IRS CSIRC, their immediate supervisor, and the TIGTA;
  - d. Follow directions given from the CSIRC during an incident or as suspicious activities are evaluated;
  - e. Attend/complete an initial security briefing and acknowledge attendance at the security briefing in writing;
  - f. Complete periodic (at least annual) refresher cybersecurity awareness training;
  - g. Thoroughly read and abide by the Rules of Behavior for the systems. Consult the access control procedures (e.g., BEARS), as well as associated policies and procedures to which personnel are granted access;
  - h. Not have access to sensitive IT systems until they at least have a favorably adjudicated National Agency Check (a component of the full background investigation);
  - i. Not access sensitive or classified IT systems until they have received the in brief for the appropriate clearance for the IT system;
  - j. Complete and acknowledge the completion (e.g., signing Form 11370, electronic signature) of UNAX training;
  - k. Be responsible for protecting any SBU data including Personally Identifiable Information (PII) or tax information that they have in their possession, whether it is paper-based or in electronic form;
  - l. Receive training in acceptable computer security practices prior to system access, in addition to the Rules of Behavior (for all IRS employees involved with the management, operation, programming, maintenance, or use of IRS information systems);
  - m. Immediately report any incidents of mishandling, tampering, or the loss of a laptop computer to IRS Information Technology Cybersecurity organization (refer to IRM 10.8.26, *Information Technology (IT) Security, Government Furnished and Personally Owned Mobile Device Security Policy* for further guidance);
  - n. Complete cybersecurity awareness training. Refer to IRM 10.8.1 for detailed training requirements; and
  - o. Escort visitors of IRS facilities.
- (5) Employees shall:
- a. Protect SBU data, including PII and tax information contained on IRS IT Systems and other forms of portable media from risk of disclosure or compromise; and
  - b. Minimize the threat of viruses from portable mass storage devices (including, but not limited to, flash disks, pen drives, key drives, and thumb drives), ensuring that these devices have no additional software or firmware beyond storage management and encryption. Also, never knowingly circumvent anti-virus safeguards.
  - c. Refer to IRM 10.8.1 for additional requirements.
- (6) Employees with a mobile computing device(s) shall follow all requirements as outlined in accordance with IRM 10.8.26.

#  
#

- (7) Employees shall:
- a. Refrain from using Government IT resources for activities that are inappropriate based on established Codes of Ethical Conduct for employees;
  - b. Be responsible for their own personal and professional conduct and shall follow, among others, the rules and regulations described below;
    - The Office of Personnel Management (OPM) Employee Responsibilities which states, “An employee shall not engage in criminal, infamous, dishonest, immoral, or notoriously disgraceful conduct, or other conduct prejudicial to the Government.” (5 CFR § 735.203)
  - c. Adhere to the Office of Government Ethics (OGE) Standards of Ethical Conduct which states:
    - “Employees shall put forth honest effort in the performance of their duties...” (5 Code of Federal Regulation (CFR) § 2635.101(b)(5))
    - “...an employee shall not use or permit the use of his Government position or title or any authority associated with his public office in a manner that could reasonably be construed to imply that his agency or the Government sanctions or endorses his personal activities.” (5 CFR § 2635.702 (b))
    - “An employee has a duty to protect and conserve Government Property and shall not use such property, or allow its use, for other than authorized purposes.” (5 CFR § 2635.704(a)). Employee conduct pursuant to the IRM policy on limited personal use is considered an “authorized use” of government property as the term is used in 5 CFR § 2635.704(a). See TD 87-04(4)(e) (defining limited personal use).
    - “...an employee shall use official time in an honest effort to perform official duties” and “...in accordance with law or regulation...” (CFR § 2635.705)
    - The Department of the Treasury Employee Rules of Conduct states: (1) “Employees shall not engage in criminal, infamous, dishonest, or notoriously disgraceful conduct, or any other conduct prejudicial to the Government.” (31 CFR § 0.213)
  - d. Ensure that they do not give the false impression that they are acting in an official capacity when they are using Government IT resources for non-government purposes. In addition, they shall not post, disseminate, or otherwise use IRS documents and/or symbols as part of personal documents, Internet sites, or other forms of communication.
    - If there is an expectation that such a personal use could be interpreted to represent an agency, an adequate disclaimer must be used. One acceptable disclaimer is - “The content of this message is mine personally and does not reflect the position of the U.S. Government, the Department of the Treasury, or the IRS.”
  - e. Refer to IRM 10.8.27 for additional requirements.
- (8) Refer to IRM 10.5.1 for a detailed description of Roles and Responsibilities.
- (1) The provisions of this IRM applies to individuals and organizations having contractual arrangements with the IRS, including contractors, vendors, and outsourcing providers, which use or operate IT systems.
- (2) In accordance with Treasury’s TD P 85-01, Contractors (End Users) shall:

10.8.2.3.1.18  
(11-27-2019)  
**Contractor**

#  
#



- g. Minimize the threat of viruses by write-protecting removable media, routinely scanning files, systems and media for viruses and never circumventing anti-virus safeguards;
- h. Report any suspicious or unusual activity to the appropriate supervisor and CSIRC;
- i. Notify the CSIRC of any suspicious activities that may result in security incidents;

#  
#

- k. Follow directions given from the CSIRC during an incident or as suspicious activities are evaluated;
- l. Not access sensitive or classified IT systems until they have received the in brief for the appropriate clearance for the IT system;
- m. If involved with the management, operation, programming, maintenance, or use of IRS information systems, shall receive training in acceptable computer security practices prior to system access;
- n. Receive the same level of information security awareness and training as federal employees. While under contract to the IRS, contractors are responsible for ensuring that their employees are provided appropriate cybersecurity awareness training;
- o. Contractors with significant security responsibilities shall receive, at least annually, specialized security awareness training specific to their security role and responsibilities;
- p. Attend/complete an initial security briefing and acknowledge attendance at the security briefing in writing;
- q. Attend/complete periodic (at least annual) refresher training and briefings. Complete any acknowledgements (e.g., UNAX Form 11370); and
- r. Thoroughly read and abide by the Rules of Behavior for the systems, as well as associated policies and procedures by which personnel are granted access.

## (4) Contractors shall:

- a. Protect SBU data, including PII, contained on IRS IT Systems and other forms of portable media from risk of disclosure or compromise; and
- b. Minimize the threat of viruses from portable mass storage devices (including, but not limited to, flash disks, pen drives, key drives, and thumb drives), ensuring that these devices have no additional software or firmware beyond storage management and encryption. Also, never knowingly circumvent anti-virus safeguards.
- c. Refer to IRM 10.8.1 for additional requirements.

## (5) Contractors with an IRS-issued laptop computer(s) shall follow all requirements as outlined in accordance with IRM 10.8.26.

## (6) Refer to IRM 10.5.1 for a detailed description of Roles and Responsibilities.

10.8.2.3.1.19  
(11-27-2019)**Database Administrator  
(DBA)**

- (1) The DBA shall 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 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 DBMS environments, including the Security Specialist (SecSpec) and DBA, shall obtain database security technical training necessary to implement the requirements of this IRM. The training shall cover the security features specific to the DBMS products the individuals are required to support.
- (4) Database Administrator role accounts shall have the least level of elevated privileges required to perform DBA-related duties and shall 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 shall use a separate system administrator role account that provides these capabilities, but shall not receive full system administrator privileges.
  - a. DBA's system administrator accounts with limited privileges shall 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 shall:
  - 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.

10.8.2.3.1.20  
(09-30-2021)  
**Encryption Recovery  
Agent**

- (1) Encryption Recovery Agents shall be required for the safe recovery of data, whenever encryption keys are lost or compromised.
- (2) The role of Encryption Recovery Agents shall be established in all organizations that administer IT systems with encryption and resources.
- (3) Business and functional unit owners shall establish policies and procedures for the administration of recovery agents for all IT environments.
- (4) In accordance with NIST SP 800-57, *Recommendation for Key Management – Part 1: General (Revision 4)*, Encryption Recovery Agents shall be responsible for:
  - a. The keying material that needs to be saved for a given application;

- b. How and where the keying material would be saved;
  - c. Who shall be responsible for protecting the Key Recovery Information (KRI), whether it be an individual or an external organization;
  - d. Who is authorized to receive the KRI upon request and under what conditions;
  - e. What audit capabilities and procedures would be included in the Key Recovery System (KRS), including a policy which identifies the events to be audited;
  - f. How the KRS would deal with aged keying material or the destruction of the keying material;
  - g. Who would be notified when keying material is recovered and under what conditions; and
  - h. The procedures that need to be followed when the KRS or some portion of the data within the KRS is compromised.
- (5) The Encryption Recovery Agent shall provide support during key recovery procedures.

10.8.2.3.1.21  
(11-27-2019)

**Network Administrator**

- (1) Network Administrators (NAs) shall be responsible for the day-to-day administration of the network devices under their purview.
- (2) At a minimum, the NA shall:
- 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 his/her 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) The NA shall support CSIRC efforts and security incident handling.
- (4) The NA shall apply patches and hot fixes as directed, following configuration management policies and procedures. Refer to IRM 10.8.50, for further information concerning security patch management.

10.8.2.3.1.22  
(05-16-2014)

**Program Developer/Programmer**

- (1) Program Developers/Programmers shall be responsible for the development, testing and maintenance of application programs.
- (2) At a minimum, Program Developers/Programmers shall:

- 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 CM practices and the ELC requirements; and
- d. Create installation scripts, processes, and instructions for production organizations to utilize. The developer shall incorporate feedback mechanisms into the installation processes as needed.

10.8.2.3.1.23  
(05-16-2014)

**Web Developer**

- (1) Web Developer shall be responsible for:
  - a. Development of Web sites and applications, including creating/manipulating/implementing graphic images and formulating documentation for Web sites 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.
  - c. Refer to IRM 10.8.22 for additional requirements.

10.8.2.3.1.24  
(03-31-2017)

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

- (1) The roles and responsibilities for the Resource Access Control Facility (RACF) Specialist have been relocated to IRM 10.8.33, *Information Technology (IT) Security, Mainframe System Security Policy*. Refer to IRM 10.8.33 for RACF Specialist responsibilities.

10.8.2.3.1.25  
(11-27-2019)

**Security Specialist  
(SecSpec)**

- (1) The SecSpec shall be 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) The SecSpec shall oversee any and all user (e.g., system, database, application, etc.) administration regardless of how or who performs it.
- (3) Additionally, the SecSpec shall:
  - 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 his/her 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) The SecSpec shall 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) A SecSpec shall not perform system/security administration on any system/platform/application, etc.
- (6) The SecSpec shall have read-only access to system resources and shall not modify audit settings.
- (7) SecSpecs shall:
  - 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.
  - d. Refer to IRM 10.8.1 for additional requirements.
- (8) The IT SecSpec shall be 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 shall cover 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 ISSO and Information System Owner) as necessary to bring systems into compliance with IRM 10.8.21.
  - e. Refer to IRM 10.8.21 for additional requirements.
- (9) The IT SecSpec shall be concerned with the security and integrity of Linux/Unix servers, workstations and devices, and be 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 shall ensure 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.
  - e. Refer to IRM 10.8.15 for additional requirements.
- (10) IT SecSpecs shall be concerned with the security and integrity of Windows servers, workstations and devices, and be 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 shall ensure 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 10.8.20; and
  - d. Not have operating System Administrator privileges.
  - e. Refer to IRM 10.8.20 for additional requirements.
- (11) IT SecSpecs shall be concerned with the security and integrity of Web application servers and be 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.
  - d. Refer to IRM 10.8.22 for additional requirements.
- (12) Support Security Assessments and Authorization efforts; controls testing (monthly and annual), contingency testing, documentation development, POA&M weakness correction, and ongoing security vulnerability remediation efforts.

10.8.2.3.1.26  
(03-31-2017)  
**System Administrator  
(SA)**

- (1) SAs shall be 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 shall:
- 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 his/her 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) The SA shall be responsible for supporting the SecSpec's needs for read access to system resources as defined in the access control request (e.g., BEARS).
- (4) The SA shall 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 shall be documented in the Computer Operations Handbook or equivalent for the system/application and in the Security Assessments and Authorization documentation for the relevant GSS and application.
- (6) The use of non-SAs for user administration shall be established via a 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) The SA shall support CSIRC efforts and security incident handling.
- (9) The SA shall install security patches in a timely and expeditious manner based on CSIRC's criticality designation.
- (10) The SA shall apply patches and hot fixes as directed, following configuration management policies and procedures and contact IRS Information Technology Cybersecurity organization for further information concerning security patch management.
- (11) Support ISCP and DR Plan development and accuracy.

10.8.2.3.1.27  
(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 shall:
  - 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.

10.8.2.3.1.28  
(05-16-2014)  
**Telecommunications  
Specialist**

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

10.8.2.3.1.29  
(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), etc.) who provide the service.
- (2) The UA shall have no more capability than appropriate to establish a user on a system or to establish a user within an application.
- (3) The UA shall use the IRS approved access control (e.g., BEARS) process.
- (4) An SA or NA establishing user access does not assume this role.

10.8.2.3.1.30  
(05-16-2014)  
**Integrated Data Retrieval  
System (IDRS) Security  
Analyst**

- (1) In 2009, to help ensure proper separation of duties, IDRS security user and unit account administration migrated from Cybersecurity Operations to the Enterprise Operations, Operational Security Program Management Office (EOPS-OSPMO). Cybersecurity Operations will continue to perform IDRS security policy support and oversight related tasks.
- (2) The IDRS Security Officer role has been replaced with two new roles:
  - a. The IDRS Security Account Administrator performs the user and unit account administration tasks previously performed by the IDRS Security Officer.
  - b. The IDRS Security Analyst performs the policy support and oversight tasks previously performed by the IDRS Security Officer.
- (3) The IDRS Security Analyst performs IDRS security policy support and oversight related tasks for IDRS campus domains and/or IDRS computing centers.
- (4) The Integrated Data Retrieval System (IDRS) Security Analyst shall be a non-bargaining unit employee who is a member of the Cybersecurity Operations staff.

- (5) For additional related responsibilities, refer to IRM 10.8.34 *Information Technology (IT) Security, IDRS Security Controls*.

10.8.2.3.1.31  
(05-16-2014)

**Integrated Data Retrieval System (IDRS) Security Account Administrator**

- (1) In 2009, to help ensure proper separation of duties, IDRS security user and unit account administration migrated from Cybersecurity Operations to the Enterprise Operations, Operational Security Program Management Office (EOPS-OSPMO). Cybersecurity Operations will continue to perform IDRS security policy support and oversight related tasks.
- (2) The IDRS Security Officer role has been replaced with two new roles:
- a. The IDRS Security Account Administrator performs the user and unit account administration tasks previously performed by the IDRS Security Officer.
  - b. The IDRS Security Analyst performs the policy support and oversight tasks previously performed by the IDRS Security Officer.
- (3) The IDRS Security Account Administrator performs tasks relating to the administration of IDRS user and unit accounts.
- (4) The IDRS Security Account Administrator shall be a non-bargaining unit employee who is a member of the Security Operations & Standards Division (EOPS-SOSD) staff.
- (5) To help ensure proper separation of duties, the IDRS Security Account Administrator shall not simultaneously serve as Computing Center IDRS Security Administrator.
- (6) The IDRS Security Account Administrator shall maintain a current list of Unit Security Representatives (USRs), alternate USRs, Terminal Security Administrators (TSAs), managers, and the designated Primary Recipients for all IDRS units in the IDRS Unit and USR Database (IUUD). To the extent practical, this listing should be complete and accurate and include at least the following information:
- Name
  - SEID
  - Division business unit
  - Name of unit or function
  - IDRS unit number(s) covered
  - Telephone number
  - IDRS unit security role
  - Business mailing addresses
  - Indicate when command code ASNPW is in the individual's profile.
- (7) For additional related responsibilities, refer to IRM 10.8.34.

10.8.2.3.1.32  
(05-16-2014)

**Computer Audit Specialist**

- (1) The Computer Audit Specialist (CAS) security role, which is specific to IRS business units (e.g., Large Business and International (LB&I)), shall be 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 shall load, run and configure 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 shall have the ability to add, configure and remove software. This will allow 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.

10.8.2.3.1.33  
(05-16-2014)

**Functional Workstation  
Specialist**

- (1) The Functional Workstation Specialist shall include, but not be limited to the following responsibilities:
  - a. Have a full analytical and operational knowledge of specific software applications in order 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, etc.);
  - h. Coordinate activities relating to the security posture of the application with responsible business units and IRS Information Technology (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.

- 10.8.2.3.1.34  
(05-16-2014)  
**Management/Program Analyst**
- (1) The Management/Program Analyst, in support of meeting FISMA requirements, shall:
- 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.
- 10.8.2.3.1.35  
(09-30-2021)  
**System Designer**
- (1) System Designers shall be responsible for developing, implementing, and monitoring polices and controls to ensure data accuracy, security and legal regulatory compliance throughout the system lifecycle.
- (2) System Designers shall 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 shall be responsible for identifying IT assets and determining their value for establishing implementation security safeguard priorities.
- (4) System Designers (a.k.a. System Developers) shall 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.
- a. Refer to IRM 10.8.1 (e.g., SA-11 Developer Security Testing and Evaluation) for additional security control assessments requirements.
- (5) System Designers shall consult and collaborate with the IRS Enterprise Architect and concerned Information System Security Engineer (ISSE) and ISSO whenever designing new system(s) and/or sub-systems functionality.
- 10.8.2.3.1.36  
(05-16-2014)  
**Technical Support Staff (Desktop)**
- (1) The Technical Support staff shall educate end-users in security procedures and practices in the context of performing their tasks.
- 10.8.2.3.1.37  
(09-30-2021)  
**Security Staff (Physical Security)**
- (1) Physical Security Staff The physical security office is responsible for developing and enforcing appropriate physical security controls, often in consultation with information security management, program and functional managers, and others.
- (2) The Security Staff shall:
- 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.

- 10.8.2.3.1.38  
(09-12-2022)  
**Cyber Critical  
Infrastructure Protection  
(CIP) Coordinator**
- (1) The Cyber Critical Infrastructure Protection (CIP) Coordinator is designated by the CIO. In this role, the IRS Cyber CIP Coordinator shall:
- 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 Working 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  
(11-27-2019)  
**IRS Information  
Technology  
Cybersecurity  
Organization**
- (1) In collaboration with the Business and Functional Unit Owner, the IRS Information Technology Cybersecurity organization shall:
- 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 Information Technology Cybersecurity organization;
  - f. Implement corrective actions and validate fixes to mitigate vulnerabilities assigned to IRS Information Technology 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 Information Technology Cybersecurity organization shall:
- 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 Information Technology 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 Information Technology Cybersecurity organization to resolve (if possible) issues identified during DR testing or document reasons/risk/impact.
  - l. Refer to IRM 10.8.60 for additional requirements.
- (3) IRS Information Technology Cybersecurity organization shall:
- 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.
  - e. Refer to IRM 10.8.1 for additional requirements.
- (4) IRS Information Technology organization shall notify the CSIRC of suspicious activities and shall comply with CSIRC directions.
- a. IRS Information Technology organization shall comply with their internal configuration management requirements.
  - b. IRS Information Technology organization shall perform containment activities.
- 10.8.2.3.2.2 (05-16-2014)  
**IRS Information Technology User and Network Services (UNS) Organization**
- (1) IRS Information Technology UNS Organization shall administer the firewall devices comprising the perimeter firewall environment.
- a. Refer to IRM 10.8.54 for additional requirements.
- (2) The UNS, Engineering and Capacity Management (EC&M) shall design the IRS network perimeter Demilitarized Zone (DMZ), including firewall requirements, and work directly with IRS Information Technology UNS, Network Operations Support Services (NOSS) on its implementation and maintenance.
- (3) The IRS Information Technology NOSS shall ensure that the IRS minimum firewall requirements and policies are met.
- (4) The IRS Information Technology NOSS shall provide 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 Information System Owner for IRS Information Technology UNS Organization shall:
- a. Be responsible for notifications and routing of information to the appropriate organizational POCs;



#  
#  
#  
#

- (3) In accordance with Treasury Incident Response plan policy, CSIRC shall:
- a. Serve as primary coordination point for IR within the IRS;
    - i. It is crucial at the initial analysis stage for the 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 TSSSOC for all communications and follow up activities in response to an incident;
  - d. Ensure compliance with the Treasury Incident Response Plan policy; and
  - e. Report to TSSSOC in accordance with the Incident Response Plan section 4.2.3 Reporting and Escalation reporting requirements.
  - f. See Exhibit 10.8.2-2, Incident, Breach, and Event Definitions for Treasury definitions of Incidents and breaches.

#  
#  
#

- (4) CSIRC shall operate and maintain a wireless intrusion detection system.
- a. Refer to IRM 10.8.55 for additional requirements.
- (5) CSIRC shall:
- 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 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 shall include the contacts' various pager and phone numbers 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.
- w. Refer to IRM 10.8.1 for additional requirements.

(6) CSIRC shall:

- 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 Information Technology organization DMZ efforts.
- d. Refer to IRM 10.8.54 for additional requirements.

10.8.2.3.2.4  
(07-12-2010)  
**Situational Awareness  
Management Center  
(SAMC)**

- (1) The SAMC shall:
- a. Process physical security incidents; and
  - b. Establish a MOA/MOU with the 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.
  - c. Refer to IRM 10.8.60 for additional requirements.

10.8.2.3.2.5  
(07-12-2010)  
**IRS Patch and  
Vulnerability Group  
(PVG)**

- (1) IRS PVG shall:
- a. Facilitate the identification and distribution of patches in accordance with NIST SP 800-40 Rev 3 *Creating a Patch and Vulnerability Management Program*;
  - b. Inventory the organization's IT resources to determine which hardware equipment, operating systems, and software applications are used within the organization;
  - c. 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;
  - d. Prioritize the order in which the organization addresses remediating vulnerabilities;
  - e. Create a database of remediations that need to be applied organization-wide;
  - f. Conduct testing of patches and non-patch remediations on IT devices that use standardized configurations;
  - g. Oversee vulnerability remediation;
  - h. Distribute vulnerability and remediation information to local administrators;
  - i. Perform automated deployment of patches to IT devices using enterprise patch management tools;
  - j. Configure automatic update of applications whenever possible and appropriate;
  - k. Verify vulnerability remediation through network and host vulnerability scanning; and
  - l. Train administrators, who apply vulnerability remediations, how to apply them appropriately.

**Note:** This group may be an independent entity, or its duties may be performed by existing group(s) (e.g. Configuration Control Boards, Executive Steering Committees etc.).

- m. Refer to IRM 10.8.50 for additional requirements.

**Exhibit 10.8.2-1 (09-12-2022)****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.

- i. Roles with direct impact on system security (e.g., ISSOs) require 8 hours of specialized training.
- ii. Roles with ancillary impact on system security (e.g., Help Desk Personnel) require 4 hours of specialized training.

**Note:** The roles and specialized training hours listed come from TD P 85-01 Appendix H.

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

**Exhibit 10.8.2-1 (Cont. 1) (09-12-2022)**  
**Roles That Require Specialized Training**

Quality Assurance Personnel - Individuals responsible for ensuring the quality of an information system(s) and/ or it's 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.	4

**Exhibit 10.8.2-2 (09-12-2022)**  
**Incident, Breach, and Event Definitions**

All confirmed or suspected cyber incidents and certain cyber events that involve PII are also “breaches” as that term is defined. All breaches are considered incidents in the case where an incident is also a breach, it is important that bureaus also follow the breach guidance contained within the Treasury Incident Response Plan. Incidents that are not breaches do not require the application of the breach sections of the Treasury Incident Response Plan.

Activity Type	Definition
Breach	<p>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).</p> <p><b>INFORMATIONAL:</b> A breach is a type of incident.</p>
Incident	<p>An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.</p>
Major Incident	<p>A major incident is EITHER:</p> <p>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, <b>Computer Security Incident Handling Guide</b>, OR,</p> <p>II. A breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, 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.</p>

**Exhibit 10.8.2-2 (Cont. 1) (09-12-2022)**  
**Incident, Breach, and Event Definitions**

Significant cyber incident	<p>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.</p> <p>All major incidents are also deemed significant cyber incidents. However, only when a breach of PII 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 PPD-41.</p>
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.
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.
Cyber event	Any observance occurrence in a network or system that may indicate a cyber incident has occurred.

**Exhibit 10.8.2-3 (09-12-2022)****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 goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

**ACIO** – Associate CIO

**ACIOCS** – Associate CIO for Cybersecurity

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

**ATO** – Authority 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 is; or a comprehensive assessment and report on the financial condition and/or the results of performance of a government entity, program or related activity.

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

**Authorizing Official (AO)** – Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals.

**Availability** – The ability to access a specific resource within a specific time frame as defined with the IT product specification. The availability of an IT system allows the accessibility and usability upon demand by an authorized entity. This state is the prevention of the unauthorized withholding of information or resources.

**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 - Use BEARS to request access to and perform recertifications on subapps (entitlements) which have been migrated from OL5081.

**BIA** – Business Impact Assessment

**BPA** – Business Purchase Agreement

**BR** – Business Resumption

**BSP** – Business System Planner

**Exhibit 10.8.2-3 (Cont. 1) (09-12-2022)****Terms and Acronyms****C**

**Campus IDRS Security Officer** – The Campus IDRS Security Officer role no longer exists. In 2009, to help ensure proper separation of duties, IDRS security user and unit account administration migrated from Cybersecurity Operations to the Enterprise Operations, Operational Security Program Management Office (EOPS-OSPMO). Cybersecurity Operations will continue to perform IDRS security policy support and oversight related tasks. The IDRS Security Officer role has been replaced with two new roles: a. The IDRS Security Account Administrator performs the user and unit account administration tasks previously performed by the IDRS Security Officer. b. The IDRS Security Analyst performs the policy support and oversight tasks previously performed by the IDRS Security Officer.

**CAS** – Computer Audit Specialist

**CCB** – Configuration Control Board

**CCRB** – Configuration Control Review Board

**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.

**Certification Authority (CA)** – A trusted entity in a public key infrastructure (PKI) that issues and revokes certificates exacting compliance to a PKI policy.

**CFO** – Chief Financial Officer

**CFR** – Code of Federal Regulation

**Chief Information Officer (CIO)** – An agency official responsible for:

- 1) Providing advice and other assistance to the head of the executive agency and other senior management/executive official of the agency to ensure that IT is acquired and information resources are managed in a manner that is consistent with laws, E.O.s, directives, policies, regulations, and priorities established by the head of the agency.
- 2) Developing, maintaining, and facilitating the implementation of a sound and integrated IT architecture for the agency.
- 3) Promoting the effective and efficient design and operation of all major information management processes for the agency, including to work processes of the agency.

**CIO** – Chief Information Officer

**Exhibit 10.8.2-3 (Cont. 2) (09-12-2022)****Terms and Acronyms**

**CIP** – Critical Infrastructure Protection

**CISO** – Chief Information Security Officer

**CM** – Configuration Management

**CNSS** – Committee on National Security Systems

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

**Contingency Plan** – Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disaster.

**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.

**COTS** – Commercial-off-the-shelf

**CPO** – Chief Procurement Officer

**CSIRC** – Computer Security Incident Response Center

**D**

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

**DBA** – Database Administrator

**DBMS** – Database Management System

**Denial of Authorization** – A denial of authorization means that the information system is not authorized to operate and not placed into operation; common controls are not authorized to be provided to systems; or that the provider's system is not authorized for use by the customer organization.

**Department** – In the context of this IRM, the terms department, departments, departmental, etc. refer solely to the IRS unless there is a specific reference to Treasury. The terms “department employee(s)” and “Treasury employee(s)” also refer to the IRS.

**DHS** – Department of Homeland Security

**Disaster Recovery Plan (DRP)** – Applies to major, usually physical disruptions to service that deny access to the primary facility infrastructure for an extended period. A DRP is an information system-focused plan created and maintained by the IRS Information Technology organization or any information technology service provider designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency. The DRP may be supported by multiple information system contingency plans to address recovery of impacted individual systems once the alternate facility has been established. A DRP may support a Business Continuity Plan or Continuity of Operations plan by recovering supporting systems for mission/business processes or mission essential functions at an alternate location. The DRP only addresses information system disruptions that require relocation.

**DMZ** – Demilitarized Zone

**Exhibit 10.8.2-3 (Cont. 3) (09-12-2022)****Terms and Acronyms**

**DR** – Disaster Recovery

**E**

**EO** – Executive Order

**EC&MA** – Engineering and Capacity Management

**Education** – Education level integrates all security skills and competencies of the various functional specialties into a common body of knowledge, adds a multi-disciplinary study of concepts, issues, and principles (both technological and social), and strives to produce IT security specialists and professionals capable of forward thinking vision and pro-active response.

**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.

**Enterprise Life Cycle (ELC)** – The approach used to manage and implement business change and information systems initiatives.

**EOPS-OSPMO** – Enterprise Operations, Operational Security Program Management Office

**EOPS-SOSD** – Security Operations & Standards Division

**F**

**FCR** – Firewall Change Request

**FEA** – Federal Enterprise Architecture

**Federal Information Security Management Act (FISMA)** – requires agencies to integrate information security into their capital planning and enterprise architecture processes at the agency, conduct annual security reviews of all programs and systems, and report the results of those reviews to the OMB.

**FIPS** – Federal Information Processing Standard

**Form 14201** – Risk Acceptance Request - Used to request the AO make a Risk-Based Decision (RBD) to deviate from a specific requirement and not accept the risk associated with said RBD.

**G**

**GFIRST** – Government Forum of Incident Response Teams

**GSA** – General Service Administration

**GSP** – Guidelines, Standards and Procedures

**GSS** – General Support System

**H, I**

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

**IDRS** – Integrated Data Retrieval System

**IDS** – Intrusion Detection System

**Exhibit 10.8.2-3 (Cont. 4) (09-12-2022)****Terms and Acronyms**

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

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

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

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

**Information System Owner** – Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

**Information System Security Officer (ISSO)** – Individual assigned responsibility by the senior agency information security officer/chief information security officer, authorizing official, management official, or information system owner for ensuring the appropriate operational security posture is maintained for an information system or program.

**Information Security Continuous Monitoring** – 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 service or equipment or the personnel that support any part of the lifecycle of those services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

1) For purposes of this definition, equipment is used by an agency if the equipment is used by the agency directly or is used by a contractor under a contract with the agency that requires:

- a. Its use; or
- b. To a significant extent, its use in the performance of a service or the furnishing of a product.

2) The term “information technology” includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services and cloud computing), and related resources.

3) The term “information technology” does not include any equipment that

- a. Is acquired by a contractor incidental to a contract; or
- b. Contains imbedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment, such as elec-

**Exhibit 10.8.2-3 (Cont. 5) (09-12-2022)****Terms and Acronyms**

tronic thermostats or temperature control devices, and medical equipment where information technology integral to its operation, is not information technology.

**Information System Contingency Plan (ISCP)** – Established procedures created and maintained by IRS

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

**Integrity** – The prevention of the unauthorized/improper modification or destruction of information; includes ensuring information non-repudiation and authenticity.

**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

**IRP** – Incident Response Plan

**ISSE** – Information System Security Officer

**IUUD** – IDRS Unit and USR Database

**J, K**

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

**Key Pair** – Two mathematically related keys having the properties that one key can be used to encrypt a message that can only be decrypted using the other key. Even knowing one key, it is computationally infeasible to discover the other key.

**KISAM** – Knowledge Incident/Problem Service Asset Management

**L**

**LB&I** – Large Business and International

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

**Exhibit 10.8.2-3 (Cont. 6) (09-12-2022)****Terms and Acronyms**

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

**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.

**MOA** – Memorandums of Agreement

**MOU** – Memorandums of Understanding

**N**

**NA** – Network Administrators

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

**NOM** – Network Operations Management

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

**NOSS** – Network Operations Support Services

**NSI** – National Security Information

**O**

**OGE** – Office of Government Ethics

**OMB** – Office of Management and Budget

**OPM** – Office of Personnel Management

**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.

**Exhibit 10.8.2-3 (Cont. 7) (09-12-2022)****Terms and Acronyms**

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 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 document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

**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** – The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.

**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 Information** – This type of information may be disclosed to the public without restriction, but requires protection against erroneous manipulation or alteration. Example: public Web site.

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

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

**PVG** – Patch and Vulnerability Group

**Q, R**

**RACF** – Resource Access Control Facility

**RBD** – Risk-Based Decision

**RDBMS** – Relational Database Management Systems

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

**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

**Exhibit 10.8.2-3 (Cont. 8) (09-12-2022)****Terms and Acronyms**

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** – The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

**Risk Assessment** – The process of identifying risks to agency operations (including mission, functions, image, or reputation), agency assets, or individuals by determining the probability of occurrence, the resulting impact, and additional security controls that would mitigate this impact. Part of risk management (incorporating threat and vulnerability analyses), the output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process. The risk assessment brings together important information for agency officials with regard to the protection of the information system and generates essential information required for the security plan. The periodic assessment of risk to agency assets or operations resulting from the operation of an information system is an important activity required by FISMA. (also Security Risk Assessment)

**RMF** – Risk Management Framework

**S**

**Safeguards** – Protective measures prescribed to meet the security requirements (i.e., CIA) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

**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, E.O.s, directives, policies, instructions, regulations, or organizational (mission) needs to ensure the CIA 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

**Exhibit 10.8.2-3 (Cont. 9) (09-12-2022)****Terms and Acronyms**

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** – 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 5 U.S.C. § 552a (the Privacy Act), but has not been specifically authorized under criteria established by an E.O. or an act of Congress to be kept classified in the interest of national defense or foreign policy. Examples of such sensitive information include personal financial information and information that discloses law enforcement investigative methods. Other particular classes of information may have additional statutory limits on disclosure that require that information to also be treated as sensitive. Examples include tax information, which is protected by Section 6103 of the IRC (26 U.S.C. § 6103) and advanced procurement information, protected by the Procurement Integrity Act (41 U.S.C. § 423).

**SOP** – Standard Operating Procedure

**SP** – Special Publication

**SPMO** – Security Program Management Officer

**SPP** – Security and Privacy Profile

**SRM** – Security Risk Management

**System** – A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. A system normally includes hardware, software, information, data, applications, communications, and people.

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

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

**System Security Plan** – 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

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

**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

### Exhibit 10.8.2-3 (Cont. 10) (09-12-2022)

#### Terms and Acronyms

**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

**TSSSOC** – Treasury Shared Services Security Operations Center

#### U, V

**UA** – User Administrator

**UNS** – User and Network Services Organization

**USR** – Unit Security Representative

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

**Vulnerability Assessment** – Formal description and evaluation of the vulnerabilities in an information system.

**Exhibit 10.8.2-4 (05-01-2023)****Related Resources****Department of the Treasury Publications**

- TD P 85-01, Version 3.1.1 *Treasury Information Technology Security Program*, July 16, 2020
- TD P 87-04, *Personal Use of Government Information Technology Resources*, January 27, 2012
- TD P 15-03, *Intelligence Information Systems Security Policy Manual*, September 19, 2013
- Treasury Chief Information Officer (TCIO) Memo 17-01, *Roles and Responsibilities*, December 22, 2016,
- Treasury Information Security Continuous Monitoring (ISCM) Framework, November 11, 2014
- Department of the Treasury OCIO - Cybersecurity, Version 1.3, *Departmental Incident Response Plan (IRP)*, December 20, 2021

**IRS Publications**

- IRM 1.1.32, *Organization and Staffing, Office of the Chief Procurement Officer*
- IRM 1.4.X series, *Resource Guide For Managers*
- 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, Policy and Guidance*
- 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 10.8.15, *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 10.24, *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 10.8.54, *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)*
- IRM 10.8.62, *Information Technology (IT) Security, Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Process*
- IRM 10.9.1, *Classified National Security Information, (NSI)*

The IRS' Office of Service-wide Policy, Directives and Electronic Research (SPDER), in partnership with

#  
#

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

- NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998
- NIST SP 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006

**Exhibit 10.8.2-4 (Cont. 1) (05-01-2023)****Related Resources**

- NIST SP 800-37 Rev. 2 *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, September 20, 2018
- NIST SP 800-40 Rev. 3 *Creating a Patch and Vulnerability Management Program*, July 2013
- NIST SP 800 - 53 Rev. 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, September 2020 (Updated 12/10/2020)
- NIST SP 800-53A, Rev. 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, January 2022
- NIST SP 800-57 Part 1, *Recommendation for Key Management – Part 1: General (Revision 4)* January 28, 2016
- NIST SP 800-61 Rev 2, *Computer Security Incident Handling Guide*, August 2012
- NIST SP 800-64 Rev. 2, *Security Considerations in the System Development Life Cycle*, October 2008
- NIST SP 800-100, *Information Security Handbook: A Guide for Managers*, October 2006  
*Information regarding the NIST publications noted above is available on the NIST web site: <https://www.nist.gov>*

**Other References**

- FISMA requirements (see <http://csrc.nist.gov/sec-cert>)
- Privacy Act of 1974
- OMB Memorandum for Chief Acquisition Officers - Revisions to the Federal Acquisition Certification for Contracting Officer's Representatives (FAC-COR), September 6, 2011
- OMB Circular No. A-130, *Management Information as a Strategic Resource*, July 27, 2016
- Public Law 105-35, *Taxpayer Browsing Protection Act of 1997*
- Consolidated Appropriations Act, 2016 (H.R. 4818)
- Code of Federal Regulations (CFR), Title 5 - Administrative Personnel
- Presidential Policy Directive (PPD), *United States Cyber Incident Coordination (PPD-41)*, July 26, 2016

