



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.6

SEPTEMBER 12, 2025

EFFECTIVE DATE

(09-12-2025)

PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.8.6, *Information Technology (IT) Security, Application Security and Development*.

MATERIAL CHANGES

- (1) IRM updated to align with IRM 1.11.2, *Internal Management Documents System, Internal Revenue Manual (IRM) Process Internal Controls*.
- (2) Entire IRM, added the leading zero to the control numbers to align with NIST.
- (3) Entire IRM, requirements written with “shall” verbiage updated to “must” to align with industry writing best practices.
- (4) Entire IRM, added reference to IRM 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy* for further guidance on specific controls.
- (5) Entire IRM, updated the citations to align with the Security Policy Boilerplate.
- (6) IRM 10.8.6, IRM Part Title - updated to include Artificial Intelligence.
- (7) IRM 10.8.6, Audience - updated to align with Security Policy Boilerplate.
- (8) IRM 10.8.6.1, Program Scope and Objectives - updated to align with Security Policy Boilerplate.
- (9) IRM 10.8.6.1.1, Background - updated to align with Security Policy Boilerplate.
- (10) IRM 10.8.6.1.2, Authority - updated to align with Security Policy Boilerplate.
- (11) IRM 10.8.6.1.3, Roles and Responsibilities - updated to align with Security Policy Boilerplate.
- (12) IRM 10.8.6.1.4, Program Management and Review - updated to align with Security Policy Boilerplate.
- (13) IRM 10.8.6.1.5, Program Controls - updated to align with Security Policy Boilerplate.
- (14) IRM 10.8.6.1.6, Terms and Acronyms - updated to align with Security Policy Boilerplate.
- (15) IRM 10.8.6.1.7, Related Resources - updated to align with Security Policy Boilerplate.
- (16) IRM 10.8.6, Risk Acceptance and Risk-Based Decisions - updated URL for accurate FISMA Doc Library location and other language to align with the Security Policy Boilerplate.
- (17) IRM 10.8.6.4.1.1, AC-02 Account Management - moved item 2 to IA-02 item 8 and added item 10 from IA-04.
- (18) IRM 10.8.6.4.1.6, AC-08 System Use Notification - updated the name of the display banner to Standard Mandatory IRS System Use Notification Banner.
- (19) IRM 10.8.6.4.3.1, AU-03 Content of Audit Records - moved item 12 to AU-06 item 4.

- (20) IRM 10.8.6.4.5.3, CM-05 Access Restrictions for Change - moved item 3 to CM-14 Signed Components per NIST.
- (21) IRM 10.8.6.4.5.5, CM-07 Least Functionality - item 6 added to align with DISA STIGs.
- (22) IRM 10.8.6.4.5.8, Created new subsection - CM-14 Signed Components.
- (23) IRM 10.8.6.4.7.3, IA-04 Identifier Management - Removed to align with DISA SRG.
- (24) IRM 10.8.6.4.13, Created new subsection - PM - Program Management.
- (25) IRM 10.8.6.4.14, Created new subsection - PM-14 Testing, Training, and Monitoring.
- (26) IRM 10.8.6.4.18.3, SA-10 Developer Configuration Management - Added item 2 from SA-11.
- (27) Exhibit 10.8.6-4, Terms and Acronyms - updated table to include items referenced throughout the IRM.
- (28) Exhibit 10.8.6-5, Related Resources - updated items to include new IRMs and publications referenced throughout the IRM.
- (29) Editorial changes (including grammar, spelling, URL links, and minor clarifications) were made throughout the IRM.

EFFECT ON OTHER DOCUMENTS

IRM 10.8.6 dated November 08, 2023, is superseded. This IRM supplements IRM 10.8.1, *Information Technology (IT) Security, Security Policy and Guidance*, and IRM 10.8.2, *Information Technology Security Roles and Responsibilities*.

AUDIENCE

IRM 10.8.6 must be distributed to all personnel responsible for ensuring adequate security for developing, overseeing, managing, and implementing application security for IRS information and information systems. This IRM is not intended as a primer for novice program developers or programmers. The reader is expected to be well-versed and experienced in general systems engineering, software development, and software testing practices. The reader should have a thorough understanding of technology involved in secure application development and in-depth experience with the development of software applications and web services. The Application Security and Development Policy will consist of, but will not be limited to, agency-defined requirements, authoritative guidance, legislative mandates, and national standards. This IRM applies to all employees, contractors, and vendors of the IRS.

Kaschit Pandya
Acting, Chief Information Officer

10.8.6

Application Security and Development

Table of Contents

10.8.6.1 Program Scope and Objectives

- 10.8.6.1.1 Background
- 10.8.6.1.2 Authority
- 10.8.6.1.3 Roles and Responsibilities
- 10.8.6.1.4 Program Management and Review
- 10.8.6.1.5 Program Controls
- 10.8.6.1.6 Terms and Acronyms
- 10.8.6.1.7 Related Resources

10.8.6.2 Risk Acceptance and Risk-Based Decisions

10.8.6.3 IT Security Controls

- 10.8.6.3.1 AC - Access Control
 - 10.8.6.3.1.1 AC-02 Account Management
 - 10.8.6.3.1.2 AC-03 Access Enforcement
 - 10.8.6.3.1.3 AC-04 Information Flow Enforcement
 - 10.8.6.3.1.4 AC-06 Least Privilege
 - 10.8.6.3.1.5 AC-07 Unsuccessful Logon Attempts
 - 10.8.6.3.1.6 AC-08 System-Use Notification
 - 10.8.6.3.1.7 AC-09 Previous Logon (Access) Notification
 - 10.8.6.3.1.8 AC-10 Concurrent Session Control
 - 10.8.6.3.1.9 AC-12 Session Termination
 - 10.8.6.3.1.10 AC-16 Security and Privacy Attributes
 - 10.8.6.3.1.11 AC-17 Remote Access
 - 10.8.6.3.1.12 AC-23 Data Mining Protection
- 10.8.6.3.2 AT - Awareness and Training
 - 10.8.6.3.2.1 AT-03 Role-Based Training
- 10.8.6.3.3 AU - Audit and Accountability
 - 10.8.6.3.3.1 AU-03 Content of Audit Records
 - 10.8.6.3.3.2 AU-04 Audit Log Storage Capacity
 - 10.8.6.3.3.3 AU-05 Response to Audit Logging Process Failures
 - 10.8.6.3.3.4 AU-06 Audit Record Review, Analysis, and Reporting
 - 10.8.6.3.3.5 AU-07 Audit Record Reduction and Report Generation
 - 10.8.6.3.3.6 AU-08 Time Stamps
 - 10.8.6.3.3.7 AU-09 Protection of Audit Information
 - 10.8.6.3.3.8 AU-10 Non-Repudiation
 - 10.8.6.3.3.9 AU-11 Audit Record Retention

- 10.8.6.3.3.10 AU-12 Audit Record Generation
- 10.8.6.3.3.11 AU-14 Session Audit
- 10.8.6.3.4 CA - Assessment, Authorization, and Monitoring
 - 10.8.6.3.4.1 CA-2 Control Assessments
- 10.8.6.3.5 CM - Configuration Management
 - 10.8.6.3.5.1 CM-03 Configuration Change Controls
 - 10.8.6.3.5.2 CM-04 Impact Analyses
 - 10.8.6.3.5.3 CM-05 Access Restrictions for Change
 - 10.8.6.3.5.4 CM-06 Configuration Settings
 - 10.8.6.3.5.5 CM-07 Least Functionality
 - 10.8.6.3.5.6 CM-09 Configuration Management Plan
 - 10.8.6.3.5.7 CM-11 User-Installed Software
 - 10.8.6.3.5.8 CM-14 Signed Components
- 10.8.6.3.6 CP Contingency Planning
 - 10.8.6.3.6.1 CP-02 Contingency Plan
 - 10.8.6.3.6.2 CP-09 System Backup
 - 10.8.6.3.6.3 CP-10 Information System Recovery and Reconstitution
 - 10.8.6.3.6.4 CP-11 Alternate Communications Protocols
- 10.8.6.3.7 IA - Identification and Authentication
 - 10.8.6.3.7.1 IA-02 Identification and Authentication (Organizational Users)
 - 10.8.6.3.7.2 IA-03 Device Identification and Authentication
 - 10.8.6.3.7.3 IA-05 Authenticator Management
 - 10.8.6.3.7.4 IA-06 Authenticator Feedback
 - 10.8.6.3.7.5 IA-07 Cryptographic Module Authentication
 - 10.8.6.3.7.6 IA-08 Identification and Authentication (Non-Organizational Users)
 - 10.8.6.3.7.7 IA-11 Re-authentication
- 10.8.6.3.8 IR - Incident Response
- 10.8.6.3.9 MA - Maintenance
 - 10.8.6.3.9.1 MA-4 Non-Local Maintenance
- 10.8.6.3.10 MP - Media Protection
 - 10.8.6.3.10.1 MP-03 Media Marking
- 10.8.6.3.11 PE - Physical and Environmental Protection
- 10.8.6.3.12 PL - Planning
- 10.8.6.3.13 PM - Program Management
- 10.8.6.3.14 PM - 14 Testing, Training, and Monitoring
- 10.8.6.3.15 PS - Personnel Security
- 10.8.6.3.16 PT - Personally Identifiable Information Processing and Transparency
- 10.8.6.3.17 RA - Risk Assessment
- 10.8.6.3.18 SA - System and Services Acquisition

- 10.8.6.3.18.1 SA-04 Acquisition Process
- 10.8.6.3.18.2 SA-05 System Documentation
- 10.8.6.3.18.3 SA-10 Developer Configuration Management
- 10.8.6.3.18.4 SA-11 Developer Testing and Evaluation
- 10.8.6.3.18.5 SA-15 Development Process, Standards, and Tools
- 10.8.6.3.18.6 SA-22 Unsupported System Components
- 10.8.6.3.19 SC - System and Communications Protection
 - 10.8.6.3.19.1 SC-02 Separation of System and User Functionality
 - 10.8.6.3.19.2 SC-03 Security Function Isolation
 - 10.8.6.3.19.3 SC-04 Information in Shared System Resources
 - 10.8.6.3.19.4 SC-05 Denial-of-Service Protection
 - 10.8.6.3.19.5 SC-07 Boundary Protection
 - 10.8.6.3.19.6 SC-08 Transmission Confidentiality and Integrity
 - 10.8.6.3.19.7 SC-10 Network Disconnect
 - 10.8.6.3.19.8 SC-13 Cryptographic Protection
 - 10.8.6.3.19.9 SC-17 PKI Certificate Validation
 - 10.8.6.3.19.10 SC-18 Mobile Code
 - 10.8.6.3.19.11 SC-23 Session Authenticity
 - 10.8.6.3.19.12 SC-24 Fail in Known State
 - 10.8.6.3.19.13 SC-28 Protection of Information at Rest
 - 10.8.6.3.19.14 SC-39 Process Isolation
- 10.8.6.3.20 SI - System and Information Integrity
 - 10.8.6.3.20.1 SI-02 Flaw Remediation
 - 10.8.6.3.20.2 SI-04 System Monitoring
 - 10.8.6.3.20.3 SI-05 Security Alerts, Advisories, and Directives
 - 10.8.6.3.20.4 SI-06 Security and Privacy Function Verification
 - 10.8.6.3.20.5 SI-10 Information Input Validation
 - 10.8.6.3.20.6 SI-11 Error Handling
 - 10.8.6.3.20.7 SI-16 Memory Protection
- 10.8.6.3.21 SR - Supply Chain Risk Management

Exhibits

#

10.8.6-5 Related Resources

10.8.6.1
(09-12-2025)
Program Scope and Objectives

- (1) **Overview:** This IRM lays the foundation to implement and manage security controls and guidance for the use of applications and application development within the Internal Revenue Service (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 applications and application development 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 applications and application development for off-premises cloud deployments.
- (2) **Program Purpose:** Develop and publish security policies to protect the IRS against potential security threats, risks, and vulnerabilities and to ensure compliance with federal mandates and legislation.
- (3) **Audience:** The provisions within this IRM apply to:
 - a. All offices, business units, operating units, 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.

10.8.6.1.1
(09-12-2025)
Background

- (1) This IRM establishes comprehensive Information Technology (IT) security policies and provides guidance to all IRS organizations developing or modifying applications code for use within the IRS. This IRM must be used in conjunction with coding guidelines found in:
 - a. IRM 2.5.3, *Systems Development, Programming and Source Code Standards*
 - b. Open Web Application Security Project (OWASP) website at *OWASP*
- (2) IRM 10.8.6 is part of the IRM 10.8 Information Technology (IT) Security series IT Cybersecurity.

10.8.6.1.2
(09-12-2025)
Authority

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

10.8.6.1.3
(09-12-2025)

**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.

10.8.6.1.4
(09-12-2025)

**Program Management
and Review**

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

10.8.6.1.5
(09-12-2025)

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 information systems, which include IRS production, development, test and contractor systems. 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 on protecting classified information.
- (4) This IRM establishes the minimum baseline security policy and requirements for all IRS application security and development.
- (5) To define a security policy baseline for IRS systems, risk impact level and overlay designators may be assigned to a requirement and appear at the end of it in brackets, which will help identify if the requirement applies to a system.

Note: Note: When there are sub-parts (e.g., a, b, i, ii) to a primary requirement and a designator is indicated for the primary requirement but not the sub-parts, the designator indicated for the primary applies to the sub-parts as well.

- a. A FIPS 199 security impact-level designator may be assigned to each requirement. This designator indicates that the requirement only applies to systems categorized at that FIPS 199 impact-level, thus establishing a baseline for each level. Example: A requirement with an indicator of “H” indicates the requirement only applies to systems categorized as FIPS 199 impact-level HIGH.
- b. Controls designated as program-level controls are identified with an “O” indicator. The following apply for controls designated as program-level requirements:
 - i. Implemented at the organization level; ii. Not directed at individual systems; iii. Independent of any system impact level; and iv. Not associated with security control baselines.

Note: This indicator is in place of the FIPS 199 designators previously defined.

- c. Controls identified as part of the privacy control baseline are identified with a “(P)” indicator.
- d. Controls designated as a critical infrastructure protection (CIP) overlay control are identified with a “CIP” indicator. Systems designated as cyber critical infrastructure assets must implement controls identified as CIP overlay controls.

Note: The critical infrastructure control overlay must be applied to all components within the designated cyber critical infrastructure asset system’s security boundary.

Note: Information systems normally consist of components (servers, routers, batch processing routines, mainframes, etc.) that when combined allow the overall system to perform its intended function. The intent is to increase the trustworthiness and resiliency of the overall system by applying the control overlay to all the components of the designated system, where applicable. It is understood that security controls are applicable only to information system components that provide or support the capability addressed by the controls. Document the implementation accordingly.

Note: CIP overlay controls may be tailored as long as the following criteria is met:

The AO, in coordination with the system and organizational officials determines that a control in the overlay is not to be implemented (also referred to as “tailoring-out”) on a designated cyber critical infrastructure asset; and the associated documentation for this risk-based decision not to implement must be submitted to the Department Cyber CIP Program Manager and the Departmental CISO for review and approval.

- e. Controls designated as a high value asset (HVA) overlay control are identified with an “HVA” indicator. Systems designated as an HVA must implement security controls identified as HVA overlay controls.

10.8 Information Technology (IT) Security

Note: The PM and PT family of controls in the CISA government-wide baseline are excluded from the IRM 10.8.24 baseline.

Note: The HVA control overlay is defined by CISA.

- f. Controls designated as a critical software (CSW) overlay control are identified with a “CSW” indicator. Software designated as critical software and platforms hosting critical software must implement security controls identified as CSW overlay controls. [NIST: NIST Security Measures for EO-Critical Software Use]

Note: Security controls identified as CSW align with the security measures defined by NIST.

Indicator	Applicability
(L)	Applies to systems categorized as FIPS 199
(M)	Applies to systems categorized as FIPS 199 Impact-level MEDIUM
(H)	Applies to systems categorized as FIPS 199 Impact-level HIGH
(CIP)	Overlay - Applies to systems identified as Cyber Critical Infrastructure
(HVA)	Overlay - Applies to systems identified as Cyber High Value Assets
(P)	Privacy Baseline Controls
(O)	Program-level Controls (i.e., Program Management (PM))
(CSW)	Overlay - Applies to software identified as Critical Software and systems hosting Critical Software

- (6) In an effort to provide an authoritative source for a requirement, a citation may be provided at the end of a requirement within brackets. If a NIST impact-level baseline (i.e., L, M, H) or control overlay (i.e., CIP, HVA) applies to a requirement, they would be provided at the end of a requirement within brackets also. The citations, baselines, and overlays are broken down into two parts: the first part is a generic identifier, such as NIST, DISA, Baseline, Overlay, etc.; the second part identifies the specific source, baseline or overlay that applies. Below are some examples of how a citation, baseline, and or overlay may appear for a particular type of source:

- a. Citations

Citation	Example
NIST Control	NIST Control [NIST: SP 800-53, AC-02]
Treasury Control	Treasury Control [Treasury: TD P 85-01, AC-03_T.002]
Treasury Publication	Treasury Publication [Treasury: TD P 15-71]
Federal	Federal [Federal: P.L. 113-283]
U.S. Code	U.S. Code [USC: 44 USC 3551]
Executive Order	Executive Order [EO: 14028]
OMB Memorandum	OMB Memorandum [OMB: M-22-09]
CISA Directive	CISA [CISA: BOD-23-01]
NIST Publication	[NIST: SP 800-40]
DISA STIG or SRG	[DISA: SRG-APP-000516-NDM-000350]
IRS Defined with no business unit source	[IRS: IRS-defined]
IRS Defined with CSIRC as source	[CSIRC: IRS-defined]

b. Baseline

NIST Baseline	[Baseline: P, L, M, H, O]
---------------	---------------------------

c. Overlay

Control Overlay	[Overlay: CIP, HVA, CSW]
-----------------	--------------------------

Example: How a source, baseline, overlay could appear at the end of a requirement: [NIST: SP 800-53, SA-15 | Baseline: M, H | Overlay: HVA].

Note: Citations correlate to a reference listed in Exhibit 10.8.63-3, Related Resources within this IRM.

Note: The citation, baseline, and overlay are formatted to be simple enough for manual identification while being distinct enough for automated detection and extraction. This is intended to allow for easy identification and parsing by applications (manual or automated), using distinct patterns.

- (7) 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.

- (8) 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 or requirements in this policy are more restrictive.

10.8.6.1.6
(09-12-2025)

Terms and Acronyms

- (1) Refer to Exhibit # 10.8.6-4 #, **Terms and Acronyms**, for a list of terms, acronyms, and definitions.

10.8.6.1.7
(09-12-2025)

Related Resources

- (1) In addition to federal guidance cited throughout this IRM, this IRM incorporates IRS-defined policy, regulatory and mandated guidance, and policy from other sources. Refer to Exhibit 10.8.6-5, **Related Resources**, for a list of related resources and references.

10.8.6.2
(09-12-2025)

Risk Acceptance and Risk-Based Decisions

- (1) Any exception to this IRM requires the 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 Standard Operating Procedures (SOP).

Note: Users can access the 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.

10.8.6.3
(09-12-2025)

IT Security Controls

- (1) The security controls in this IRM supplement the requirements defined in IRM 10.8.1.

Note: Refer to IRM 10.8.1 for security control families and security controls not addressed within this IRM.

- (2) It is acceptable to configure settings to be more restrictive than those defined in this IRM.
- (3) To configure less restrictive requirements requires a risk-based decision. Refer to the Risk Acceptance and Risk-Based Decisions (RBD) subsection within this IRM for additional guidance.

10.8.6.3.1
(09-12-2025)

AC - Access Control

- (1) In addition to the Access Control guidance defined within this IRM, the following controls must be implemented in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable):

- AC-01 Policy and Procedures
- AC-05 Separation of Duties
- AC-11 Device Lock
- AC-14 Permitted Actions Without Identification and Authentication
- AC-18 Wireless Access
- AC-19 Access Control for Mobile Devices
- AC-20 Use of External Systems
- AC-21 Information Sharing
- AC-22 Publicly Accessible Content
- AC-24 Access Control Decisions
- AC-25 Reference Monitor

10.8.6.3.1.1
(09-12-2025)
**AC-02 Account
Management**

- (1) The application must provide automated mechanisms for supporting account management functions. [DISA: APSC-DV-000280]
- (2) The application must automatically remove or disable temporary user accounts after account creation in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-000300]

Note: If official documentation exists that disallows the use of temporary user accounts within the application, this requirement is not applicable.

- (3) The application must automatically disable accounts after a period of account inactivity in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-000320]

Note: If the application is configured to use an enterprise-based application user management capability that is compliant with IRM 10.8.1, this requirement is not applicable.

- (4) Unnecessary application accounts must be disabled, or deleted. [DISA: APSC-DV-000330]
- (5) The application must automatically audit the following:

- a. Account creation. [DISA: APSC-DV-000340]

Note: If the application is configured to use an enterprise-based application user management capability that is compliant with IRM 10.8.1, this requirement is not applicable.

- b. Account modification. [DISA: APSC-DV-000350]

Note: If the application is configured to use an enterprise-based application user management capability that is compliant with IRM 10.8.1, this requirement is not applicable.

- c. Account disabling actions. [DISA: APSC-DV-000360]

Note: If the application is configured to use an enterprise-based application user management capability that is compliant with IRM 10.8.1, this requirement is not applicable.

- d. Account removal actions. [DISA: APSC-DV-000370]

Note: If the application is configured to use an enterprise-based application user management capability that is compliant with IRM 10.8.1, this requirement is not applicable.

- e. Account enabling actions. [DISA: APSC-DV-000420]

- (6) The application must notify system administrators (SA) and system security officers (SSO) when the following occur:

- a. Account creation. [DISA: APSC-DV-000380]

Note: If the application is configured to use an enterprise-based application user management capability that is compliant with IRM 10.8.1, this requirement is not applicable.

- b. Account modification. [DISA: APSC-DV-000390]

Note: If the application is configured to use an enterprise-based application user management capability that is compliant with IRM 10.8.1, this requirement is not applicable.

- c. Account disabling actions. [DISA: APSC-DV-000400]

Note: If the application is configured to use an enterprise-based application user management capability that is compliant with IRM 10.8.1, this requirement is not applicable.

- d. Account removal actions. [DISA: APSC-DV-000410]

Note: If the application is configured to use an enterprise-based application user management capability that is compliant with IRM 10.8.1, this requirement is not applicable.

- e. Account enabling actions. [DISA: APSC-DV-000430]

Note: If the application is configured to use an enterprise-based application user management capability that is compliant with IRM 10.8.1, this requirement is not applicable.

- (7) The SSO must ensure an account management process is implemented, verifying only authorized users can gain access to the application, and individual accounts designated as inactive, suspended, or terminated are promptly removed. [DISA: APSC-DV-002880]
- (8) The application must disable device identifiers after a defined period of inactivity in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-001670]

Note: If the application is not designed to authenticate devices (such as mobile phones, gateways or other smart devices), or uses IRS PKI certificates to authenticate these devices, this requirement is not applicable.

- (9) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Account Management.

10.8.6.3.1.2 (09-12-2025) **AC-03 Access Enforcement**

- (1) The application must enforce approved authorizations for logical access to information and system resources in accordance with applicable access control policies. [DISA: APSC-DV-000460]
- (2) The application must enforce IRS-defined discretionary access control policies over defined subjects and objects. [DISA: APSC-DV-000470]

Note: If the application does not implement discretionary access controls, this requirement is not applicable.

- (3) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Access Enforcement.

10.8.6.3.1.3 (09-12-2025) **AC-04 Information Flow Enforcement**

- (1) The application must enforce approved authorizations for controlling the flow of information within the system based on IRS-defined information flow control policies. [DISA: APSC-DV-000480]

Note: If the application does not provide data flow control capabilities, this requirement is not applicable.

- (2) The application must enforce approved authorizations for controlling the flow of information between interconnected systems based on IRS-defined information flow control policies. [DISA: APSC-DV-000490]

Note: If the application does not provide data flow control capabilities, this requirement is not applicable.

- (3) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Information Flow Enforcement.

10.8.6.3.1.4
(09-12-2025)
AC-06 Least Privilege

- (1) The application must prevent non-privileged users from executing privileged functions to include disabling, circumventing, or altering implemented security safeguards or countermeasures. [DISA: APSC-DV-000500]
- (2) The application must execute without excessive account permissions. [DISA: APSC-DV-000510]
- (3) The application must audit the execution of privileged functions. [DISA: APSC-DV-000520]
- (4) Application web servers must be on a separate network segment (i.e., demilitarized zone (DMZ)) from the application and database servers if it is a tiered application operating in the IRS DMZ. [DSIA: APSC-DV-002890]

Note: If the application is not hosted in an IRS DMZ, this requirement is not applicable.

- (5) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Least Privilege.

10.8.6.3.1.5
(09-12-2025)
AC-07 Unsuccessful Logon Attempts

- (1) The application must enforce the limit of three consecutive invalid logon attempts by a user during a time period in accordance with in IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-000530]
- (2) The application administrator must follow an approved process to unlock locked user accounts in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable) [DISA: APSC-DV-000540]
- (3) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Unsuccessful Logon Attempts.

10.8.6.3.1.6
(09-12-2025)
AC-08 System-Use Notification

- (1) The application must display the Standard Mandatory IRS System Use Notification Banner before granting access to the application in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-000550]
- Note:** If the application has no interactive user interface, this requirement is not applicable.
- (2) The application must retain the Standard Mandatory IRS System Use Notification Banner on the screen until users acknowledge the usage conditions and take explicit actions to log on for further access in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-000560]

Note: If the application has no interactive user interface, this requirement is not applicable.

- (3) The publicly accessible application must display the Standard Mandatory IRS System Use Notification Banner before granting access to the application in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-000570]

Note: If the application is not publicly accessible, this requirement is not applicable.

- (4) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on System-Use Notification.

10.8.6.3.1.7
(09-12-2025)

**AC-09 Previous Logon
(Access) Notification**

- (1) The application must display the time and date of the user's last successful logon. [DISA: APSC-DV-000580]

Note: If the application does not provide a user interface, this requirement is not applicable.

- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Previous Logon (Access) Notification.

10.8.6.3.1.8
(09-12-2025)

**AC-10 Concurrent
Session Control**

- (1) The application must provide a capability to limit the number of logon sessions per user in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-000010]

- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Concurrent Session Control.

10.8.6.3.1.9
(09-12-2025)

**AC-12 Session
Termination**

- (1) The application must clear temporary storage and cookies when the session is terminated. [DISA: APSC-DV-000060]

- (2) The application must automatically terminate the non-privileged user session and log off non-privileged users after an idle time period has elapsed in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-000070]

- (3) The application must automatically terminate the admin user session and log off admin users after an idle time period is exceeded in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-000080]

- (4) Applications requiring user access authentication must provide a logoff capability for user-initiated communication sessions. [DISA: APSC-DV-000090]

Note: If the application does not provide an interface for interactive user access, this is not applicable.

- (5) The application must display an explicit logoff message to users indicating the reliable termination of authenticated communications sessions. [DISA: APSC-DV-000100]

Note: If the application does not provide an interface for interactive user access, this is not applicable.

- (6) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Session Termination.

10.8.6.3.1.10
(09-12-2025)
**AC-16 Security and
Privacy Attributes**

- (1) The application must associate IRS-defined types of security attributes having IRS-defined security attribute values with information in storage. [DISA: APSC-DV-000110]

Note: If the application does not contain classified, For Official Use Only (FOUO), or other data that is required to be marked, this requirement is not applicable.

- (2) The application must associate IRS-defined types of security attributes having IRS-defined security attribute values with information in process. [DISA: APSC-DV-000120]

Note: If the application does not contain classified, FOUO, or other data that is required to be marked, this requirement is not applicable.

- (3) The application must associate IRS-defined types of security attributes having IRS-defined security attribute values with information in transmission. [DISA: APSC-DV-000130]

Note: If the application does not contain classified, FOUO or have data marking requirements, or if the application does not transmit data, this requirement is not applicable.

- (4) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Security and Privacy Attributes.

10.8.6.3.1.11
(09-12-2025)
AC-17 Remote Access

- (1) The application must implement IRS-approved encryption (i.e., transport layer security (TLS)) to protect the confidentiality of remote access sessions. [DISA: APSC-DV-000160]

- (2) The application must implement cryptographic mechanisms to protect the integrity of remote access sessions. [DISA: APSC-DV-000170]

- (3) Applications with simple object access protocol (SOAP) messages requiring integrity must sign the following message elements: [DISA: APSC-DV-000180]

- Message ID.
- Service Request.
- Timestamp.
- Security Assertion Markup Language (SAML) Assertion.

Note: SAML assertions are optionally included in messages.

- All elements of the message must be digitally signed

Note: If the application does not utilize SOAP messages, this check is not applicable

- (4) Messages protected with WS_Security must use time stamps with creation and expiration times. [DISA: APSC-DV-000190]

Note: If the application does not utilize WS_Security tokens, this check is not applicable.

- (5) Validity periods must be verified on all application messages using WS_Security or SAML assertions. [DISA: APSC-DV-000200]

Note: If the application does not utilize web services security (WSS) or SAML assertions, this requirement is not applicable.

- (6) The application must ensure each unique asserting party provides unique assertion ID references for each SAML assertion. [DISA: APSC-DV-000210]

Note: If the application does not utilize SAML assertions, this requirement is not applicable.

- (7) The application must ensure encrypted assertions, or equivalent confidentiality protections are used when assertion data is passed through an intermediary, and confidentiality of the assertion data is required when passing through the intermediary. [DISA: APSC-DV-000220]

Note: If the application does not utilize WS_Security tokens, this requirement is not applicable.

- (8) The application must use the NotOnOrAfter condition when using the Subject-Confirmation element in a SAML assertion. [DISA: APSC-DV-000230]

Note: If the application does not utilize SAML assertions, this requirement is not applicable.

- (9) The application must use both the NotBefore and NotOnOrAfter elements or OneTimeUse element when using the Conditions element in a SAML assertion. [DISA: APSC-DV-000240]

Note: If the application does not utilize SAML assertions, this requirement is not applicable.

- (10) The application must ensure if a OneTimeUse element is used in an assertion, there is only one of the same used in the Conditions element portion of an assertion. [DISA: APSC-DV-000250]

Note: If the application does not utilize SAML assertions, this requirement is not applicable.

- (11) The application must ensure messages are encrypted when the SessionIndex is tied to privacy data. [DISA: APSC-DV-000260]

Note: If the application does not utilize SAML assertions, this requirement is not applicable.

- (12) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Remote Access.

10.8.6.3.1.12
(09-12-2025)

AC-23 Data Mining Protection

- (1) Application data protection requirements must be identified and documented. [DISA: APSC-DV-000440]

- (2) The application must utilize IRS-defined data mining detection techniques for IRS-defined data storage objects to adequately detect data mining attempts. [DISA: APSC-DV-000450]

Note: If there are no data mining protections required, this requirement is not applicable.

- (3) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Data Mining Protection.

10.8.6.3.2
(09-12-2025)
AT - Awareness and Training

- (1) In addition to the Awareness and Training guidance defined within this IRM, the following controls must be implemented in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable).
 - AT-01 Policy and Procedures
 - AT-02 Literacy Training and Awareness
 - AT-04 Training Records
 - AT-06 Training Feedback

10.8.6.3.2.1
(09-12-2025)
AT-03 Role-Based Training

- (1) The program manager must verify all levels of program management, designers, developers, and testers receive annual security training pertaining to their job function in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-003400]

Note: This requirement is meant to be applied to developers and development teams only; otherwise, this requirement is not applicable.

- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Role-Based Training.

10.8.6.3.3
(09-12-2025)
AU - Audit and Accountability

- (1) In addition to the Audit and Accountability guidance defined within this IRM, the following controls must be implemented in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable).
 - AU-01 Policy and Procedures
 - AU-02 Event Logging
 - AU-13 Monitoring for Information Disclosure
 - AU-16 Cross-Organization Audit Logging

10.8.6.3.3.1
(09-12-2025)
AU-03 Content of Audit Records

- (1) The application must log application shutdown events. [DISA: APSC-DV-000940]
 - (2) The application must log destination IP addresses. [DISA: APSC-DV-000950]
- Note:** If the application design documentation indicates the application does not initiate connections to remote systems this requirement is not applicable.
- (3) The application must log user actions involving access to data. [DISA: APSC-DV-000960]
 - (4) The application must log user actions involving changes to data. [DISA: APSC-DV-000970]
 - (5) The application must produce audit records containing information to establish when (date and time) the events occurred. [DISA: APSC-DV-000980]
 - (6) The application must produce audit records containing enough information to establish which component, feature or function of the application triggered the audit event. [DISA: APSC-DV-000990]
 - (7) When using centralized logging; the application must include a unique identifier in order to distinguish itself from other application logs. [DISA: APSC-DV-001000]

Note: If the application is logging locally and does not utilize a centralized logging solution, this requirement is not applicable.

- (8) The application must produce audit records that contain information to establish the outcome of the events. [DISA: APSC-DV-001010]
- (9) The application must generate audit records containing information that establishes the identity of any individual or process associated with the event. [DISA: APSC-DV-001020]
- (10) The application must generate audit records containing the full-text recording of privileged commands or the individual identities of group account users. [DISA: APSC-DV-001030]
- (11) The application must implement transaction recovery logs when transaction based. [DISA: APSC-DV-001040]
- (12) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Content of Audit Records.

10.8.6.3.3.2
(09-12-2025)

AU-04 Audit Log Storage Capacity

- (1) The application must off-load audit records onto a different system or media than the system being audited. [DISA: APSC-DV-001070]
Note: If the application is configured to utilize a centralized logging solution, this requirement is not applicable.
- (2) The application must be configured to write application logs to a centralized log repository. [DISA: APSC-DV-001080]
- (3) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Audit Log Storage Capacity.

10.8.6.3.3.3
(09-12-2025)

AU-05 Response to Audit Logging Process Failures

- (1) The application must provide an immediate warning to the SA and SSO (at a minimum) when allocated audit record storage volume reaches 75% of the repository maximum audit record storage capacity. [DISA: APSC-DV-001090]
Note: If the application utilizes a centralized logging system that provides storage capacity alarming, this requirement is not applicable.
- (2) Applications categorized as having a moderate or high impact must provide an immediate real-time alert to the SA and SSO (at a minimum) for all audit failure events in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-001100]
Note: If the application utilizes a centralized logging system that provides the real-time alarms, this requirement is not applicable.
- (3) The application must alert the SSO and SA (at a minimum) in the event of an audit processing failure. [DISA: APSC-DV-001110]
Note: If the application utilizes a centralized logging system that provides the audit processing failure alarms, this requirement is not applicable.
- (4) The application must shut down by default upon audit failure (unless availability is an overriding concern). [DISA: APSC-DV-001120]
- (5) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Response to Audit Logging Process Failures.

10.8.6.3.3.4
(09-12-2025)
**AU-06 Audit Record
Review, Analysis, and
Reporting**

- (1) The application must provide the capability to centrally review and analyze audit records from multiple components within the system. [DISA: APSC-DV-001130]

Note: If the application utilizes a centralized logging system that provides the capability to review the log files from one central location, this requirement is not applicable.

- (2) The SSO must ensure audit trails are reviewed periodically in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-002910]
- (3) The SSO must report all suspected violations of information assurance (IA) policies in accordance with IRS information system IA procedures. [DISA: APSC-DV-002920]
- (4) The application must provide centralized management and configuration of the content to be captured in audit records generated by all application components. [DISA: APSC-DV-001050]

Note: If the application is configured to log application event entries to a centralized, enterprise-based logging solution that meets this requirement, this requirement is not applicable.

- (5) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Audit Record Review, Analysis, and Reporting.

10.8.6.3.3.5
(09-12-2025)
**AU-07 Audit Record
Reduction and Report
Generation**

- (1) The application must provide the capability to filter audit records for events of interest based upon IRS-defined criteria. [DISA: APSC-DV-001140]

Note: If the application utilizes a centralized logging system that provides the capability to filter log events based upon IRS-defined event criteria, this requirement is not applicable.

- (2) The application must provide an audit reduction capability that supports on-demand reporting requirements. [DISA: APSC-DV-001150]

Note: If the application utilizes a centralized logging system that provides the capability to generate reports based on filtered log events, this requirement is not applicable.

- (3) The application must provide an audit reduction capability that supports on-demand audit review and analysis. [DISA: APSC-DV-001160]

Note: If the application utilizes a centralized logging system that provides the capability to generate reports based on filtered log events, this requirement is not applicable.

- (4) The application must provide an audit reduction capability that supports after-the-fact investigations of security incidents. [DISA: APSC-DV-001170]

Note: If the application uses a centralized logging solution that performs the audit reduction (event filtering) functions, this requirement is not applicable.

- (5) The application must provide a report generation capability that supports on-demand audit review and analysis. [DISA: APSC-DV-001180]

Note: If the application uses a centralized logging solution that provides immediate, customizable audit review and analysis functions, this requirement is not applicable.

- (6) The application must provide a report generation capability that supports on-demand reporting requirements. [DISA: APSC-DV-001190]

Note: If the application uses a centralized logging solution that provides immediate, customizable, ad-hoc report generation functions, this requirement is not applicable.

- (7) The application must provide a report generation capability that supports after-the-fact investigations of security incidents. [DISA: APSC-DV-001200]

Note: If the application uses a centralized logging solution that performs the report generation functions, this requirement is not applicable.

- (8) The application must provide an audit reduction capability that does not alter original content or time ordering of audit records. [DISA: APSC-DV-001210]

Note: If the application uses a centralized logging solution that performs the audit reduction (event filtering) functions, this requirement is not applicable.

- (9) The application must provide a report generation capability that does not alter original content or time ordering of audit records. [DISA: APSC-DV-001220]

Note: If the application does not provide a report generation capability, this requirement is not applicable.

- (10) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Audit Record Reduction and Report Generation.

10.8.6.3.3.6 (09-12-2025) **AU-08 Time Stamps**

- (1) The application must use internal system clocks to generate time stamps for audit records in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-001250]
- (2) The application must record time stamps for audit records that can be mapped to Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT) in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-001260]
- (3) The application must record time stamps for audit records that meet a granularity of one second for a minimum degree of precision in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-001270]

Note: If the application utilizes the underlying operating system (OS) for time stamping and time synchronization when writing the audit logs, this requirement is not applicable.

- (4) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Time Stamps.

10.8.6.3.3.7 (09-12-2025) **AU-09 Protection of Audit Information**

- (1) The application must protect audit information from the following:
- Any type of unauthorized read access. [DISA: APSC-DV-001280]
 - Unauthorized modification. [DISA: APSC-DV-001290]

- c. Unauthorized deletion. [DISA: APSC-DV-001300]
- (2) The application must protect audit tools from the following:
 - a. Any type of unauthorized read access. [DISA: APSC-DV-001310]
Note: If the application does not provide a distinct audit tool oriented functionality that is a separate tool with an ability to view and manipulate log data, this requirement is not applicable.
 - b. Unauthorized modification. [DISA: APSC-DV-001320]
Note: If the application does not provide a distinct audit tool oriented functionality that is a separate tool with an ability to view and manipulate log data, this requirement is not applicable.
 - c. Unauthorized deletion. [DISA: APSC-DV-001330]
Note: If the application does not provide a distinct audit tool oriented functionality that is a separate tool with an ability to view and manipulate log data, this requirement is not applicable.
- (3) The application must back up audit records at least every seven days onto a different system or system component than the system or component being audited in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-001340]
Note: If the application does not include a built-in backup capability for backing up its own audit records, this requirement is not applicable.
- (4) The application must use FIPS validated cryptographic mechanisms to protect the integrity of audit information. [DISA: APSC-DV-001350]
Note: If the application is configured to utilize a centralized audit log solution that uses cryptographic methods that meet this requirement such as creating cryptographic hash values or message digests that can be used to validate integrity of audit files, this requirement is not applicable.
- (5) Application audit tools must be cryptographically hashed using FIPS 140-validated cryptographic mechanisms. [DISA: APSC-DV-001360]
Note: If the application does not provide a separate tool in the form of a file which provides an ability to view and manipulate application log data, query data, or generate reports, this requirement is not applicable.
- (6) The integrity of the audit tools must be validated by checking the files for changes in the cryptographic hash value. [DISA: APSC-DV-001370]
Note: If the application does not provide a separate tool in the form of a file which provides an ability to view and manipulate application log data, query data or generate reports, this requirement is not applicable.
- (7) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Protection of Audit Information.

10.8.6.3.3.8
(09-12-2025)
AU-10 Non-Repudiation

- (1) The application must protect against an individual (or process acting on behalf of an individual) falsely denying having performed IRS-defined actions to be covered by non-repudiation. [DISA: APSC-DV-000590]

Note: If the application documentation specifically states that non-repudiation services for application users are not defined as part of the application design, this requirement is not applicable.

- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Non-Repudiation.

10.8.6.3.3.9
(09-12-2025)

AU-11 Audit Record Retention

- (1) The SSO must ensure application audit trails records are retained in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-002900]
- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Audit Record Retention.

10.8.6.3.3.10
(09-12-2025)

AU-12 Audit Record Generation

- (1) For applications providing audit record aggregation, the application must compile audit records from IRS-defined information system components into a system-wide audit trail that is time-correlated with an IRS-defined level of tolerance for the relationship between time stamps of individual records in the audit trail. [DISA: APSC-DV-000600]

Note: If the application does not provide log aggregation services, this requirement is not applicable.

- (2) The application must provide audit record generation capability for the following:
 - a. The creation of session IDs. [DISA: APSC-DV-000620]
 - b. The destruction of session IDs. [DISA: APSC-DV-000630]
 - c. The renewal of session IDs. [DISA: APSC-DV-000640]
 - d. Session timeouts. [DISA: APSC-DV-000660]
 - e. HTTP headers including User-Agent, Referer, GET, and POST. [DISA: APSC-DV-000680]
 - f. Connecting system IP addresses. [DISA: APSC-DV-000690]
- (3) The application must not write sensitive data into the application logs. [DISA: APSC-DV-000650]
- (4) The application must record the following:
 - a. A time stamp indicating when the event occurred. [DISA: APSC-DV-000670]
 - b. The username or user ID of the user associated with the event. [DISA: APSC-DV-000700]
- (5) The application must generate audit records when the following occurs:
 - a. Successful or unsuccessful attempts to grant privileges. [DISA: APSC-DV-000710]
 - b. Successful or unsuccessful attempts to access security objects. [DISA: APSC-DV-000720]
 - c. Successful or unsuccessful attempts to access security levels. [DISA: APSC-DV-000730]
 - d. Successful or unsuccessful attempts to access categories of information (e.g., classification levels). [DISA: APSC-DV-000740]

Note: If the application requirements do not call for compartmentalized data and data protection, this requirement is not applicable.

- e. Successful or unsuccessful attempts to modify privileges. [DISA: APSC-DV-000750]
- f. Successful or unsuccessful attempts to modify security objects. [DISA: APSC-DV-000760]
- g. Successful or unsuccessful attempts to modify security levels. [DISA: APSC-DV-000770]
- h. Successful or unsuccessful attempts to modify categories of information (e.g., classification levels). [DISA: APSC-DV-000780]

Note: If the application requirements do not call for compartmentalized data and data protection, this requirement is not applicable.

- i. Successful or unsuccessful attempts to delete privileges. [DISA: APSC-DV-000790]
- j. Successful or unsuccessful attempts to delete security levels. [DISA: APSC-DV-000800]
- k. Successful or unsuccessful attempts to delete application database security objects. [DISA: APSC-DV-000810]
- l. Successful or unsuccessful attempts to delete categories of information (e.g., classification levels). [DISA: APSC-DV-000820]

Note: If the application requirements do not call for compartmentalized data and data protection, this requirement is not applicable.

- m. Successful or unsuccessful logon attempts. [DISA: APSC-DV-000830]
- n. Successful or unsuccessful accesses to objects. [DISA: APSC-DV-000860]

(6) The application must generate audit records for the following:

- a. All direct access to the information system. [DISA: APSC-DV-000870]

Note: If the application does not provide direct access to the system, this requirement is not applicable.

- b. All account creations, modifications, disabling, and termination events. [DISA: APSC-DV-000880]
- c. Privileged activities or other system-level access. [DISA: APSC-DV-000840]

(7) The application must generate audit records showing starting and ending time for user access to the system. [DISA: APSC-DV-000850]

(8) The application must generate audit records when concurrent logons from different workstations occur. [DISA: APSC-DV-003360]

(9) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Audit Record Generation.

10.8.6.3.3.11
(09-12-2025)

AU-14 Session Audit

(1) The application must initiate session auditing upon startup. [DISA: APSC-DV-000910]

(2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Session Audit.

- 10.8.6.3.4
(09-12-2025)
CA - Assessment, Authorization, and Monitoring
- (1) In addition to the Assessment, Authorization, and Monitoring guidance defined within this IRM, the following controls must be implemented in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable).
- CA-01 Policy and Procedures
 - CA-03 Information Exchange
 - CA-05 Plan of Action and Milestones (POA&M)
 - CA-06 Authorization
 - CA-07 Continuous Monitoring
 - CA-08 Penetration Testing
 - CA-09 Internal System Connections
- 10.8.6.3.4.1
(09-12-2025)
CA-2 Control Assessments
- (1) The SSO must ensure active vulnerability (production) and fuzz (pre-production) testing is performed. [DISA: APSC-DV-002930]
- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Control Assessments.
- 10.8.6.3.5
(09-12-2025)
CM - Configuration Management
- (1) In addition to the Configuration Management (CM) guidance defined within this IRM, the following controls must be implemented in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable).
- CM-01 Policy and Procedures
 - CM-02 Baseline Configuration
 - CM-08 System Component Inventory
 - CM-10 Software Usage Restrictions
 - CM-12 Information Location
 - CM-13 Data Action Mapping
- 10.8.6.3.5.1
(09-12-2025)
CM-03 Configuration Change Controls
- (1) Configuration Change Control requirements must be implemented in accordance with IRM 10.8.1.
- (2) A Configuration Control Board (CCB) must be established to manage the CM process. [DISA: APP4040]
- (3) The SSO must be a member of the CCB. [DISA: APP4040]
- (4) The CCB must meet at least every release cycle or more often. [DISA: APP4040]
- (5) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Configuration Change Controls.
- 10.8.6.3.5.2
(09-12-2025)
CM-04 Impact Analyses
- (1) Execution flow diagrams and design documents must be created to show how deadlock and recursion issues in web services are being mitigated. [DISA: APSC-DV-002950]
- Note:** If the application does not deploy web services, this requirement is not applicable.
- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Impact Analysis.

10.8.6.3.5.3
(09-12-2025)

**CM-05 Access
Restrictions for Change**

- (1) The application must enforce access restrictions associated with changes to application configuration. [DISA: APSC-DV-001410]
- (2) The application must audit who makes configuration changes to the application. [DISA: APSC-DV-001420]
- (3) The application must limit privileges to change the software resident within software libraries. [DISA: APSC-DV-001440]
- (4) The designer must ensure the application does not store configuration and control files in the same directory as user data. [DISA: APSC-DV-002960]
- (5) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Access Restrictions for Change.

10.8.6.3.5.4
(09-12-2025)

**CM-06 Configuration
Settings**

- (1) An application vulnerability assessment must be conducted. [DISA: APSC-DV-001460]
- (2) The ISSO must ensure if an IRS or OWASP guide is not available, follow guidance in accordance with CM-02 Baseline configurations of IRM 10.8.1. [DISA: APSC-DV-002970]
- (3) The application must allow the use of a temporary password for system logons with an immediate change to a permanent password. [DISA: APSC-DV-001790]

Note: If the application does not use passwords, this requirement is not applicable.

- (4) The application must have a process, feature or function that prevents removal or disabling of emergency accounts. [DISA: APSC-DV-000310]

Note: If emergency accounts are not used, this requirement is not applicable.

- (5) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Configuration Settings.

10.8.6.3.5.5
(09-12-2025)

**CM-07 Least
Functionality**

- (1) The application must prevent program execution in accordance with IRS-defined policies regarding software program usage and restrictions, and or rules authorizing the terms and conditions of software program usage. [DISA: APSC-DV-001480]

Note: If the policy, terms, or conditions state there are no usage restrictions, this requirement is not applicable.

- (2) The application must employ a deny-all, permit-by-exception (whitelist) policy to allow the execution of authorized software programs. [DISA: APSC-DV-001490]

Note: If the application is not a configuration management or similar type of application designed to manage system processes and configurations, this requirement is not applicable.

- (3) The application must be configured to disable non-essential capabilities. [DISA: APSC-DV-001500]

- (4) The application must be configured to use only functions, ports, and protocols permitted in accordance with UNS and CSIRC. [DISA: APSC-DV-001510]
- (5) New IP addresses, data services, and associated ports used by the application must be configured to comply with IRS-approved ports and protocol guidance in accordance with UNS and CSIRC. [DISA: APSC-DV-002980, APSC-DV-002990]
- (6) The application must be registered with UNS and CSIRC for the ports, protocols, and services it uses. [DISA: APSC-DV-002990]
- (7) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Least Functionality.

10.8.6.3.5.6
(09-12-2025)

CM-09 Configuration Management Plan

- (1) The CM repository must be properly patched and security technical implementation guide (STIG) compliant. [DISA: APSC-DV-002995]

Note: Identify if the STIG is being applied to application developers or organizations responsible for code management or who have and operate an application CM repository. If this is not the case, this requirement is not applicable.

- (2) Access privileges to the CM repository must be reviewed every three months. [DISA: APSC-DV-003000]

Note: If application development is not done in house and if a code configuration management repository does not exist, this requirement is not applicable.

- (3) A Software Configuration Management (SCM) plan describing the configuration control and change management process of application objects developed by the IRS and the roles and responsibilities of the IRS must be created and maintained. [DISA: APSC-DV-003010]

Note: If application development is not done in house and if a code configuration management repository does not exist, this requirement is not applicable.

- (4) A CCB that meets at least every release cycle, for managing the CM process must be established. [DISA: APSC-DV-003020]

Note: If application development is not done in house, this requirement is not applicable.

- (5) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Configuration Management (CM) Plan.

10.8.6.3.5.7
(09-12-2025)

CM-11 User-Installed Software

- (1) The application must prohibit user installation of software without explicit privileged status. [DISA: APSC-DV-001390]

Note: If the application does not provide the ability to install software components, modules, plugins, or extensions, this requirement is not applicable.

- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on User-Installed Software.

10.8.6.3.5.8
(09-12-2025)
**CM-14 Signed
Components**

- (1) The application must have the capability to prevent the installation of patches, service packs, or application components without verification the software component has been digitally signed using a certificate that is recognized and approved by the IRS. [DISA: APSC-DV-001430]
- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Signed Components.

10.8.6.3.6
(09-12-2025)
**CP Contingency
Planning**

- (1) In addition to the Contingency Planning guidance defined within this IRM, the following controls must be implemented in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable).
 - CP-01 Policy and Procedures
 - CP-03 Contingency Planning
 - CP-04 Contingency Plan Testing
 - CP-06 Alternate Storage Site
 - CP-07 Alternate Processing Site
 - CP-08 Telecommunications Service
 - CP-12 Safe Mode
 - CP-13 Alternative Security Mechanisms
- (2) See IRM 10.8.60, *Information Technology (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance*, 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 guidance on Contingency Planning.

10.8.6.3.6.1
(09-12-2025)
CP-02 Contingency Plan

- (1) The application must not be hosted on a general purpose machine if the application is designated as critical or high availability in accordance with IRM 10.8.2. [DISA: APSC-DV-003040]
- (2) A disaster recovery or continuity plan must exist in accordance with IRS policy based on the application's availability requirements. [DISA: APSC-DV-003050]
- (3) Recovery procedures and technical system features must exist so recovery is performed in a secure and verifiable manner. The SSO will document circumstances inhibiting a trusted recovery. [DISA: APSC-DV-003060]
- (4) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Contingency Plan.

10.8.6.3.6.2
(09-12-2025)
CP-09 System Backup

- (1) Data backup must be performed at required intervals in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-003070]
- (2) Back-up copies of the application software or source code must be stored in a fire-rated container or stored separately (offsite). [DISA: APSC-DV-003080]
- (3) Procedures must be in place to assure the appropriate physical and technical protection of the backup and restoration of the application. [DISA: APSC-DV-003090]

Note: If application does not implement key exchange, this requirement is not applicable.

- (4) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on System Backup.
- 10.8.6.3.6.3
(09-12-2025)
CP-10 Information System Recovery and Reconstitution
- (1) Information System Recovery and Reconstitution requirements must be implemented in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable).
- (2) A disaster recovery plan must exist based on the criticality of the data as documented in the system's security documentation. [DISA: APP6200]
- (3) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Information System Recovery and Reconstitution.
- 10.8.6.3.6.4
(09-12-2025)
CP-11 Alternate Communications Protocols
- (1) The application services and interfaces must be compatible with and ready for IPv6 networks. [DISA: APSC-DV-003030]
- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on for additional IPv6 requirements.
- (3) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Alternate Communications Protocols.
- 10.8.6.3.7
(09-12-2025)
IA - Identification and Authentication
- (1) In addition to the Identification and Authentication guidance defined within this IRM, the following controls must be implemented in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable).
- IA-01 Policy and Procedures
 - IA-04 Identifier Management
 - IA-09 Service Identification and Authentication
 - IA-10 Adaptive Authentication
 - IA-12 Identity Proofing
 - IA-13 Identity Providers and Authorization Servers
- 10.8.6.3.7.1
(09-12-2025)
IA-02 Identification and Authentication (Organizational Users)
- (1) The application must uniquely identify and authenticate IRS users (or processes acting on behalf of organizational users). [DISA: APSC-DV-001540]
- Note:** If the application is publicly available, providing access to publicly releasable data and the users are non-organizational users such as individuals who no longer have a person identity verification (PIV) (e.g., retirees) or members of the public with no requirement for IRS credentials, this requirement is not applicable.
- (2) The application must accept PIV credentials. [DISA: APSC-DV-001560]
- Note:** If the application is not public key (PK)-enabled due to the hosted data being publicly releasable, this check is not applicable.
- (3) The application must electronically verify PIV credentials. [DISA: APSC-DV-001570]
- Note:** If the application is not PK-enabled due to the hosted data being publicly releasable, this check is not applicable.
- (4) The application must use multifactor (e.g., PIV, Alt. Token) authentication for the following:

- a. Network access to privileged accounts. [DISA: APSC-DV-001550]
- b. Network access to nonprivileged accounts. [DISA: APSC-DV-001580]

Note: If the application is not PK-enabled due to the hosted data being publicly releasable, this check is not applicable.

- c. Local access to privileged accounts. [DISA: APSC-DV-001590]
- d. Local access to non-privileged accounts. [DISA: APSC-DV-001600]

Note: If the application is not PK-enabled due to the hosted data being publicly releasable, this check is not applicable.

- (5) The application must ensure users are authenticated with an individual authenticator prior to using a group authenticator. [DISA: APSC-DV-001610]

Note: If the application does not use group or shared accounts, this requirement is not applicable.

- (6) The application must implement replay-resistant authentication mechanisms for network access to privileged accounts. [DISA: APSC-DV-001620]

Note: If the application is hosting publicly releasable information that does not require authentication, or if the application users are not eligible for an IRS PIV, this requirement is not applicable.

- (7) The application must implement replay-resistant authentication mechanisms for network access to nonprivileged accounts. [DISA: APSC-DV-001630]

Note: If the application is hosting publicly releasable information that does not require authentication, or if the application users are not eligible for an IRS PIV, this requirement is not applicable.

- (8) Shared or group account credentials must be terminated when members leave the group. [DISA: APSC-DV-000290]

Note: If there is no official requirement for shared or group application accounts, this requirement is not applicable.

- (9) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Identification and Authentication (Organizational Users).

10.8.6.3.7.2 (09-12-2025) **IA-03 Device Identification and Authentication**

- (1) The application must utilize mutual authentication when endpoint device non-repudiation protections are required by organizational policy or by the data owner. [DISA: APSC-DV-001640]
- (2) The application must authenticate all network connected endpoint devices before establishing any connection. [DISA: APSC-DV-001650]

Note: If the application is designed to provide end-user, interactive application access only and does not use web services or allow connections from remote devices, this requirement is not applicable.

- (3) Service-Oriented Applications handling non-releasable data must authenticate endpoint devices via mutual secure level socket (SSL)/TLS. [DISA: APSC-DV-001660]
- (4) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Device Identification and Authentication.

10.8.6.3.7.3
(09-12-2025)
**IA-05 Authenticator
Management**

- (1) The application must enforce a minimum password length as defined in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-001680]

Note: This requirement is only applicable to systems unable to implement Multi-Factor Authentication (MFA). Refer to IRM 10.8.1 for further guidance.

- (2) The application must enforce password complexity by requiring the following be used in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable):

- a. At least one uppercase character; [DISA: APSC-DV-001690]

Note: This requirement is only applicable to systems unable to implement Multi-Factor Authentication (MFA). Refer to IRM 10.8.1 for further guidance.

- b. At least one lower-case character; [DISA: APSC-DV-001700]

Note: This requirement is only applicable to systems unable to implement Multi-Factor Authentication (MFA). Refer to IRM 10.8.1 for further guidance.

- c. At least one numeric character; and [DISA: APSC-DV-001710]

Note: This requirement is only applicable to systems unable to implement Multi-Factor Authentication (MFA). Refer to IRM 10.8.1 for further guidance.

- d. At least one special character; [DISA: APSC-DV-001720]

Note: This requirement is only applicable to systems unable to implement Multi-Factor Authentication (MFA). Refer to IRM 10.8.1 for further guidance.

- (3) The application must require new account passwords differ from the previous password by at least changing the number of characters in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable) when a password is changed. [DISA: APSC-DV-001730]

Note: If the application does not use passwords, this requirement is not applicable.

- (4) The application must only store cryptographic representations of passwords. [DISA: APSC-DV-001740]

Note: If the application does not use passwords, this requirement is not applicable.

- (5) The application must transmit only cryptographically-protected passwords. [DISA: APSC-DV-001750]

Note: If the application does not use passwords, this requirement is not applicable.

- (6) The application must enforce minimum password lifetime in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-001760]

Note: If the application does not use passwords, this requirement is not applicable.

- (7) The application must enforce maximum password lifetime in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-001770]

Note: If the application does not use passwords, this requirement is not applicable.

- (8) The application must prohibit password reuse in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-001780]

Note: If the application does not use passwords, this requirement is not applicable.

- (9) The application password must not be changeable by users other than the administrator or the user with which the password is associated. [DISA: APSC-DV-001795]

Note: If the application does not use passwords, this requirement is not applicable.

Note: If the application does not allow users to change or reset their passwords, this requirement is not applicable.

- (10) The application must terminate existing user sessions upon account deletion. [DISA: APSC-DV-001800]

- (11) The application, when utilizing PKI-based authentication, must validate certificates by constructing a certification path (which includes status information) to an accepted trust anchor in accordance with Treasury's PKI X.509 Certificate Policy. [DISA: APSC-DV-001810]

- (12) The application, when utilizing PKI-based authentication, must enforce authorized access to the corresponding private key in accordance with Treasury's PKI X.509 Certificate Policy. [DISA: APSC-DV-001820]

Note: If the application does not perform code signing or other cryptographic tasks requiring a private key, this requirement is not applicable.

- (13) The application must map the authenticated identity to the individual user or group account for PKI-based authentication in accordance with Treasury's PKI X.509 Certificate Policy. [DISA: APSC-DV-001830]

- (14) The application must, for PKI-based authentication, implement a local cache of revocation data to support path discovery and validation in case of the inability to access revocation information via the network. [DISA: APSC-DV-001840]

Note: If the application resides on a classified network and does not have access to the root certificate authorities (CAs), this requirement is not applicable.

- (15) The application must use encryption to implement key exchange and authenticate endpoints prior to establishing a communication channel for key exchange. [DISA: APSC-DV-003100]

- (16) The application must not contain embedded authentication data. [DISA: APSC-DV-003110]

- (17) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Authenticator Management.

10.8.6.3.7.4
(09-12-2025)

**IA-06 Authenticator
Feedback**

- (1) The application must not display passwords or personal identification number (PIN)s as clear text. [DISA: APSC-DV-001850]
- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Authenticator Feedback.

10.8.6.3.7.5
(09-12-2025)

**IA-07 Cryptographic
Module Authentication**

- (1) The application must use mechanisms meeting the requirements of IRM 10.8.1, applicable federal laws, executive orders, directives, policies, regulations, standards, and guidance (i.e., FIPS-approved) for authentication to a cryptographic module. [DISA: APSC-DV-001860]

Note: If the application does not provide authenticated access to a cryptographic module, this requirement is not applicable.

- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Cryptographic Module Authentication.

10.8.6.3.7.6
(09-12-2025)

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

- (1) The application must uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-IRS users). [DISA: APSC-DV-001870]

Note: If the application does not host non-organizational users, this requirement is not applicable.

- (2) The application must accept PIV credentials from other federal agencies. [DISA: APSC-DV-001880]

Note: If the application is not PK-enabled due to the hosted data being publicly releasable, this check is not applicable.

Note: If the application is only deployed to classified, this requirement is not applicable.

Note: If the application is not intended to be available to Federal government (non-IRS) partners this requirement is not applicable.

- (3) The application must electronically verify PIV credentials from other federal agencies. [DISA: APSC-DV-001890]

Note: If the application is not PK-enabled due to the hosted data being publicly releasable, this check is not applicable.

Note: If the application is only deployed to classified, this requirement is not applicable.

Note: If the application is not intended to be available to federal government (non-IRS) partners this requirement is not applicable.

- (4) The application must accept Federal Identity, Credential, and Access Management (FICAM) approved third-party credentials. [DISA: APSC-DV-001900]

Note: If the application is not PK-enabled due to the hosted data being publicly releasable, this check is not applicable.

Note: If the application is only deployed to classified, this requirement is not applicable.

Note: If the application is not intended to be available to federal government (non-IRS) partners this requirement is not applicable.

- (5) The application must conform to FICAM-issued profiles in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-001910]

Note: If the application is not PK-enabled due to the hosted data being publicly releasable, this check is not applicable.

Note: If the application is only deployed to secret internet protocol router network (SIPRNet), this requirement is not applicable.

Note: If the application is not intended to be available to federal government (non-IRS) partners this requirement is not applicable.

- (6) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Identification and Authentication (Non-Organizational Users).

10.8.6.3.7.7
(09-12-2025)

IA-11 Re-authentication

- (1) The application must require devices to re-authenticate when IRS-defined circumstances or situations require re-authentication. [DISA: APSC-DV-001530]
- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Reauthentication.

10.8.6.3.8
(09-12-2025)

IR - Incident Response

- (1) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Incident Response Policy and Procedures.

10.8.6.3.9
(09-12-2025)

MA - Maintenance

- (1) In addition to the Maintenance guidance defined within this IRM, the following controls must be implemented in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable).

- MA-01 Policy and Procedures
- MA-02 Controlled Maintenance
- MA-03 Maintenance Tools
- MA-05 Maintenance Personnel
- MA-06 Timely Maintenance
- MA-07 Field Maintenance

10.8.6.3.9.1
(09-12-2025)

MA-4 Non-Local Maintenance

- (1) Applications used for non-local maintenance sessions must audit non-local maintenance and diagnostic sessions for IRS-defined auditable events. [DISA: APSC-DV-001930]

Note: If the application does not provide non-local maintenance and diagnostic capability, this requirement is not applicable.

- (2) Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the integrity of non-local maintenance and diagnostic communications. [DISA: APSC-DV-001940]

Note: If the application does not provide non-local maintenance and diagnostic capability, this requirement is not applicable.

- (3) Applications used for non-local maintenance sessions must implement cryptographic mechanisms to protect the confidentiality of non-local maintenance and diagnostic communications. [DISA: APSC-DV-001950]

Note: If the application does not provide non-local maintenance and diagnostic capability, this requirement is not applicable.

- (4) Applications used for non-local maintenance sessions must verify remote disconnection at the termination of non-local maintenance and diagnostic sessions. [DISA: APSC-DV-001960]

Note: If the application does not provide non-local maintenance and diagnostic capability, this requirement is not applicable.

- (5) The application must employ strong authenticators in the establishment of non-local maintenance and diagnostic sessions. [DISA: APSC-DV-001970]

Note: If the application does not provide non-local maintenance and diagnostic capability, this requirement is not applicable.

- (6) The application must terminate all sessions and network connections when non-local maintenance is completed. [DISA: APSC-DV-001980]

Note: If the application does not provide nonlocal maintenance and diagnostic capability, this requirement is not applicable.

- (7) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Non-Local Maintenance.

10.8.6.3.10
(09-12-2025)
MP - Media Protection

- (1) In addition to the media protection guidance within this IRM, the following controls must be implemented in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable):

- MP-01 Policy and Procedures
- MP-02 Media Access
- MP-04 Media Storage
- MP-05 Media Transport
- MP-06 Media Sanitization
- MP-07 Media Use
- MP-08 Media Downgrading

10.8.6.3.10.1
(09-12-2025)
MP-03 Media Marking

- (1) The application must have the capability to mark sensitive output when required. [DISA: APCS-DV-003120]
- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Media Marking.

10.8.6.3.11
(09-12-2025)
PE - Physical and Environmental Protection

- (1) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Physical and Environmental Protection.

10.8.6.3.12
(09-12-2025)
PL - Planning

- (1) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Planning.

10.8.6.3.13
(09-12-2025)
**PM - Program
Management**

- (1) In addition to the Program Management guidance defined within this IRM, the following controls must be implemented in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable):

- PM-01 Information Security Program Plan
- PM-02 Information Security Program Leadership Role
- PM-03 Information Security and Privacy Resources
- PM-04 Plan of Action and Milestones Process
- PM-05 System Inventory
- PM-06 Measures of Performance
- PM-07 Enterprise Architecture
- PM-08 Critical Infrastructure Plan
- PM-09 Risk Management Strategy
- PM-10 Authorization Process
- PM-11 Mission and Business Process Definition
- PM-12 Insider Threat Program
- PM-13 Security and Privacy Workforce
- PM-15 Security and Privacy Groups and Associations
- PM-16 Threat Awareness Program
- PM-17 Protecting Controlled Unclassified Information on External Systems
- PM-18 Privacy Program Plan
- PM-19 Privacy Program Leadership Role
- PM-20 Dissemination of Privacy Program Information
- PM-21 Accounting of Disclosures
- PM-22 Personally Identifiable Information Quality Management
- PM-23 Data Governance Body
- PM-24 Data Integrity Board
- PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research
- PM-26 Complaint Management
- PM-27 Privacy Reporting
- PM-28 Risk Framing
- PM-29 Risk Management Program Leadership Roles
- PM-30 Supply Chain Risk Management Strategy
- PM-31 Continuous Monitoring Strategy
- PM-32 Purposing

10.8.6.3.14
(09-12-2025)
**PM - 14 Testing,
Training, and Monitoring**

- (1) Prior to each release of the application, updates to system, or applying patches; test plans and procedures must be created and executed. [DISA: APSC-DV-003130]

Note: If the review is not being done with the developer of the application, this requirement is not applicable.

- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Testing, Training, and Monitoring.

10.8.6.3.15
(09-12-2025)
PS - Personnel Security

- (1) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Personnel Security.

10.8.6.3.16 (09-12-2025) PT - Personally Identifiable Information Processing and Transparency	(1) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Personally Identifiable Information Processing and Transparency.
10.8.6.3.17 (09-12-2025) RA - Risk Assessment	(1) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Risk Assessment.
10.8.6.3.18 (09-12-2025) SA - System and Services Acquisition	<p>(1) In addition to the System and Services Acquisition guidance defined within this IRM, the following controls must be implemented in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable).</p> <ul style="list-style-type: none"> • SA-01 Policy and Procedures • SA-02 Allocation of Resources • SA-03 System Development Life Cycle (SDLC) • SA-08 Security and Privacy Engineering Principles • SA-09 External System Services • SA-16 Developer-Provided Training • SA-17 Developer Security and Privacy Architecture and Design • SA-20 Customized Development of Critical Components • SA-21 Developer Screening • SA-22 Unsupported System Components • SA-23 Specialization <p>(2) Refer to the Critical Software section within IRM 10.8.1 for Executive Order 14028, Improving the Nation's Cybersecurity.</p>
10.8.6.3.18.1 (09-12-2025) SA-04 Acquisition Process	<p>(1) Unnecessary built-in application accounts must be disabled in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-003270]</p> <p>(2) Default passwords must be changed in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-003280]</p> <p>(3) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Acquisition Process.</p>
10.8.6.3.18.2 (09-12-2025) SA-05 System Documentation	<p>(1) An Application Configuration Guide must be created and included with the application. [DISA: APSC-DV-003285]</p> <p>(2) If the application contains classified data, a Security Classification Guide must exist containing data elements and their classification. [DISA: APSC-DV-003290]</p> <p>Note: If the application does not process classified information, this requirement is not applicable.</p> <p>(3) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on System Documentation.</p>

10.8.6.3.18.3
(09-12-2025)
**SA-10 Developer
Configuration
Management**

- (1) Application files must be cryptographically hashed prior to being deployed to IRS operational networks in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-003140]
- (2) Flaws found during a code review must be tracked in a defect tracking system. [DISA: APSC-DV-003190]

Note: If application development is not being done or managed by the organization, this requirement is not applicable.

- (3) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Developer Configuration Management.

10.8.6.3.18.4
(09-12-2025)
**SA-11 Developer Testing
and Evaluation**

- (1) The application must not be vulnerable to race conditions. [DISA: APSC-DV-001995]

Note: If the application is a commercial off-the-shelf (COTS) application and the vendor will not provide code review test results that demonstrate the application has been tested and is not susceptible to race conditions, this requirement is not applicable.

- (2) At least one tester must be designated to test for security flaws in addition to functional testing. [DISA: APSC-DV-003150]

Note: If the organization operating the application is not doing development work, this requirement is not applicable.

- (3) Test procedures must be created and at least annually executed to ensure system initialization, shutdown, and aborts are configured to verify the system remains in a secure state. [DISA: APSC-DV-003160]
- (4) An application code review must be performed on the application by the developer of the information system, system component, or information system service. [DISA: APSC-DV-003170]

Note: This requirement is meant to apply to developers or organizations that are doing the application development work and have the responsibility for maintaining the application source code. Otherwise, this requirement is not applicable.

- (5) Code coverage statistics must be maintained for each release of the application. [DISA: APSC-DV-003180]

Note: If the organization does not do or manage the application development work for the application, this requirement is not applicable.

- (6) Changes to an application must be assessed for Information Assurance (IA) and accreditation impact prior to implementation. [DISA: APSC-DV-003200]
- (7) Security flaws must be fixed or addressed in the project plan, within the time period directed by an authoritative source (e.g. CSIRC), IRM 10.8.50, **Enterprise Incident, Vulnerability, and Security Patch Management**). [DISA: APSC-DV-003210]

Note: This requirement is meant to apply to developers or organizations that are doing application development work. If the organization managing the application is not performing or managing the development of the application, this requirement is not applicable.

- (8) The test environment must be an approved close simulation of the intended production environment, in which the application will be integrated. [IRS-defined]
- (9) Applications being developed must meet the security requirements defined in the IRM 10.8 series and the applicable OS IRM for the applicable OS environment it will function in. [IRS-defined]
- (10) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Developer Testing and Evaluation.

10.8.6.3.18.5
(09-12-2025)

**SA-15 Development
Process, Standards, and
Tools**

- (1) The application development team must follow a set of coding standards. [DISA: APSC-DV-003215]

Note: This requirement is meant to apply to developers or organizations that are doing application development work. If the organization operating the application under review is not doing the development or managing the development of the application, this requirement is not applicable.

Note: Coding standards are established in concurrence to industry best practices based on programming style and methodology.

Note: Coding standards are implemented under the purview of IRM 2.5.3. to ensure that the appropriate System Development Life Cycle (SDLC) and security requirements are followed. Well-documented and enforceable coding standards are essential to secure software development. Coding standards encourage programmers to follow a uniform set of rules and guidelines determined by the requirements of the project and organization, not by the programmer's familiarity or preference.

- (2) The designer must create and update the Design Document for each release of the application. [DISA: APSC-DV-003220]

Note: This requirement is meant to apply to developers or organizations that are doing application development work. If the organization operating the application is not doing the development or managing the development of the application, this requirement is not applicable.

- (3) Threat models must be documented and reviewed for each application release and updated as required by design and functionality changes or when new threats are discovered. [DISA: APSC-DV-003230]

Note: If the organization operating the application is not doing the development or is not managing the development of the application, this requirement is not applicable.

- (4) The application must not be subject to error handling vulnerabilities. [DISA: APSC-DV-003235]
- (5) The application development team must create an application incident response plan. [DISA: APSC-DV-003236]

Note: If the application is a COTS application and the development team is not accessible to interview, this requirement is not applicable.

- (6) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Development Process, Standards, and Tools.

10.8.6.3.18.6
(09-12-2025)

**SA-22 Unsupported
System Components**

- (1) All products must be supported by the vendor or the development team. [DISA: APSC-DV-003240]
- (2) The application must be decommissioned when maintenance or support is no longer available. [DISA: APCS-DV-003250]
- (3) Procedures must be in place to notify users when an application is decommissioned. [DISA: APCS-DV-003260]
- (4) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Unsupported System Components.

10.8.6.3.19
(09-12-2025)

**SC - System and
Communications
Protection**

- (1) In addition to the System and Communication Protection guidance defined within this IRM, the following controls must be implemented in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable).
- SC-01 Policy and Procedures
 - SC-06 Resource Availability
 - SC-12 Cryptographic Key Establishment and Management
 - SC-15 Collaborative Computing Devices and Applications
 - SC-16 Transmission of Security and Privacy Attributes
 - SC-20 Secure Name or Address Resolution Service (Authoritative Source)
 - SC-21 Secure Name or Address Resolution Service (Recursive or Caching Resolver)
 - SC-22 Architecture and Provisioning for Name or Address Resolution Service
 - SC-25 Thin Nodes
 - SC-26 Decoys
 - SC-27 Platform-Independent Applications
 - SC-29 Heterogeneity
 - SC-30 Concealment and Misdirection
 - SC-31 Covert Channel Analysis
 - SC-32 System Partitioning
 - SC-34 Non-Modifiable Executable Programs
 - SC-35 External Malicious Code Identification
 - SC-36 Distributed Processing and Storage
 - SC-37 Out-of-Band Channels
 - SC-38 Operations Security
 - SC-40 Wireless Link Protection
 - SC-41 Port and I/O Device Access
 - SC-42 Sensor Capability and Data
 - SC-43 Usage Restrictions
 - SC-44 Detonation Chambers
 - SC-45 System Time Synchronization
 - SC-46 Cross Domain Policy Enforcement
 - SC-47 Alternate Communication Paths
 - SC-48 Sensor Relocation
 - SC-49 Hardware-Enforced Separation and Policy Enforcement

- SC-50 Software-Enforced Separation and Policy Enforcement
- SC-51 Hardware-Based Protection

10.8.6.3.19.1
(09-12-2025)

**SC-02 Separation of
System and User
Functionality**

- (1) The application user interface must be either physically or logically separated from data storage and management interfaces. [DISA: APCS-DV-002150]
- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Separation of System and User Functionality.

10.8.6.3.19.2
(09-12-2025)

**SC-03 Security Function
Isolation**

- (1) The application must set the HTTPOnly flag on session cookies. [DISA: APSC-DV-002210]
- (2) The application must set the secure flag on session cookies. [DISA: APSC-DV-002220]
- (3) The application must not expose session IDs. [DISA: APSC-DV-002230]
- (4) The application must destroy the session ID value and or cookie on logoff or browser close. [DISA: APSC-DV-002240]
- (5) The application must isolate security functions from non-security functions. [DISA: APSC-DV-002360]
- (6) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Security Function Isolation.

10.8.6.3.19.3
(09-12-2025)

**SC-04 Information in
Shared System
Resources**

- (1) The application must prevent unauthorized and unintended information transfer via shared system resources. [DISA: APSC-DV-002380]
- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Information in Shared System Resources.

10.8.6.3.19.4
(09-12-2025)

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

- (1) Extensible markup language (XML)-based applications must mitigate Denial-of-Service (DoS) attacks by using XML filters, parser options, or gateways. [DISA: APSC-DV-002390]

Note: If the application does not contain or utilize XML, this requirement is not applicable.

- (2) The application must restrict the ability to launch DoS attacks against itself or other information systems. [DISA: APSC-DV-002400]
- (3) The web service design must include redundancy mechanisms when used with high-availability systems.

Note: If the application has not been designated as a high availability system, this requirement is not applicable.

[DISA: APSC-DV-002410]

- (4) Protections against DoS attacks must be implemented. [DISA: APSC-DV-003320]
- (5) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Denial-of-Service Protection.

10.8.6.3.19.5
(09-12-2025)
**SC-07 Boundary
Protection**

- (1) Connections between the IRS operational networks and the Internet or other public or commercial wide area networks must require a DMZ. [DISA: APSC-DV-003350]
- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Boundary Protection.

10.8.6.3.19.6
(09-12-2025)
**SC-08 Transmission
Confidentiality and
Integrity**

- (1) The application must protect the confidentiality and integrity of transmitted information in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-002440]
- (2) The application must implement cryptographic mechanisms to prevent unauthorized disclosure of information and or detect changes to information during transmission unless otherwise protected by alternative physical safeguards, such as, at a minimum, a Protected Distribution System (PDS). [DISA: APSC-DV-002450]
- (3) The application must maintain the confidentiality and integrity of information during preparation for transmission. [DISA: APSC-DV-002460]
- (4) The application must maintain the confidentiality and integrity of information during reception. [DISA: APSC-DV-002470]
- (5) The application must not disclose unnecessary information to users. [DISA: APSC-DV-002480]
- (6) The application must not store sensitive information in hidden fields. [DISA: APSC-DV-002485]
- (7) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Transmission Confidentiality and Integrity.

10.8.6.3.19.7
(09-12-2025)
**SC-10 Network
Disconnect**

- (1) The application must terminate all network connections associated with a communications session at the end of the session. [DISA: APSC-DV-002000]
- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Network Disconnect.

10.8.6.3.19.8
(09-12-2025)
**SC-13 Cryptographic
Protection**

- (1) The application must utilize FIPS-validated cryptographic modules when signing application components. [DISA: APSC-DV-002020]
- (2) The application must utilize FIPS-validated cryptographic modules when generating cryptographic hashes. [DISA: APSC-DV-002030]
- (3) The application must utilize FIPS-validated cryptographic modules when protecting unclassified information that requires cryptographic protection. [DISA: APSC-DV-002040]
- (4) Applications making SAML assertions must use FIPS-approved random numbers in the generation of SessionIndex in the SAML Element <AuthnStatement>. [DISA: APSC-DV-002050]
- (5) If the application contains classified data, the application must implement National Security Agency (NSA)-approved cryptography to protect classified information in accordance with applicable federal laws, executive orders, directives, policies, regulations, and standards. [DISA: APSC-DV-002010]

Note: If the application does not process classified data, this requirement is not applicable.

- (6) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Cryptographic Protection.

10.8.6.3.19.9
(09-12-2025)
SC-17 PKI Certificate Validation

- (1) Public Key Infrastructure (PKI) must be implemented in accordance with IRM 10.8.1 and IRM 10.8.52, *Information Technology (IT) Security, IRS PKI Security Policy*.
- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on PKI Certificate Validation.

10.8.6.3.19.10
(09-12-2025)
SC-18 Mobile Code

- (1) Unsigned Category 1A mobile code must not be used in the application in accordance with IRS policy. [DISA: APSC-DV-002870]

Note: If the application does not contain mobile code, or if the mobile code executes within the client browser, this requirement is not applicable.

- (2) The designer must ensure uncategorized or emerging mobile code is not used in applications. [DISA: APSC-DV-003300]
- (3) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Mobile Code.

10.8.6.3.19.11
(09-12-2025)
SC-23 Session Authenticity

- (1) Applications must use system-generated session identifiers that protect against session fixation. [DISA: APSC-DV-002250]

Note: If the application does not use SAML assertions, this requirement is not applicable.

- (2) Applications must validate session identifiers. [DISA: APSC-DV-002260]
- (3) Applications must not use uniform resource locator (URL) embedded session IDs. [DISA: APSC-DV-002270]
- (4) The application must not re-use or recycle session IDs. [DISA: APSC-DV-002280]
- (5) The application must use the FIPS validated cryptographic modules and random number generator if the application implements encryption, key exchange, digital signature, and hash functionality. [DISA: APSC-DV-002290]
- (6) The application must only allow the use of IRS-approved certificate authorities for verification of the establishment of protected sessions in accordance with IRM 10.8.52. [DISA: APSC-DV-002300]
- (7) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Session Authority.

10.8.6.3.19.12
(09-12-2025)
SC-24 Fail in Known State

- (1) The application must fail to a secure state if system initialization fails, shutdown fails, or aborts fail. [DISA: APSC-DV-002310]

- (2) In the event of a system failure, applications must preserve any information necessary to determine cause of failure and any information necessary to return to operations with least disruption to mission processes. [DISA: APSC-DV-002320]
- (3) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Fail in Known State.

10.8.6.3.19.13
(09-12-2025)
**SC-28 Protection of
Information at Rest**

- (1) The application must protect the confidentiality and integrity of stored information in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-002330]
- (2) The application must implement approved cryptographic mechanisms to prevent unauthorized modification of IRS-defined information at rest on IRS-defined information system components in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable). [DISA: APSC-DV-002340]

Note: If the data the application processes is strictly publicly releasable information and system documentation specifies no data encryption is required for any hosted application data, this is not applicable.

- (3) The application must use appropriate cryptography in order to protect stored IRS information when required by the information owner or IRS policy in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable)¹. [DISA: APSC-DV-002350]

Note: If the data the application processes is strictly publicly releasable information with no sensitive but unclassified (SBU), FOUO, or classified and system documentation specifies no data encryption is required for any hosted application data, this requirement is not applicable.

- (4) Production database exports must have database administration credentials and sensitive data removed before releasing the export. [DISA: APSC-DV-003310]

Note: If no data is exported to test or development databases, this requirement is not applicable.

- (5) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Protection of Information at Rest.

10.8.6.3.19.14
(09-12-2025)
SC-39 Process Isolation

- (1) The application must maintain a separate execution domain for each executing process. [DISA: APSC-DV-002370]
- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Process Isolation.

10.8.6.3.20
(09-12-2025)
**SI - System and
Information Integrity**

- (1) In addition to the System and Information Integrity guidance defined within this IRM, the following controls must be implemented in accordance with IRM 10.8.1 or IRM 10.8.24 (as applicable):
 - S1-01 Policy and Procedures
 - SI-03 Malicious Code Protection
 - SI-07 Software, Firmware and Information Integrity
 - SI-08 Spam Protection

- SI-12 Information Management and Retention
- SI-13 Predictable Failure Prevention
- SI-14 Non-Persistence
- SI-15 Information Output Filtering
- SI-17 Fail Safe Procedures
- SI-18 Personally Identifiable Information Quality Operations
- SI-19 De-Identification
- SI-20 Tainting
- SI-21 Information Refresh
- SI-22 Information Diversity
- SI-23 Information Fragmentation

10.8.6.3.20.1
(09-12-2025)

SI-02 Flaw Remediation

- (1) The application must remove IRS-defined software components after updated versions have been installed. [DISA: APSC-DV-002610]
- (2) Security-relevant software updates and patches must be kept up to date. [DISA: APSC-DV-002630]
- (3) Security Patch Management must be implemented in accordance with IRM 10.8.1 and IRM 10.8.50, *Information Technology (IT) Security, Enterprise Incident, Vulnerability, and Security Patch Management*.
- (4) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Flaw Remediation.

10.8.6.3.20.2
(09-12-2025)

SI-04 System Monitoring

- (1) The system must alert an administrator when low resource conditions are encountered. [DISA: APSC-DV-003330]
- (2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on System Monitoring.

10.8.6.3.20.3
(09-12-2025)

SI-05 Security Alerts, Advisories, and Directives

- (1) At least one application administrator must be registered to receive update notifications or security alerts, when automated alerts are available. [DISA: APSC-DV-003340]
- (2) The application must provide notifications or alerts when product update and security related patches are available. [DISA: APSC-DV-003345]
- (3) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Security Alerts, Advisories, and Directives.

10.8.6.3.20.4
(09-12-2025)

SI-06 Security and Privacy Function Verification

- (1) The application performing IRS-defined security functions must verify correct operation of security functions. [DISA: APSC-DV-002760]
- (2) The application must perform verification of the correct operation of security functions. [DISA: APSC-DV-002770]
 - a. Upon system startup and or restart; upon command by a user with privileged access; and or every 30 days in accordance with IRM 10.8.1 . (L, M)
 - b. In accordance with IRM 10.8.1. (H)
- (3) The application must notify the ISSO and ISSM (Information Systems Security Manager) of failed security verification tests. [DISA: APSC-DV-002780]

	(4) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Security and Privacy Function Verification.
10.8.6.3.20.5 (09-12-2025) SI-10 Information Input Validation	<p>(1) The application must protect from Cross-Site Scripting (XSS) vulnerabilities. [DISA: APSC-DV-002490]</p> <p>(2) The application must protect from Cross-Site Request Forgery (CSRF) vulnerabilities. [DISA: APSC-DV-002500]</p> <p>(3) The application must protect from command injection. [DISA: APSC-DV-002510]</p> <p>(4) The application must protect from canonical representation vulnerabilities. [DISA: APSC-DV-002520]</p> <p>(5) The application must validate all input. [DISA: APSC-DV-002530]</p> <p>(6) The application must not be vulnerable to SQL injection. [DISA: APSC-DV-002540]</p> <p>(7) The application must not be vulnerable to XML-oriented attacks. [DISA: APSC-DV-002550]</p> <p>Note: If the application does not process XML, this requirement is not applicable.</p> <p>(8) The application must not be subject to input handling vulnerabilities. [DISA: APSC-DV-002560]</p> <p>(9) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Input Validation.</p>
10.8.6.3.20.6 (09-12-2025) SI-11 Error Handling	<p>(1) The application must generate error messages that provide information necessary for corrective actions without revealing information that could be exploited by adversaries. [DISA: APSC-DV-002570]</p> <p>(2) The application must reveal error messages only to the SSO or SA. [DISA: APSC-DV-002580]</p> <p>(3) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Error Handling.</p>
10.8.6.3.20.7 (09-12-2025) SI-16 Memory Protection	<p>(1) The application must not be vulnerable to overflow attacks. [DISA: APSC-DV-002590]</p> <p>(2) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Memory Protection.</p>
10.8.6.3.21 (09-12-2025) SR - Supply Chain Risk Management	<p>(1) Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) for additional guidance on Supply Chain Risk Management.</p>

This Page Intentionally Left Blank

#

#####

#

#####

[illegible]

[illegible][illegible]

#####

[illegible][illegible]

[illegible]

#####

[illegible][illegible]

[illegible]

#####

##

[illegible]

[illegible]

#

Exhibit 10.8.6-5 (09-12-2025)**Related Resources****IRS Publications**

- 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 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy*.
- IRM 10.8.50, *Information Technology (IT) Security, Enterprise Incident, Vulnerability, and Security Patch Management*.
- IRM 10.8.52, *Information Technology (IT) Security, IRS Public Key Infrastructure (PKI) X.509 Certificate Policy*.
- IRM 10.8.60, *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) Process*
- IRM 10.9.1, *Classified National Security Information (CNSI)*.
- IRM 2.5.3, *Systems Development, Programming and Source Code Standards*

Department of the Treasury Publications

- TD P 85-01: Treasury Directive Publication 85-01 Version 3.1.3, *"Treasury Information Technology (IT) Security Program"*, issued February 28, 2022.

National Institute of Standards and Technology (NIST) Publications

- FIPS Pub 140-2: Federal Information Processing Standards Publication 140-2, **"Security Requirements for Cryptographic Modules"**, issued May 25, 2001 (Change Notice 2, 12/3/2002).
- FIPS Pub 140-3: Federal Information Processing Standards Publication 140-3, *"Security Requirements for Cryptographic Modules"*, March 22, 2019.
- FIPS Pub 199: Federal Information Processing Standards Publication 199, *"Standards for Security Categorization of Federal Information and Information Systems"* February 1, 2004.
- FIPS Pub 200: Federal Information Processing Standards Publication 200, *"Minimum Security Requirements for Federal Information and Information Systems"*. March 1, 2006
- SP 800-28 : NIST Special Publication 800-28 Version 2, *"Guidelines on Active Content and Mobile Content"*, issued March 2008.
- SP 800-37: NIST Special Publication 800-37 Revision 2, *"Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy"*, issued December 20, 2018.
- SP 800-53: NIST Special Publication 800-53 Revision 5.1.1 *"Security and Privacy Controls for Information Systems and Organizations"*, issued November 7, 2023.
- SP 800-53A: NIST Special Publication 800-53A Revision 5 *"Guide for Assessing the Security Controls in Federal Information Systems and Organizations"*, issued January 2022.
- SP 800-218: NIST Special Publication 800-218 Version 1.1, *"Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities"*, issued February 2022.

Defense Information Systems Agency (DISA) Publications

- Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG): *Application Security and Development V6R1*, July 24, 2024.
- STIGs are used as a basis for producing IRS Security Requirements Checklists. The security requirements checklists are updated as DISA releases updated guidance and are posted on the IRS

Exhibit 10.8.6-5 (Cont. 1) (09-12-2025)**Related Resources**

Security Control Exhibit SharePoint site. The DISA version and release for each guide is contained within each checklist. Refer to the Security Requirements Checklists exhibit for additional information.

- DISA Security Guides are available at: *DISA Security Guides* site.

Executive Orders

- EO: 14028: Executive Order 14028, “*Improving the Nation’s Cybersecurity*,” issued May 12, 2021.

Other Publications

- Open Web Application Security Project (OWASP):
 - *OWASP Testing Guide v4.2*
 - *OWASP Developer Cheat Sheets v2*
 - *Application Security Desk Reference (ASDR)*
 - *OWASP Application Security Verification Standard*
 - *OWASP API Top 10*
- *AJAX (Asynchronous JavaScript and XML) and other “Rich” Interface Technologies*.
- Information Assurance Technology Analysis Center (IATAC) Software Security Assurance State of the Art Report (SOAR), July 31, 2007.
- *Java Community of Practice SharePoint site*.

