



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.33

AUGUST 14, 2025

EFFECTIVE DATE

(08-14-2025)

PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.8.33, *Information Technology (IT) Security, Mainframe System Security Policy*.

MATERIAL CHANGES

- (1) Section 33 Mainframe System Security Policy - Updated subsections to align with standard Security Policy language. All NIST control family identifiers were updated to include a leading zero (0) for single digit identifiers, changed all 'shall' to 'must' where appropriate. Updated metadata author attributes. Updated section 33 parttitle to include artificial intelligence.
- (2) 10.8.33.1 Program Scope and Objectives - Updated subsection to align with standard Security Policy language.
- (3) 10.8.33.1.1 Background - Updated subsection to align with standard Security Policy language.
- (4) 10.8.33.1.2 Authority - Updated subsection to align with standard Security Policy language.
- (5) 10.8.33.1.3 Roles and Responsibilities - Moved mainframe specific roles and responsibilities to 10.8.33.3 and updated subsection to align with standard Security Policy language.
- (6) 10.8.33.1.4 Program Management and Review - Updated subsection to align with standard Security Policy language.
- (7) 10.8.33.1.5 Program Controls - Updated subsection to align with standard Security Policy language.
- (8) 10.8.33.1.6 Terms and Acronyms - Updated subsection to align with standard Security Policy language.
- (9) 10.8.33.1.7 Related Resources - Updated subsection to align with standard Security Policy language.
- (10) 10.8.33.2 Risk Acceptance and Risk-Based Decisions (RBD) - Relocated from 10.8.33.1.8 and updated subsection to aligned with standard Security Policy language.
- (11) 10.8.33.3 Mainframe Roles and Responsibilities - Added new subsection and updated content to aligned with standard Security Policy language.
- (12) 10.8.33.3.1 System Programmer - Relocated subsection and aligned with standard Security Policy language.
- (13) 10.8.33.3.2 Resource Access Control Facility (RACF) System Administrator (RSA) - Relocated subsection and aligned with standard Security Policy language.
- (14) 10.8.33.3.3 Resource Access Control Facility (RACF) User and Group Administrator - Relocated subsection and aligned with standard Security Policy language.
- (15) 10.8.33.3.4 Resource Access Control Facility (RACF) System and Group Auditor - Relocated subsection and aligned with standard Security Policy language.
- (16) 10.8.33.4 IT Security Controls - Updated subsection to align with standard Security Policy language.

- (17) 10.8.33.4.1 AC – Access Control - Updated subsection to align with standard Security Policy language.
- (18) 10.8.33.4.1.1 AC-02 Account Management - Updated subsection to align with standard Security Policy language.
- (19) 10.8.33.4.1.2 AC-03 Access Enforcement - Updated subsection to align with standard Security Policy language.
- (20) 10.8.33.4.1.3 AC-04 Information Flow Enforcement - Updated subsection to align with standard Security Policy language.
- (21) 10.8.33.4.1.4 AC-06 Least Privilege - Updated subsection to align with standard Security Policy language.
- (22) 10.8.33.4.1.5 AC-07 Unsuccessful Logon Attempts - Updated subsection to align with standard Security Policy language.
- (23) 10.8.33.4.1.6 AC-10 Concurrent Session Control - Updated subsection to align with standard Security Policy language.
- (24) 10.8.33.4.1.7 AC-11 Session Lock - Updated subsection to align with standard Security Policy language.
- (25) 10.8.33.4.1.8 AC-12 Session Termination - Updated subsection to align with standard Security Policy language.
- (26) 10.8.33.4.1.9 AC-16 Security and Privacy Attributes - Updated subsection to align with standard Security Policy language.
- (27) 10.8.33.4.2 AT – Awareness and Training - Updated subsection to align with standard Security Policy language.
- (28) 10.8.33.4.3 AU – Audit and Accountability - Updated subsection to align with standard Security Policy language.
- (29) 10.8.33.4.3.1 AU-03 Content of Audit Records - Updated subsection to align with standard Security Policy language.
- (30) 10.8.33.4.3.2 AU-04 Audit Log Storage Capacity - Updated subsection to align with standard Security Policy language.
- (31) 10.8.33.4.3.3 AU-05 Response to Audit Logging Process Failures - Updated subsection to align with standard Security Policy language.
- (32) 10.8.33.4.3.3 AU-05 Response to Audit Logging Process Failures - Per DISA: Removed SRG-APP-000109-MFP-000155 requirement because it is not appropriate to define at the enterprise level (DSPAV).
- (33) 10.8.33.4.3.4 AU-06 Audit Record Review, Analysis, and Reporting - Updated subsection to align with standard Security Policy language.
- (34) 10.8.33.4.3.5 AU-07 Audit Record Reduction and Report Generation - Updated subsection to align with standard Security Policy language.
- (35) 10.8.33.4.3.6 AU-08 Time Stamps - Updated subsection to align with standard Security Policy language.

- (36) 10.8.33.4.3.7 AU-09 Protection of Audit Information - Updated subsection to align with standard Security Policy language.
- (37) 10.8.33.4.3.8 AU-10 Non-Repudiation - Updated subsection to align with standard Security Policy language.
- (38) 10.8.33.4.3.9 AU-12 Audit Record Generation - Updated subsection to align with standard Security Policy language.
- (39) 10.8.33.4.3.10 AU-14 Session Audit - Updated subsection to align with standard Security Policy language.
- (40) 10.8.33.4.4 CA – Assessment, Authorization, and Monitoring - Updated subsection to align with standard Security Policy language.
- (41) 10.8.33.4.5 CM – Configuration Management - Updated subsection to align with standard Security Policy language.
- (42) 10.8.33.4.5.1 CM-03 Configuration Change Control - Updated subsection to align with standard Security Policy language.
- (43) 10.8.33.4.5.2 CM-05 Access Restrictions for Change - Updated subsection to align with standard Security Policy language.
- (44) 10.8.33.4.5.3 CM-06 Configuration Settings - Updated subsection to align with standard Security Policy language.
- (45) 10.8.33.4.5.4 CM-07 Least Functionality - Updated subsection to align with standard Security Policy language.
- (46) 10.8.33.4.5.5 CM-11 User-Installed Software - Updated subsection to align with standard Security Policy language.
- (47) 10.8.33.4.5.6 CM-14 System and Communications Protection - Security Impact Analysis - Updated subsection to align with standard Security Policy language.
- (48) 10.8.33.4.6 CP – Contingency Planning - Updated subsection to align with standard Security Policy language.
- (49) 10.8.33.4.7 IA – Identification and Authentication - Updated subsection to align with standard Security Policy language.
- (50) 10.8.33.4.7.1 IA-02 Identification and Authentication - Organizational Users - Updated subsection to align with standard Security Policy language.
- (51) 10.8.33.4.7.2 IA-05 Authenticator Management - Updated subsection to align with standard Security Policy language.
- (52) 10.8.33.4.7.3 IA-06 Authenticator Feedback - Updated subsection to align with standard Security Policy language.
- (53) 10.8.33.4.7.4 IA-07 Cryptographic Module Authentication - Updated subsection to align with standard Security Policy language.
- (54) 10.8.33.4.7.5 IA-08 Identification and Authentication - Non-organizational Users - Updated subsection to align with standard Security Policy language.

- (55) 10.8.33.4.7.6 IR – Incident Response - Updated subsection to align with standard Security Policy language.
- (56) 10.8.33.4.8 IR – Incident Response - Updated subsection to align with standard Security Policy language.
- (57) 10.8.33.4.9 MA – Maintenance - Updated subsection to align with standard Security Policy language.
- (58) 10.8.33.4.9.1 MA-03 Maintenance Tools - Updated subsection to align with standard Security Policy language.
- (59) 10.8.33.4.9.2 MA-04 Nonlocal Maintenance - Updated subsection to align with standard Security Policy language.
- (60) 10.8.33.4.10 MP – Media Protection - Updated subsection to align with standard Security Policy language.
- (61) 10.8.33.4.11 PE – Physical and Environmental Protection - Updated subsection to align with standard Security Policy language.
- (62) 10.8.33.4.12 PL – Planning - Updated subsection to align with standard Security Policy language.
- (63) 10.8.33.4.13 PM – Program Management Information Security Program Plan - Updated subsection to align with standard Security Policy language.
- (64) 10.8.33.4.14 PS – Personnel Security - Updated subsection to align with standard Security Policy language.
- (65) 10.8.33.4.15 PT – Personally Identifiable Information Processing and Transparency - Updated subsection to align with standard Security Policy language.
- (66) 10.8.33.4.16 RA – Risk Assessment - Updated subsection to align with standard Security Policy language.
- (67) 10.8.33.4.16.1 RA-05 Vulnerability Monitoring and Scanning - Updated subsection to align with standard Security Policy language.
- (68) 10.8.33.4.17 SA – System and Services Acquisition - Updated subsection to align with standard Security Policy language.
- (69) 10.8.33.4.18 SC – System and Communications Protection - Updated subsection to align with standard Security Policy language.
- (70) 10.8.33.4.18.1 SC-02 Separation of System and User Functionality - Updated subsection to align with standard Security Policy language.
- (71) 10.8.33.4.18.2 SC-03 Security Function Isolation - Updated subsection to align with standard Security Policy language.
- (72) 10.8.33.4.18.3 SC-13 Cryptographic Protection - Updated subsection to align with standard Security Policy language.
- (73) 10.8.33.4.18.4 SC-17 Public Key Infrastructure Certificates - Updated subsection to align with standard Security Policy language.
- (74) 10.8.33.4.18.5 SC-18 Mobile Code - Updated subsection to align with standard Security Policy language.

- (75) 10.8.33.4.18.6 SC-24 Fail in Known State - Updated subsection to align with standard Security Policy language.
- (76) 10.8.33.4.18.7 SC-28 Protection of Information at Rest - Updated subsection to align with standard Security Policy language.
- (77) 10.8.33.4.18.8 SC-39 Process Isolation - Updated subsection to align with standard Security Policy language.
- (78) 10.8.33.4.18.9 SC-45 System Time Synchronization - Updated subsection to align with standard Security Policy language.
- (79) 10.8.33.4.19 SI – System and Information Integrity - Updated subsection to align with standard Security Policy language.
- (80) 10.8.33.4.19.1 SI-02 Flaw Remediation - Updated subsection to align with standard Security Policy language.
- (81) 10.8.33.4.19.2 SI-03 Malicious Code Protection - Updated subsection to align with standard Security Policy language.
- (82) 10.8.33.4.19.3 SI-06 Security and Privacy Function Verification - Updated subsection to align with standard Security Policy language.
- (83) 10.8.33.4.19.4 SI-07 Software, Firmware, and Information Integrity - Updated subsection to align with standard Security Policy language.
- (84) 10.8.33.4.19.5 SI-10 Information Input Validation - Updated subsection to align with standard Security Policy language.
- (85) 10.8.33.4.19.6 SI-11 Error Handling - Updated subsection to align with standard Security Policy language.
- (86) 10.8.33.4.19.7 SI-16 Memory Protection - Updated subsection to align with standard Security Policy language.
- (87) 10.8.33.4.20 SR – Supply Chain Risk Management - Updated subsection to align with standard Security Policy language.
- (88) Exhibit 10.8.33-1 Security Requirements Checklists - Updated subsection to align with standard Security Policy language.
- (89) Exhibit 10.8.33-2 Terms and Acronyms - Removed Enterprise Life Cycle (ELC) to align with standard Security Policy language.
- (90) Exhibit 10.8.33-3 Related Resources - Updated subsection with new SRG version.

EFFECT ON OTHER DOCUMENTS

IRM 10.8.33 dated November 03, 2023, is superseded. This IRM supplements IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance; and IRM 10.8.2, Information Technology (IT) Security, IT Security Roles and Responsibilities; and IRM 10.8.24, Information Technology (IT) Security, Cloud Computing Security Policy.

AUDIENCE

IRM 10.8.33 must be distributed to all personnel responsible for implementing, managing, monitoring, and ensuring compliance with mainframe security controls to protect the confidentiality, integrity and availability of IRS systems and data. This policy applies to all employees, contractors and vendors of the IRS.

Kaschit Pandya
Acting, Chief Information Officer

Mainframe System Security Policy

10.8.33.1 Program Scope and Objectives

- #### 10.8.33.2 Risk Acceptance and Risk-Based Decisions (RBD)

10.8.33.3.1	System Programmer
10.8.33.3.2	Resource Access Control Facility (RACF) System Administrator (RSA)
10.8.33.3.3	Resource Access Control Facility (RACF) User and Group Administrator
10.8.33.3.4	Resource Access Control Facility (RACF) System and Group Auditor

#

[illegible]

#

Exhibits

- 10.8.33-1 Security Requirements Checklists
- 10.8.33-2 Terms and Acronyms
- 10.8.33-3 Related Resources

10.8.33.1
(08-14-2025)
Program Scope and Objectives

- (1) **Overview:** This IRM lays the foundation to implement and manage security controls and guidance for the use of mainframe systems within the IRS.
 - a. This IRM is subordinate to IRM 10.8.1, *Information Technology (IT) Security, Security Policy*, and augments the existing requirements identified within IRM 10.8.1, as they relate to IRS mainframe products for on-premises systems, including on-premises cloud deployments.
 - b. This IRM is subordinate to IRM 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy*, and augments the existing requirements identified within IRM 10.8.24, as they relate to IRS mainframe products for off-premises cloud deployments.
- (2) **Program Purpose:** Develop and publish security policies to protect the IRS against potential security threats, risks, and vulnerabilities to ensure compliance with federal mandates and legislation.
- (3) **Audience:** The provisions within this IRM apply to:
 - a. All offices and business, operating, and functional units within the IRS.
 - b. IRS personnel and organizations having contractual arrangements with the IRS, including employees, contractors, vendors and outsourcing providers, which use or operate systems that store, process, or transmit IRS Information or connect to an IRS network or system.
 - c. All NIST impact-level baselines (i.e., Low, Moderate, High), unless a requirement indicates differently.
- (4) **Policy Owner:** Chief Information Officer (CIO)
- (5) **Program Owner:** Cybersecurity, Cybersecurity Threat Response and Remediation.
- (6) **Program Goals:** To protect the confidentiality, integrity, and availability of IRS information and information systems.

10.8.33.1.1
(08-14-2025)
Background

- (1) This IRM defines the security controls for the protection of IRS mainframe systems.
- (2) FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, mandates the use of NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, as an initial set of baseline security controls for the creation of agency IT security policy.
- (3) IRM 10.8.33 is part of the IRM 10.8 Information Technology (IT) Security series for IRS IT Cybersecurity.

10.8.33.1.2
(08-14-2025)
Authority

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

10.8.33.1.3
(08-14-2025)

**Roles and
Responsibilities**

- (1) The IRS must implement security roles in accordance with federal laws and IT security guidelines (e.g., FISMA, NIST, OMB) that are appropriate for their specific operations and missions. The roles and responsibilities are defined in IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*.
- (2) The supplemental roles and responsibilities specific to the implementation of IBM Mainframe Product Systems are located in IRM 10.8.33.3, IT Roles and Responsibilities, subsection of this IRM.

10.8.33.1.4
(08-14-2025)

**Program Management
and Review**

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

10.8.33.1.5
(08-14-2025)

Program Controls

- (1) Each IRM in the 10.8 series is assigned an author who reviews the IRM to ensure accuracy. The IRM authors continuously monitor federal guidance (e.g., OMB, CISA, NIST, Defense Information Systems Agency (DISA)) for potential revisions to security policies and security requirements checklists. Revisions to security policies and checklists are reviewed by the security policy team, in collaboration with applicable stakeholders, for potential impact to the IRS operational environment.
- (2) Security policy provides a report identifying security policies and security requirements checklists that have recently been revised or are in the revision process.
- (3) This IRM applies to all IRS information and systems, which store, process, or transmit IRS information or connect to an IRS network or system. For systems that store, process, or transmit classified national security information, refer to IRM 10.9.1, *Classified National Security Information (CNSI)*, for additional guidance for protecting classified information.
- (4) This IRM establishes the minimum baseline security policy and requirements for all IRS mainframe systems in order to:

- a. Protect the critical infrastructure and assets of the IRS against attacks that exploit IRS assets.
- b. Prevent unauthorized access to IRS assets.
- c. Enable IRS IT computing environments to meet the security requirements of this IRM and support the business needs of the organization.

- (5) In the event there is a discrepancy between this IRM and IRM 10.8.1, IRM 10.8.1 has precedence, unless the security controls or requirements in this IRM are more restrictive.

10.8.33.1.6
(08-14-2025)

Terms and Acronyms

- (1) Refer to Exhibit 10.8.33-2 Terms and Acronyms for a list of terms, acronyms, and definitions.

10.8.33.1.7
(08-14-2025)

Related Resources

- (1) In addition to federal guidance cited throughout this IRM, this IRM incorporates IRS-defined policy, regulatory and mandatory guidance, and policy from other sources. Refer to Exhibit 10.8.33-3, Related Resources for a list of related resources and references.

10.8.33.2
(08-14-2025)

Risk Acceptance and Risk-Based Decisions (RBD)

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

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

- (3) Refer to *IRM 10.8.1* for additional guidance on risk acceptance and RBDs.

10.8.33.3
(08-14-2025)

Mainframe Roles and Responsibilities

- (1) The following supplemental roles and responsibilities are specific to the implementation of IRS mainframe systems.

Note: No specific roles are listed within this IRM for Unisys.

- (2) For the purpose of this IRM, the table below is a correlation between the IBM Mainframe Product Roles referred to within the Vanguard Configuration Manager (VCM) to a corresponding IRS Role defined either within this IRM or IRM 10.8.2.

Note: These VCM roles are defined in the DISA (Defense Information Systems Agency) STIGs (Security Technical Implementation Guides).

IBM Mainframe Produce Role	IRS Role
System Programmer	System Administrator (SA)
Security Administrator	Resource Access Control Facility (RACF) System Administrator (RSA)

IBM Mainframe Produce Role	IRS Role
Information System Security Manager (ISSM)	<i>System Security Officer (SSO) (formerly known as Information System Security Officer (ISSO)).</i>
Information Assurance Officer (IAO)	SSO
Auditor	Security Specialist (SecSpec)
	SSO
Audit Personnel	SecSpec
	SSO
	RACF System Auditor
	RACF Group Auditor

10.8.33.3.1
(08-14-2025)
System Programmer

- (1) A System Programmer in the z/OS Support Section is responsible for installing and updating the RACF security product on the IBM Mainframes as part of regularly scheduled z/OS upgrades or maintenance or both.

10.8.33.3.2
(08-14-2025)
**Resource Access
Control Facility (RACF)
System Administrator
(RSA)**

- (1) A RACF System Administrator (RSA) is in the system administrator role, with a subset of the *generic system administrator responsibilities*.
- (2) The RSA maintains the security product and must:
 - a. Identify and maintain security system level resources.
 - b. Perform the initial setup of the RACF system.
 - c. Have overall responsibility for all security matters within RACF.
- (3) The RSA, in coordination with the operating system program developer(s), *systems operations staff*, must identify and install all critical system resources, components, data sets, and connections which are to be protected by RACF. The RSA must:
 - a. Implement the RACF setup for system datasets, resources profiles, and datasets associated with those resources, and is responsible for information as to its setup.
 - b. Determine the owner(s) of the aforementioned resources.
- (4) The RSA determines the appropriate access control levels and security monitoring requirements for system resources. The RSA coordinates with system programmers and security stakeholders to ensure the following are accomplished:
 - a. Configure RACF and related system security parameters in accordance with documented security standards, including applicable IRMs and system life cycle documentation.
 - b. Maintain documentation related to RACF-protected resources, including datasets, resource classes, and access control definitions.

- c. Provide oversight on the security implications of system startup, shutdown, and recovery processes, as they pertain to RACF-controlled resources.
- d. Coordinate with system and operations personnel to ensure security requirements are integrated into system backup, recovery, and contingency processes.
- e. Collaborate with operations and monitoring teams to support audit trail integrity and alerting on unauthorized access or anomalous security activity

Note: Items such as system hardware configuration, performance monitoring, and application management fall outside the scope of direct RSA responsibility, but the RSA may be consulted or provide input on access control implications associated with those activities.

- (5) The RACF System Administrator must participate in contingency planning and contingency plan testing activities, as specified by *IRM 10.8.1, IRM 10.8.13, Business Impact Analysis (BIA) Security Policy, IRM 10.8.60, IT Service Continuity Management (ITSCM) Policy and Guidance* and *IRM 10.8.62, Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Process*.

10.8.33.3.3
(08-14-2025)

**Resource Access
Control Facility (RACF)
User and Group
Administrator**

- (1) The RACF user administrator (RUA) performs user account administration in collaboration with the RACF system administrator (RSA). The RUA must:
 - a. Perform the initial setup of user and group access profiles.
 - b. Establish and maintain least privilege user roles and the role based access matrix outlining the access for each role.
 - c. Ensure that users are established using an access control system (e.g., *Business Entitlement Access Request System (BEARS)* or once required approvals are satisfied.
 - d. Perform application management activities.
- (2) The RACF group administrator functions within the security administrator role and performs user account administration at the group level. Distributed security administration is allowed, but not required.
 - a. RACF group administrators must have overall responsibility for all security matters within the scope of their group.

10.8.33.3.4
(08-14-2025)

**Resource Access
Control Facility (RACF)
System and Group
Auditor**

- (1) The RACF system or group auditor, functions within the security specialist role. Refer to the *security specialist (SecSpec) section within IRM 10.8.2* for general requirements.
 - a. Independent auditor(s) are assigned at the system or user group level; to provide a system of checks and balances; and
 - b. Independent auditor(s) must review user activities in areas where they perform no activities relating to administration, programming, or security administration.

#

#

#

#

#

#

#

#####

#####

#

#

[illegible]

[illegible]

[illegible]

#

#

#####

[illegible]

#####

#

#

[illegible]

#####

#

#####

[illegible]

#####

[illegible]

#

#

#

#

#

#

#

#

#

#

Exhibit 10.8.33-1 (08-14-2025)
Security Requirements Checklists

1. Security Requirements Checklists (if accompanying this IRM) serve as the secure configuration baseline and are developed in accordance with NIST Special Publication (SP) 800-70, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*.

- a. IRMs with accompanying checklists contain a checklist with general security requirements (e.g., DISA, Security Requirements Guide (SRG)), as well as checklists with platform or technology specific security requirements (e.g., Security Technical Implementation Guides (STIGs), Center for Internet Security (CIS) Benchmarks). In the event a platform or technology specific security checklist is not available, the general security requirements checklist must be used (e.g., Database (General), Operating System (General), Router (General)).
- b. Security requirements checklists must be used in addition to the IRS and Treasury defined requirements within the IRM.
- c. In the event of a conflict between a checklist and this IRM, excluding Treasury-defined requirements, the requirement(s) from the checklist takes precedence.

Note: The order of precedence only applies when there is a conflict between the IRM and one of its accompanying checklists and does not apply when there is a discrepancy with IRM 10.8.1.

- d. Implementation of Security Requirements Checklists is required, per CM-06.

#

3. Security requirements checklists are effective immediately. Vulnerabilities must be remediated in accordance with IRM 10.8.50, Information Technology (IT) Security, Enterprise Incident, Vulnerability, and Security Patch Management, remediation timelines table. The source's publication date can be found in the external reference row of the checklist. (Typically row 10)

4. Checklists for technologies identified as *Beyond Sunset* or *Removed by Enterprise Architecture (EA) Enterprise Standards Profile (ESP)* will not receive further updates. These checklists will be removed from the active checklist and moved to an *Archive* folder during the next checklist update cycle.

5. Evaluate system configurations and implement controls while protecting system functionality.

Exhibit 10.8.33-2 (02-24-2022)**Terms and Acronyms**

Terms and Acronyms	
Access control	The process of granting or denying specific requests to: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).
Assessment, Authorization, and Monitoring	(Formerly known as Security Assessment & Authorization (SA&A)) – Assessment, Authorization, and Monitoring (AA&M) is a testing and evaluation process with a resulting authorization based on the NIST Special Publication 800-series; specifically, SP 800-37 and SP 800-53. The new AA&M process and terminology replaces the Security Assessment & Authorization process, which were based on earlier NIST SP 800 guidance.
Authorizing Official (AO)	Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Accountable for the security risks associated with information system operations. Previously known as the Designated Approving Authority.
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's identity.
BEARS	<i>Business Entitlement Access Request System</i>
CSIRC	<i>Computer Security Incident Response Center</i>
DISA	<i>Defense Information Systems Agency</i>
EA (<i>Enterprise Architecture</i>)	The description of an enterprise's entire set of systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture.
ESP (<i>Enterprise Standards Profile</i>)	The authoritative repository for IRS approved products and standards. The ESP allows project owners and other stakeholders to select pre-approved technology products and standards.
FIRECALL UserID	A privileged user-id used only in emergency situations when privileged users are not available.
FIPS	Federal Information Processing Standards
<i>FISMA</i>	The E-Government Act of 2002 (P.L. 107-347) Title III, Federal Information Security Modernization Act of 2014
IPL	Initial Program Load
IRM	<i>Internal Revenue Manual</i>
IT	Information Technology

Exhibit 10.8.33-2 (Cont. 1) (02-24-2022)

Terms and Acronyms

Legacy System	A system is designated as legacy if it measurably obstructs IRS mission-critical outcomes by: [CIO: IRS-defined] • Limiting functionality essential to key operations or business objectives; • Increasing operational risk (e.g., security vulnerabilities, system failures); or • Degrading performance (e.g., causing delays or inefficiencies). Legacy status is determined by impact on the agency's evolving mission requirements, regardless of system age, programming language, or vendor support status.
NIST	<i>National Institute of Standards and Technology</i>
OneSDLC	<i>One Solution Delivery Lifecycle</i> , a delivery model that positions our IT teams to respond to emergent needs as quickly as possible by encouraging agility with appropriate guardrails for quality and security.
Password	A string of characters known to the computer system and a user, who must specify it to gain full or limited access to a system and to the data stored therein.
PIV	Personal Identity Verification
RBD (Risk Based Decision Process)	Decision made by individuals responsible for ensuring security by utilizing a wide variety of information, analysis, assessment, and processes. The type of information taken into account when making a risk-based decision may change based on life cycle phase and decision is made taking entire posture of the system into account. Some examples of information taken into account are formal and informal risk assessments, risk analysis, assessments, recommended risk mitigation strategies, and business impact. (This list is not intended to be all inclusive).
Security	The protection of resources from damage or misuse and the protection of data against accidental or intentional disclosure to unauthorized persons or unauthorized modifications or destruction.
SMF	System Management Facility
SMP/E	System Modification Program/Extended
SSP	System Security Plan
STIG	<i>Security Technical Implementation Guides</i>

Exhibit 10.8.33-2 (Cont. 2) (02-24-2022)**Terms and Acronyms**

Subsystem	A software entity, with an addressing environment and a set of security attributes that protect the rest of the system by a combination of hardware and software mechanisms that control access. The main types of subsystems are: protected (both object module and common bank) and chameleon/library common bank. A protected subsystem is typically a subject acting on behalf of a user. Each action performed on behalf of the user (for example, execution of a task, transaction, or ECL statement) is a process. When a process executes within the address space of a subsystem, it acts with the subsystem's security attributes and can access objects as defined by that subsystem's security attributes. When a process references (calls) the address space of another subsystem, the operating system treats the referenced subsystem as an object and enforces security policy for access to that object. If security validations pass, a subsystem transition is allowed and the calling subsystem can enter the referenced subsystem to access.
TT&E	Test, Training, and Exercise
VCM	<i>Vanguard Configuration Manager</i>

Exhibit 10.8.33-3 (08-14-2025)**Related Resources****IRS Publications**

- IRM 1.15.1 – *Records and Information Management, The Records and Information Management Program*
- IRM 1.15.2 – *Records and Information Management, Types of Records and their Life Cycles*
- IRM 10.8.1 – *Information Technology (IT) Security, Policy and Guidance*
- IRM 10.8.2 – *Information Technology (IT) Security, IT Security Roles and Responsibilities*
- IRM 10.8.26 – *Information Technology (IT) Security, Government Furnished and Personally Owned Mobile Device Security Policy*
- IRM 10.8.50 – *Information Technology (IT) Security, Servicewide Security Patch Management*
- IRM 10.8.52 – *Information Technology (IT) Security, IRS Public Key Infrastructure (PKI) X.509 Certificate Policy*
- IRM 10.8.60 – *Information Technology (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance*
- IRM 10.8.62 – *Information Technology (IT) Security, Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training and Exercise (TT&E) Program*

Department of the Treasury Publications

- Department of the Treasury TD P 85–01, Version 3.1.3 *Treasury Information Technology (IT) Security Program*, February 28, 2022

National Institute of Standards and Technology (NIST) Publications

- NIST FIPS 199: *Standards for Security Categorization of Federal Information and Information Systems*
- NIST FIPS 200: *Minimum Security Requirements for Federal Information and Information Systems*
- 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 800-53 Rev 5.1.1, *Security and Privacy Controls for Information Systems and Organizations*, November 7, 2023
- NIST SP 800-53A Rev 5.1.1, *Assessing Security and Privacy Controls in Information Systems and Organizations*, November 7, 2023

Defense Information Systems Agency (DISA)

- DISA: Defense Information Systems Agency. Mainframe Product SRG, V3R3, 2025-01-30
- Security Technical Implementation Guides (STIGS) are used as a basis for producing *IRS Security Requirements Checklists*. The security checklists are updated as DISA releases updated guidance and are posted on the IRS IT Cybersecurity Policy SharePoint site. The DISA version and release for each guide is contained within each checklist. Refer to the Security Requirement Checklists for additional information.
- DISA Security Requirements Guides and Security Technical Implementation Guides are available at: <https://public.cyber.mil/stigs/>

Other Publications

Committee on National Security Systems (CNSS) Glossary, Committee on National Security Systems Instruction (CNSSI) No. 4009

