



# MANUAL TRANSMITTAL

Department of the Treasury  
Internal Revenue Service

10.8.22

MAY 12, 2025

## EFFECTIVE DATE

(05-12-2025)

## PURPOSE

- (1) This transmits revised IRM 10.8.22, *Information Technology (IT) Security, Web Server Security Policy*.

## MATERIAL CHANGES

- (1) IRM 10.8.22.1 updated to align with IRM 1.11.2, Internal Management Documents System, Internal Revenue Manual (IRM) Process Internal Controls.
- (2) Throughout this IRM, requirements written with “shall” verbiage updated to “must” to align with industry writing best practices.
- (3) IRM 10.8.22, IRM Part title updated to include Artificial Intelligence.
- (4) IRM 10.8.22, Audience updated to align with Security Policy Boilerplate.
- (5) IRM 10.8.22.1, Program Scope and Objectives updated to align with Security Policy Boilerplate.
- (6) IRM 10.8.22.1.3, Roles and Responsibilities updated to align with Security Policy Boilerplate.
- (7) IRM 10.8.22.1.8, Risk Acceptance and Risk-Based Decisions updated URL for accurate FISMA Doc Library location.
- (8) IRM 10.8.22.2, IT Roles and Responsibilities added to align with Security Policy Boilerplate
- (9) IRM 10.8.22.2.1.1, Created new subsection - AC-02 Account Management.
- (10) IRM 10.8.22.2.3.4, Created new subsection - AU-06 Audit Review, Analysis, and Reporting.
- (11) IRM 10.8.22.2.3.6, AU-09 Protection of Audit Information - Added subsection 4).
- (12) IRM 10.8.22.2.3.8, AU-14 Session Audit - Revised to incorporated Interim Guidance (IG) Memorandum # IT-10-1222-0030 - Policy Update Internal Revenue Manual (IRM) 10.8.22, Web Server Defense Information Systems Agency (DISA) Security Requirement.
- (13) IRM 10.8.22.2.5.1, CM-05 Access Restrictions for Change - Added subsection 4).
- (14) IRM 10.8.22.2.5.4, Created new subsection - CM-14 Signed Components.
- (15) IRM 10.8.22.2.7.1, Created new subsection - IA-02 Identification and Authentication (Organizational Users).
- (16) IRM 10.8.22.2.7.2, IA-05 Authenticator Management - Added Subsections 1) through 10).
- (17) IRM 10.8.22.2.9.1, Created new subsection - MA-04 Non-Local Maintenance.
- (18) IRM 10.8.22.2.16.4, SC-08 Transmission Confidentiality and Integrity - Updated content in subsection 2) and added subsection 10) through 12).
- (19) IRM 10.8.22.2.16.6, SC-17 Public Key Infrastructure Certificates - Added subsection 5).

- (20) IRM 10.8.22.2.16.8, SC-23 Session Authenticity - Added subsection 1a) and 1b) and updated content of subsection 5).
- (21) IRM 10.8.22.2.16.10, SC-28 Protection of Information at Rest - Added subsection 3).
- (22) IRM 10.8.22.2.16.11, Created new subsection - SC-45 System Time Synchronization.
- (23) IRM 10.8.22.2.17.2, SI-10 Information Input Validation - Added subsections 2) and 3).
- (24) IRM Exhibit 10.8.22-1, added Subsection 1) to also include subsections a) through d).
- (25) IRM Exhibit 10.8.22-1, Added the title of IRM 10.8.50 in subsection 3).
- (26) IRM Exhibit 10.8.22-1, Added test to subsection 4).
- (27) IRM Exhibit 10.8.22-2 Updated the Terms and Acronyms
- (28) IRM Exhibit 10.8.22-3 References, Updated References to Related Resources.
- (29) IRM Exhibit 10.8.22-3 References, Updated the National Institute of Standards and Technology (NIST) Publications section.
- (30) IRM Exhibit 10.8.22-3 References, Added content to the Defense Information Systems Agency (DISA) Publications.
- (31) IRM Exhibit 10.8.22-3 References, Added Public Law reference.
- (32) IRM Exhibit 10.8.22-3 References, Added U.S. Code reference.
- (33) IRM Exhibit 10.8.22-3 References, Added Executive Orders reference.
- (34) IRM Exhibit 10.8.22-3 References, Added Office of Management and Budget (OMB) Circular reference.
- (35) IRM Exhibit 10.8.22-3 References, Added Office of Management and Budget (OMB) Memoranda reference.
- (36) Entire IRM - Added the leading zero to the control numbers to align with NIST.
- (37) Updated Responsible Official from Kaschit Pandya to Rajiv Uppal.
- (38) Editorial changes (including grammar, spelling, and minor clarifications) were made throughout the IRM.

#### **EFFECT ON OTHER DOCUMENTS**

IRM 10.8.22 dated November 03, 2023, is superseded. This IRM supplements IRM 10.8.1, Information Technology (IT) Security, Security Policy and IRM 10.8.2 Information Technology (IT) Security, Security Roles and Responsibilities. This IRM incorporates Interim Guidance (IG) Memorandum # IT-10-1222-0030 - Policy Update Internal Revenue Manual (IRM) 10.8.22, Web Server Defense Information Systems Agency (DISA) Security Requirement.

**AUDIENCE**

IRM 10.8.22 must be distributed to all personnel responsible for ensuring that adequate security is provided for IRS information and systems. This policy applies to all employees, contractors, and vendors of the IRS.

Rajiv Uppal  
Chief Information Officer



## Web Server Security Policy

#### 10.8.22.1 Program Scope and Objectives

- ### 10.8.22.3 IT Security Controls

[illegible]

[illegible]

10.8.22-1	Security Requirements Checklists
10.8.22-2	Terms and Acronyms
10.8.22-3	Related Resources

10.8.22.1  
(05-12-2025)  
**Program Scope and Objectives**

- (1) **Overview:** This IRM lays the foundation to implement and manage security controls and guidance for the use of web servers within the IRS.
  - a. This IRM is subordinate to *IRM 10.8.1, Information Technology (IT) Security, Security Policy*, and augments the existing requirements identified in IRM 10.8.1, as they relate to IRM web servers for on-premise systems, including on-premise 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 web servers for off-premise cloud deployments.
- (2) **Purpose of the Program:** Develop and publish policies to protect the IRS against potential security threats, risks and vulnerabilities and ensure compliance with federal mandates and legislation.
- (3) **Audience:** The provisions within this manual apply to:
  - a. All offices and businesses, operating, and functional units within the IRS.
  - b. IRS Personnel and organizations having contractual arrangements with the IRS including employees, contractors, vendors, and outsourcing providers, which use or operate systems that store, process, or transmit IRS Information or connect to an IRS network or system.
- (4) **Policy Owner:** Chief Information Officer (CIO)
- (5) **Program Owner:** Cybersecurity, Cybersecurity Threat Response & Remediation
- (6) **Program Goals:** To protect the confidentiality, integrity, and availability of IRS information and information systems.

10.8.22.1.1  
(02-08-2022)  
**Background**

- (1) Web servers provide data via an internally or publicly-exposed interface and are well-known targets for exploitation. Unprotected Web servers provide an avenue for malicious activity such as theft or the denial of service to IRS resources. An improperly implemented server can be attacked directly and be used as a staging area to obtain unauthorized access to IRS internal resources.
  - a. This IRM defines the security controls for Web servers.
  - b. This IRM provides the security configuration standards required to ensure Web server software is integrated and used appropriately for all IRS systems.
- (2) IRM 10.8.22, is part of the IRM 10.8. Information Technology (IT) Security series for IRS IT Cybersecurity.

10.8.22.1.2  
(02-08-2022)  
**Authority**

- (1) All IRS systems and applications are required to comply with Executive Orders (E.O.s), 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), Treasury, and IRS guidelines as they apply.

10.8.22.1.3  
(11-03-2023)

**Roles and  
Responsibilities**

- (1) The IRS must implement security roles in accordance with federal laws and IT security guidelines (e.g., FISMA, NIST, OMB) that are appropriate for their specific operations and missions. The roles and responsibilities are defined in *IRM 10.8.2, Information Technology (IT) Security, IT Security Roles and Responsibilities*.
- (2) The supplemental roles and responsibilities specific to the implementation of web servers are in, *IRM 10.8.22.3, IT Roles and Responsibilities subsection of this IRM*.

10.8.22.1.4  
(05-12-2025)

**Program Management  
and Review**

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

10.8.22.1.5  
(05-12-2025)

**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, DISA) for potential revisions to security policies and security requirements checklists. Revision to security policies and checklists are reviewed by the security policy team, in collaboration with applicable stakeholders, for potential impact to the IRS operational environment.
- (2) Security Policy provides a report identifying security policies and security requirements checklists that have recently been revised or are in the process of being revised.
- (3) For systems that store, process, or transmit classified national security information, refer to IRM 10.9.1, *Classified National Security Information (CNSI)*, for additional guidance for protecting classified information.
- (4) This IRM establishes the minimum baseline security policy and requirements for all web servers.



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

10.8.22.1.6  
(05-12-2025)

**Terms and Acronyms**

- (1) Refer to Exhibit 10.8.22-2, Terms and Acronyms for a list of terms, acronyms, and definitions.

10.8.22.1.7  
(05-12-2025)

**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 10.8.22-3, Related Resources for a list of related resources and references.

10.8.22.1.8  
(02-08-2022)

**Risk Acceptance and  
Risk-Based Decisions**

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

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

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

10.8.22.2  
(05-12-2025)

**IT Roles and  
Responsibilities**

- (1) This IRM does not contain supplemental roles and responsibilities specific to the implementation of Web Server Security Policy.

10.8.22.3  
(05-12-2025)

**IT Security Controls**

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

#  
#  
#  
  
#  
#  
#  
#

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

[illegible]

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

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

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

[illegible]

[illegible]



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

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

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

[illegible]

[illegible]

[illegible]

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

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



[illegible]

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

**Exhibit 10.8.22-1 (05-12-2025)**  
**Security Requirements Checklists**

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

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

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

- a. Select the appropriate IRM folder.
- b. Security Checklists are available for the following:
  - General Web Server
  - Apache HTTP Server
  - Microsoft Intranet Information Server (IIS)
- 3. Security Checklists are effective immediately. Vulnerabilities must be remediated in accordance with IRM 10.8.50, **Information Technology (IT) Security, Enterprise Incident, Vulnerability, and Security Patch Management** remediation time lines table. The source's publication date can be found in the external reference row of the checklist. (Typically row 10)
- 4. Checklists for technologies identified as 'Beyond Sunset' or 'Remove' by Enterprise Architecture (EA) Enterprise Standards Profile (ESP) won't receive further updates. These checklists will be removed from the active checklist and moved to an 'Archive' folder during the next checklist update cycle.
- 5. Evaluate system configurations and implement controls while protecting system functionality.

**Exhibit 10.8.22-2 (05-12-2025)**  
**Terms and Acronyms**

<b>Term</b>	<b>Definition or description</b>
<b>Authentication</b>	The process of verifying the identity or location of a user, service or application. Authentication is performed using at least one of three mechanisms: “something you have”, “something you know” or “something you are”. The authenticating application may provide different services based on the location, access method, time of day, etc.
<b>Authorization</b>	The determination of what resources a user, service or application has permission to access. Accessible resources can be URLs, files, directories, servlets, databases, execution paths, etc.
<b>Authorizing Official (AO)</b>	See IRM 10.8.2 for a detailed description of an AO’s responsibilities.
<b>Basic Authentication</b>	A simple form of client-side authentication supported in HTTP. The http-client sends a request header to the web server containing a Base64 encoded username and password. If the username/password combination is valid, the web server grants the client access to the requested resource.
<b>BEARS</b>	Business Entitlement Access Request System (BEARS)
<b>CA</b>	Certification Authority
<b>CIO</b>	Chief Information Officer
<b>Cipher Suite</b>	A named combination of authentication, encryption, and message authentication code algorithms use to negotiate the security settings for a network connection using a network protocol.
<b>CIS</b>	Center for Information Security
<b>CMMI</b>	Capability Maturity Model Integration
<b>CNSI</b>	Classified National Security Information
<b>Common Gateway Interface (CGI)</b>	Programming standard for software to interface and execute applications residing on web servers.

**Exhibit 10.8.22-2 (Cont. 1) (05-12-2025)**  
**Terms and Acronyms**

<b>Compiler</b>	A computer program that translates a high-level programming language into machine readable language. The compiler usually converts the high-level language into assembly language first, and then translates the assembly language into machine language. The program fed into the compiler is called the source program; the generated machine language program is called the object program.
<b>CRL</b>	Certificate Revocation List
<b>CTL</b>	Certificate Trust List
<b>DoS</b>	Denial of Service
<b>EA</b>	Enterprise Architecture
<b>Enterprise Architecture (EA) Enterprise Standards Profile (ESP)</b>	The authoritative repository for IRS approved products and standards.
<b>EO</b>	Executive Order
<b>System Development Life Cycle (SDLC)</b>	Enterprise architecture is the dynamic, iterative process of changing the enterprise overtime by incorporating new business processes, new technology, and new capabilities, as well as maintenance, disposition and disposal of existing elements of the enterprise.
<b>File Transfer Protocol (FTP)</b>	A client/server protocol for exchanging files with a host computer.
<b>Federal Information Processing Standards (FIPS)</b>	A set of standards that describe document processing, encryption algorithms and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies.
<b>Federal Information Security Modernization Act (FISMA)</b>	Federal Information and Modernization Act (FISMA) 2014
<b>GMT</b>	Greenwich Mean Time
<b>HyperText Transfer Protocol (HTTP)</b>	A protocol scheme used on the World Wide Web. HTTP describes the way a web-client requests data and how a web server responds to those requests.
<b>HyperText Transfer Protocol Secure (HTTPS)</b>	A secure form of communication over a computer network by layering HTTP on top of the SSL/TLS protocol.

**Exhibit 10.8.22-2 (Cont. 2) (05-12-2025)**  
**Terms and Acronyms**

<b>Internet Information Services (IIS)</b>	Formerly known as Internet Information Server, is a web server product by Microsoft and is used with Microsoft operating systems.
<b>Internet Protocol (IP)</b>	The principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries.
<b>Internet Server Application Program Interface (ISAPI)</b>	An API for Microsoft's Internet Information Server (IIS) Web server. ISAPI enables programmers to develop Web-based applications running faster than conventional CGI programs.
<b>ISSO</b>	Information System Security Officer
<b>IT</b>	Information Technology
<b>ITIL</b>	Information Technology Infrastructure Library
<b>Internal Web Server</b>	A private server with a private IP address and is not visible to the Internet (i.e., irweb.irs.gov).
<b>LSS</b>	Lean Six Sigma
<b>Metabase</b>	A repository for most Internet Information Services (IIS) configuration values. The metabase is a plaintext XML file and can be edited manually or programmatically. The metabase is efficiently extensible. As IIS deployment grows, so does the metabase.
<b>MIME</b>	Multipurpose Internet Mail Extensions
<b>NARA</b>	National Archives and Records Administration
<b>NIST</b>	National Institute of Standards and Technology
<b>OMB</b>	Office of Management and Budget
<b>Public Key Infrastructure (PKI)</b>	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
<b>Public Web Server</b>	A server that is configured with a public IP address and is completely visible to the Internet (i.e., irs.gov).
<b>RBD</b>	Risk Based Decision
<b>RFC</b>	Request for Comments
<b>SA</b>	System Administrator
<b>SA&amp;A</b>	Security Assessment and Authorization

**Exhibit 10.8.22-2 (Cont. 3) (05-12-2025)**  
**Terms and Acronyms**

<b>SBU</b>	Sensitive But Unclassified
<b>Secure Sockets Layer (SSL)</b>	An industry standard public-key protocol used to create encrypted tunnels between two network-connected devices.
<b>Session ID</b>	A string of data provided by the web server, normally stored within a cookie or URL. A Session ID tracks a user's session, or perhaps just his current session, as he traverses the web site.
<b>Script</b>	A program run on a Web server, in response to input from a browser.
<b>Scripting language</b>	A programming language that allows control of one or more applications and makes the compiler of the language part of the language runtime, and as a result, enables code to be generated dynamically. "Scripts" are distinct from the core code of the application, as they are usually written in a different language and are often created or at least modified by the end-user.
<b>SOP</b>	Standard Operating Procedure
<b>SRG</b>	Security Requirements Guide
<b>SRM</b>	Security Risk Management
<b>SSP</b>	System Security Plan
<b>STIG</b>	Security Technical Implementation Guide
<b>TCP</b>	Transmission Control Protocol
<b>TD</b>	Treasury Directive
<b>Transport Layer Security (TLS)</b>	An authentication and security protocol widely implemented in browsers and Web servers.
<b>Universal Resource Locator (URL)</b>	A standard way of specifying the location of an object, normally a web page, on the Internet.
<b>UTC</b>	Coordinated Universal Time
<b>WebDAV</b>	Web Distributed Authoring
<b>Web Server</b>	A general-purpose software application that handles and responds to HTTP requests. A web server may utilize a web application for dynamic web page content.

Exhibit 10.8.22-2 (Cont. 4) (05-12-2025)  
Terms and Acronyms

Web Service	A software application that uses Extensible Markup Language (XML) formatted messages to communicate over HTTP. Typically, software applications interact with web services rather than normal users.
-------------	--



**Exhibit 10.8.22-3 (05-12-2025)****Related Resources****IRS Publications**

- IRM 1.15. series - *Records and Information Management*
- IRM 10.2. - *Physical Security Program*
- IRM 10.8.1 – *Information Technology (IT) Security, Security Policy*
- IRM 10.8.2 – *Information Technology (IT) Security, Security Roles and Responsibilities*
- IRM 10.8.6 - *Information Technology (IT) Security, Application Security and Development*
- IRM 10.8.50 - *Information Technology (IT) Security, Enterprise Incident, Vulnerability, and Security Patch Management*
- IRM 10.8.52 - *Information Technology (IT) Security, PKI Security Policy*
- IRM 10.8.60 - *Information Technology (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance*
- IRM 10.9.1 - *Classified National Security Information (CNSI)*

**Note:** IRS IRMs are available on *IRM Online*.

**Department of the Treasury Publications**

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

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

- NIST: FIPS 140-2: Federal Information Processing Standards Publication 140-2, “*Security Requirements for Cryptographic Modules*,” issued May 25, 2001 (Change Notice 2, 12/3/2002).
- NIST: FIPS 140-3: Federal Information Processing Standards Publication 140-3, “*Security Requirements for Cryptographic Modules*,” issued March 22, 2019.
- NIST: Pub 199: Federal Information Processing Standards 199, “*Standards for Security Categorization of Federal Information and Information Systems*,” issued February 2004.
- NIST: FIPS 200: Federal Information Processing Standards 200, “*Minimum Security Requirements for Federal Information and Information Systems*,” issued March 2006.
- NIST: 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 2018. NIST SP 800-52 Rev 2 *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, August 2019.
- NIST: 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.
- NIST: SP 800-53A: NIST Special Publication 800-53A Revision 5, “*Assessing Security and Privacy Controls in Information Systems and Organizations*,” issued January 2022.
- NIST: SP 800-53B: National Institute of Standards and Technology Special Publication 800-53B, “*Control Baselines for Information Systems and Organizations*” issued December 10, 2020.

**Defense Information Systems Agency (DISA) Publications**

- Web Server SRG V4R1, July 24, 2024
- STIGS are used as a basis for producing IRS Exhibit Checklists. The security checklists are updated as DISA releases updated guidance and are posted on the IRS Security Requirements Checklists 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 the *DISA* site.

**Exhibit 10.8.22-3 (Cont. 1) (05-12-2025)****Related Resources****Center for Internet Security Publications**

- CIS Benchmarks are used as a basis for producing IRS Security Requirements Checklists. The security checklists are updated as CIS releases updated guidance and are posted in the IRS Security Control Exhibit SharePoint site. The CIS version for each benchmark is contained within each checklist. Refer to the Security Requirements Checklists exhibit for additional information.
- CIS benchmarks are available at the *CIS* site.

**Public Law**

- Federal: PL 113-283: Public Law 113-283, "Federal Information Security Modernization Act of 2014," issued December 18, 2014.

**U.S. Code**

- USC: 44 USC 3551: Title 44 U.S. Code Section 3551, "Purposes," issued December 18, 2014.

**Executive Orders**

- EO: 13960: Executive Order 13960, "Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government," issued December 3, 2020.

**Office of Management and Budget (OMB) Circular**

- OMB: A-130: Office of Management and Budget Circular No. A-130, "Management of Information as a Strategic Resource," issued July 27, 2016.

**Office of Management and Budget (OMB) Memoranda**

- OMB: M-22-09: Office of Management and Budget Memorandum 22-09, "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," issued January 26, 2022.