



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.23

AUGUST 27, 2025

EFFECTIVE DATE

(08-27-2025)

PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.8.23, *Information Technology (IT) Security, Application Server Security Policy*.

MATERIAL CHANGES

- (1) Signature: Updated the name of the Chief Information Officer.
- (2) IRM 10.8.23.1, Program Scope and Objectives:
 - a. Paragraph (1)(b): Added reference to IRM 10.8.24, Information Technology (IT), Cloud Computing Security Policy.
 - b. Paragraph (2): Changed subsection title from Purpose of the Program to Program Purpose.
 - c. Paragraph (2)(c): Added statement to indicate that IRM 10.8.23 applies to all NIST impact-level baselines unless a requirement indicates differently.
- (3) IRM 10.8.23.1.3, Roles and Responsibilities: Added a statement about newly added subsection for IT Roles and Responsibilities specific to application servers.
- (4) IRM 10.8.23.1.5, Program Controls:
 - a. Paragraph (5): Added new paragraph to explain security baselines, risk impact levels, and overlay designators.
 - b. Paragraph (6): Added new paragraph to explain newly implemented requirement citation system for the IRM 10.8 series.
- (5) IRM 10.8.23.1.7, Related Resources: Updated language to indicate the IRM can contain guidance from IRS-defined policy, regulatory and mandated guidance, and policy from other sources beyond the federal guidance cited throughout the IRM.
- (6) IRM 10.8.23.3, IT Roles and Responsibilities: Added new subsection for application server-specific roles and responsibilities.
- (7) IRM 10.8.23.4, IT Security Controls: Added statements to clarify the restrictiveness of security controls.
- (8) IRM 10.8.23.4, IT Security Controls and subsequent subsections: Added leading zeros (0s) to the control numbers.
- (9) IRM 10.8.23.5.1.1, AC-02 Account Management: Added new subsection for AC-02 Account Management requirements from the latest version of DISA's Application Server SRG.
- (10) IRM 10.8.23.5.3.2, AU-03 Content of Audit Records: Moved a requirement to the alpha list to be grouped in with the other requirements and removed DISA rule SRG-APP-000356-AS-000202, which is no longer applicable according to the latest NIST SP 800-53 Rev. 5 changes.
- (11) IRM 10.8.23.5.3.7(5), AU-09 Protection of Audit Information: Added new requirement from the latest version of DISA's Application Server SRG.

- (12) IRM 10.8.23.5.4(1), CA - Assessment, Authorization, and Monitoring: Removed controls due to there not being any requirements specific requirements for application servers for the CA control family.
- (13) IRM 10.8.23.5.5.1(2), CM-05 Access Restrictions for Change: Remapped DISA rule SRG-000142-AS-000014 to IRM 10.8.23.5.5.3, CM-07 Least Functionality, remapped DISA rule SRG-APP-000131-AS-000002 to new section IRM 10.8.23.5.5.4, CM-14 Signed Components, and remapped DISA rule SRG-APP-000133-AS-000093 to IRM 10.8.23.5.16.9, SC-24 Fail in Known State.
- (14) IRM 10.8.23.5.5.3, CM-07 Least Functionality: Added DISA rule SRG-APP-000142-AS-000014 remapped from CM-05.
- (15) IRM 10.8.23.5.5.4, CM-14 Signed Components: Added new subsection for CM-14 Signed Components requirements from the latest version of DISA's Application Server SRG.
- (16) IRM 10.8.23.5.7.1(2)(3)(4)(5), IA-02 Identification and Authentication (Organizational Users): Added new requirements from the latest version of DISA's Application Server SRG.
- (17) IRM 10.8.23.5.7.3(6)(7), IA-05 Authenticator Management: Updated DISA rule SRG-APP-000171-AS-000119 from the latest version of DISA's Application Server SRG.
- (18) IRM 10.8.23.5.9.1, MA-04 Non-Local Maintenance: Added new subsection for MA-04 Non-Local Maintenance requirements from the latest version of DISA's Application Server SRG.
- (19) IRM 10.8.23.5.16.6, SC-17 Public Key Infrastructure Certificates: Added new requirement from the latest version of DISA's Application Server SRG.
- (20) IRM 10.8.23.5.16.6, SC-18 Mobile Code: Remapped DISA rule SRG-APP-000223-AS-000150 to section IRM 10.8.23.5.16.7, SC-23 Session Authenticity.
- (21) IRM 10.8.23.5.16.7, SC-23 Session Authenticity: Added DISA rule SRG-APP-000223-AS-000150 remapped from IRM 10.23.5.16.6 SC-18 Mobile Code.
- (22) IRM 10.8.23.5.16.9, SC-24 Fail in Known State: Added DISA rule SRG-APP-000133-AS-000093 remapped from CM-05.
- (23) IRM 10.8.23.5.16.10, SC-28 Protection of Information at Rest: Added new requirements from the latest version of DISA's Application Server SRG.
- (24) IRM 10.8.23.5.16.11, SC-45 System Time Synchronization: Added new subsection for SC-45 System Time Synchronization requirements from the latest version of DISA's Application Server SRG.
- (25) IRM 10.8.23.5.18, SR - Supply Chain Risk Management: Added new subsection for SR - Supply Chain Risk Management requirements.
- (26) Exhibit 10.8.23-1, Security Requirements Checklists: Removed boilerplate template text from the subsection.
- (27) Exhibit 10.8.23-2, Terms and Acronyms: Added new terms and acronyms.
- (28) Exhibit 10.8.23-3, Related Resources: Added new related resources.
- (29) Throughout: Added references to IRM 10.8.24, Information Technology (IT) Security, Cloud Computing Security Policy to account for cloud-based systems.
- (30) Editorial changes made throughout the IRM for clarity. Incorporated plain language and updated grammar, titles, website addresses, and references.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes the prior version of IRM 10.8.23 dated November 6, 2023. This IRM supplements IRM 10.8.1, *Security Policy*, IRM 10.8.2 , *IT Security Roles and Responsibilities*, and IRM 10.8.24, **Cloud Computing Security Policy**.

AUDIENCE

IRM 10.8.23 must be distributed to all personnel responsible for ensuring that adequate security is provided for IRS information and information systems. This IRM applies to all employees, contractors, and vendors of the IRS.

Kaschit Pandya
Acting Chief Information Officer

Application Server Security Policy

10.8.23.1 Program Scope and Objectives

- 10.8.23.1.1 Background
- 10.8.23.1.2 Authority
- 10.8.23.1.3 Responsibilities
- 10.8.23.1.4 Program Management and Review
- 10.8.23.1.5 Program Controls
- 10.8.23.1.6 Terms and Acronyms
- 10.8.23.1.7 Related Resources
- 10.8.23.2 Risk Acceptance and Risk-Based Decisions (RBD)
- 10.8.23.3 IT Roles and Responsibilities
- 10.8.23.4 IT Security Controls

[illegible]

[illegible]

Exhibits

#

#

10.8.23-3 Related Resources

10.8.23.1
(08-27-2025)
Program Scope and Objectives

- (1) **Overview:** This IRM lays the foundation to implement and manage security controls and guidance for the use of application servers within the IRS.
 - a. This IRM is subordinate to IRM 10.8.1, *Security Policy*, and augments the existing requirements identified within IRM 10.8.1, as they relate to IRS application servers for on-premises systems, including on-premises cloud deployments.
 - b. This IRM is subordinate to IRM 10.8.24, *Cloud Computing Security Policy*, and augments the existing requirements identified within IRM 10.8.24, as they relate to IRS application servers for off-premises cloud deployments.
- (2) **Program Purpose:** Develop and publish policies to protect the IRS against potential security threats, risks, and vulnerabilities to ensure compliance with federal mandates and legislation.
- (3) **Audience:** The provisions 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.

10.8.23.1.1
(08-27-2025)
Background

- (1) Application servers provide data via an internally or publicly-exposed interface and are well-known targets for exploitation. Unprotected application 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 policy defines the security controls for Application servers.
 - b. This IRM provides the security configuration standards required to ensure Application server software is integrated and used appropriately for all IRS systems.
- (2) IRM 10.8.23 is part of the IRM Part 10.8 Information Technology (IT) Security series for IRS IT Cybersecurity.

10.8.23.1.2
(08-27-2025)
Authority

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

10.8.23.1.3
(08-27-2025)
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, **IIT Security Role and Responsibilities**.
- (2) Supplemental roles and responsibilities specific to the implementation of application servers (if any) are located in IRM 10.8.23.3, IT Roles and Responsibilities subsection of this IRM.

10.8.23.1.4
(08-27-2025)
Program Management and Review

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

10.8.23.1.5
(08-27-2025)
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) For systems that store, process, or transmit classified national security information, refer to IRM 10.9.1, *Classified National Security Information (CNSI)*, for additional guidance for protecting classified information.
- (4) This IRM establishes the minimum baseline security policy and requirements for all IRS application servers.

- (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: 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 Federal 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. Control 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.
- i. 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:

- 1. 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
- 2. 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.

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 impact-level LOW
(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	CISA [CISA: BOD 23-01]
NIST Publication	[NIST: SP 800-40]
DISA STIG/SRG	[DISA: SRG-APP-000516-NDM-000350]
IRS Defined	[IRS: IRS-defined] or [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]

Example: How a source, baseline, overlay could appear at the end of a requirement: [NIST: SP800-53, SA-15 | Baseline: M, H | Overlay: HVA]

Note: Citations correlate to a reference listed in Exhibit 10.8.23-3, 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, 10.8.1 has precedence, unless the security controls/requirements in this IRM are more restrictive.

10.8.23.1.6
(11-06-2023)
Terms and Acronyms

(1) Refer to Exhibit 10.8.23-2, Terms and Acronyms for a list of terms, acronyms, and definitions.

- (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 10.8.23-3, Related Resources for a list of related resources and references.

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

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

(1) This IRM does not contain supplemental roles and responsibilities specific to the use of application servers.

- (1) The security controls in this IRM supplement the requirements found in IRM 10.8.1.
 - a. Refer to IRM 10.8.1 or IRM 10.8.24 (as applicable) 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]

#

#

#

#####

#

#####

#

This Page Intentionally Left Blank

#

Exhibit 10.8.23-2 (08-27-2025)

#

The table below defines some key terms used in this IRM.

Term	Definition or Description
Application server	A software server, normally using HTTP, which has the ability to execute dynamic web applications.
Authentication	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.
Authorization	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.
Authorizing official (AO)	The AO is an executive or other senior official with the authority to formally assume responsibility of the operation of an information system and the information contained therein, at an acceptable level of risk. (TD P 85-01). See IRM 10.8.2 for a detailed description of an AO’s responsibilities.
Basic authentication	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.
BEARS	Business Entitlement Access Request System
CA	Certification authority
CIO	Chief information officer
CIP	Critical infrastructure protection
Cipher suite	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.
CISA	Cybersecurity and Infrastructure Security Agency

Exhibit 10.8.23-2 (Cont. 1) (08-27-2025)

#

Compiler	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.
CMMI	Capability Maturity Model Integration
CRL	Certificate Revocation List
CSW	Critical software
CTL	Certificate Trust List
DISA	Defense Information Systems Agency
DoS	Denial-of-service
EA	Enterprise Architecture
Enterprise Architecture (EA) Enterprise Standards Profile (ESP)	The authoritative repository for IRS approved products and standards.
EFC	Enterprise FISMA Compliance
Enterprise Life Cycle (ELC)	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.
EO	Executive order
ESP	Enterprise Standards Profile
Federal Information Processing Standards (FIPS)	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.
Federal Information Security Modernization Act of 2014 (FISMA)	A framework for managing information security that must be followed for all systems used or operated by a U.S. federal government agency in the executive or legislative branches, or by a contractor or other organization on behalf of a federal agency in those branches.
FICAM	Federal Identity Credential and Access Management
GMT	Greenwich Mean Time
HA	High-availability

Exhibit 10.8.23-2 (Cont. 2) (08-27-2025)

#

High Value Asset	<p>Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or the public confidence, civil liberties, or public health and safety of the American people. HVA can fall into one of the three categories:</p> <ul style="list-style-type: none"> • Informational Value - The information or information system that processes, stores, or transmits the information is of high value to the Government or its adversaries. • Mission Essential - The agency that owns the information or information system cannot accomplish its Primary Mission Essential Functions (PMEF), as approved in accordance with Presidential Policy Directive 40 (PPD-40) National Continuity Policy, within expected timelines without the information or information system. • Federal Civilian Enterprise Essential (FCEE) - The information or information system serves a critical function in maintaining the security and resilience of the federal civilian enterprise.
HyperText Transfer Protocol (HTTP)	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.
HyperText Transfer Protocol Secure (HTTPS)	A secure form of communication over a computer network by layering HTTP on top of the SSL/TLS protocol.
ICAM	Identity, credential, and access management
Internet protocol (IP)	The principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries.
IT	Information Technology
Internal web server	A private server with a private IP address and is not visible to the Internet (i.e. irweb.irs.gov).
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
ISSO	Information system security officer
IT	Information technology
ITIL	Information Technology Infrastructure Library
ITSCM	IT Service Continuity Management

Exhibit 10.8.23-2 (Cont. 3) (08-27-2025)

#

LDAP	Lightweight Directory Access Protocol
LSS	Lean Six Sigma
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
OSCP	Online Certificate Status Protocol
PIV	Personal Identity Verification
POA&M	Plan of action and milestones
Public key infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Risk-based decisions (RBD)	Decision made by individuals responsible for ensuring security by utilizing a wide variety of information, analysis, assessment, and processes. The type of information taken into account when making a risk-based decision may change based on life cycle phase and the entire posture of the system. Some examples of information considered are formal and informal risk assessments, risk analysis, recommended risk mitigation strategies, and business impact. (This list is not intended to be all-inclusive).
SA	System administrator
SA&A	Security assessment and authorization
Script	A program run on a Web server, in response to input from a browser.
Scripting language	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.
Secure sockets layer(SSL)	An industry standard public-key protocol used to create encrypted tunnels between two network-connected devices.

Exhibit 10.8.23-2 (Cont. 4) (08-27-2025)

#

Session ID	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.
SOP	Standard Operating Procedure
SOAP	Simple object access protocol
SP	Special publication
SRM	Security risk management
SSP	System security policy
TD	Treasury Directive
Transport layer security(TLS)	An authentication and security protocol widely implemented in browsers and Web servers.
Universal resource locator(URL)	A standard way of specifying the location of an object, normally a web page, on the Internet.
UTC	Coordinated Universal Time
Web server	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 10.8.23-3 (04-14-2020)**Related Resources****IRS Publications**

- IRM 1.4.6, *Resource Guide for Managers, Managers Security Handbook*
- IRM 1.15, *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, IT Security Roles and Responsibilities*
- IRM 10.8.6, *Information Technology (IT) Security, Application Security and Development*
- 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 10.9.1, *National Security Information, Classified National Security Information (CNSI)*

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

Department of the Treasury Publications

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

National Institute of Standards and Technology Publications

- **FIPS 140-2:** Federal Information Processing Standards Publication 140-2, **"Security Requirements for Cryptographic Modules,"** May 25, 2001 (Change Notice 2, 12/3/2002).
- **FIPS 140-3:** Federal Information Processing Standards Publication 140-3, **"Security Requirements for Cryptographic Modules,"** March 22, 2019.
- **FIPS 199:** Federal Information Processing Standards 199, *"Standards for Security Categorization of Federal Information and Information Systems,"* February 2004.
- **FIPS 200:** Federal Information Processing Standards 200, *"Minimum Security Requirements for Federal Information and Information Systems,"* March 2006
- NIST SP 800-37 Rev 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* September 20, 2018
- **SP 800-52:** NIST Special Publication 800-52 Revision 2, *"Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations,"* August 2019.
- **SP 800-53:** NIST Special Publication 800-53 Revision 5.1.1, *"Security and Privacy Controls for Information Systems and Organizations,"* November 7, 2023.
- NIST SP 800-53A Rev 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations,* December 2014 (includes updates as of December 18, 2014)

Defense Information Systems Agency (DISA) Publications

- DISA Application Server SRG V4R1
- 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 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 on the *DISA STIGs Document Library* site.

