



# MANUAL TRANSMITTAL

Department of the Treasury  
Internal Revenue Service

10.8.21

SEPTEMBER 2, 2025

## EFFECTIVE DATE

(09-02-2025)

## PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.8.21, *Information Technology (IT) Security, Database Security Policy*.

## MATERIAL CHANGES

- (1) IRM 10.8.21.1(1)b., Program Scope and Objectives: Updated to align with our boilerplate and added reference to IRM 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy*
- (2) IRM 10.8.21.1 (2), Program Scope and Objectives: Changed the title to Program Purpose.
- (3) IRM 10.8.21.3, Roles and Responsibilities: Added new reference for roles and responsibilities and moved the existing roles and responsibilities to IRM 10.8.21.3
- (4) IRM 10.8.21.1.5, Program Controls: Updated language to align with our boilerplate.
- (5) IRM 10.8.21.4.1.1, AC-02 Account Management: Updated with DISA Database Security Requirements Guide (SRG) V4R3 language.
- (6) IRM 10.8.21.4.3.1, AU-03 Content of Audit Records: Add Note to clarify the requirement.
- (7) IRM 10.8.21.4.3.2, AU-04 Audit Log Storage Capacity: Updated (1) to align with the language of the DISA Database SRG V4R3.
- (8) IRM 10.8.21.4.3.3, AU-05 Response to Audit Logging Process Failures: Removed requirements DISA removed from the DISA Database SRG V4R3.
- (9) IRM 10.8.21.4.3.4, AU-06 Audit Record Review, Analysis, and Reporting: Added new language from the DISA Database SRG V4R3.
- (10) IRM 10.8.21.4.3.6, AU-09 Protection of Audit Information: Updated the language to align with the DISA Database SRG V4R3.
- (11) IRM 10.8.21.4.7, IA-02 Identification and Authentication (Organizational Users): Added new language from the DISA Database SRG V4R3.
- (12) IRM 10.8.21.4.7.2, IA-05 Authenticator Management: Added new language from the DISA Database SRG V4R3.
- (13) IRM 10.8.21.4.7.3, IA-06 Authenticator Feedback: Updated language to align with the DISA Database SRG V4R3.
- (14) IRM 10.8.21.4.7.4, IA-07 Cryptographic Module Authentication: Updated language to align with the DISA Database SRG V4R3.
- (15) IRM 10.8.21.4.18.5, SC-13 Cryptographic Protection: Added new language from the DISA Database SRG V4R3.
- (16) IRM 10.8.21.4.18.6, SC-17 Public Infrastructure Certificates: Added new language from the DISA Database SRG V4R3.

- (17) IRM 10.8.21.4.18.7, SC-23 Session Authenticity: Added new language from the DISA Database SRG V4R3.
- (18) IRM 10.8.21.4.18.9, SC-28 Protection of Information at Rest: Added new language from the DISA Database SRG V4R3.
- (19) Editorial changes (including grammar, spelling, and minor clarification) were made throughout the IRM.

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

This supersedes IRM 10.8.21, dated November 9, 2023. Additionally, this IRM was updated to incorporate Interim Guidance #IT-10-0224-0004 SA-22 Requirement. This IRM supplements IRM 10.8.1, *Information Technology (IT) Security, Security Policy*, IRM 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy*, and IRM 10.8.2 *Information Technology (IT) Security, Security Roles and Responsibilities*.

#### **AUDIENCE**

IRM 10.8.21 shall be distributed to all personnel responsible for ensuring adequate security is provided for IRS information and information systems. This policy applies to all employees, contractors, and vendors of the IRS.

Kaschit Pandya  
Acting Chief Information Officer

## Database Security Policy

#### 10.8.21.1 Program Scope and Objectives

[illegible]

[illegible]

---

Exhibits

10.8.21-2 Terms and Acronyms

#

#



10.8.21.1  
(09-02-2025)  
**Program Scope and Objectives**

- (1) **Overview:** This IRM lays the foundation to implement and manage security controls and guidance for the use of databases within the IRS.
  - a. This policy 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 database systems for on-premises systems, including on-premises cloud deployments.
  - b. This IRM is subordinate to IRM 10.8.24, *Information Technology (IT), Cloud Computing Security Policy*, and augments the existing requirements identified within IRM 10.8.24, as they relate to IRS databases for off-premise cloud deployments.
- (2) **Program Purpose:** Develop and publish security policies to protect the IRS against potential security threats, risks, and vulnerabilities to ensure compliance with federal mandates and legislation.
- (3) **Audience:** The provisions within this policy apply to:
  - a. All offices and business, operating, and functional units within the IRS.
  - b. IRS personnel and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, which use or operate systems that store, process or transmit IRS information or connect to an IRS network or system.
  - c. All National Institute of Standards and Technology (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.

10.8.21.1.1  
(09-02-2025)  
**Background**

- (1) This IRM establishes a comprehensive policy to implement the minimum security controls to safeguard databases within the IRS organization.
- (2) IRM 10.8.21 is part of the IRM 10.8 Information Technology (IT) Security series for IRS IT Cybersecurity.

10.8.21.1.2  
(11-09-2023)  
**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), NIST, Cybersecurity and Infrastructure Security Agency (CISA), National Archives and Records Administration (NARA), the Department of the Treasury, and IRS guidelines as they apply.

10.8.21.1.3  
(09-02-2025)  
**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*.

10.8.21.1.4  
(09-02-2025)  
**Program Management  
and Review**

- (2) Supplemental roles and responsibilities specific to the implementation of databases are located in IRM 10.8.21.3, IT Roles and Responsibilities subsection of this IRM.
- (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 requirement checklists. Stakeholders are notified when revisions to the security policies and security requirement checklists are made.
- (2) It is the policy of the IRS to:
  - a. Establish and manage an information security program within all its organizations. This IRM provides uniform policies and guidance to be used by each office.
  - 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), Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve IRS IT process and service efficiency and effectiveness.

10.8.21.1.5  
(09-02-2025)  
**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 requirement checklists. Revisions to security policies and checklists are reviewed by the security policy team, in collaboration with applicable stakeholders, for potential impact to the IRS operational environment.
- (2) Security Policy provides a report identifying security policies and security requirement checklists that have recently been revised or are in the 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 databases.
- (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 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
  - iv. Not associated with security control baselines

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

- c. Control identifier 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 authorizing official (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.
  2. The associated documentation for this risk-based decision not to implement must be submitted to the Department of the Treasury Cyber CIP Program Manager and the Departmental Chief Information Security Officer 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 (Program Management) and PT (Personally Identifiable Information Processing and Transparency) 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.

***Below is a listing of indicators and their applicability.***

<u>Indicator</u>	<u>Applicability</u>
(L)	Applies to systems categorized as FIPS 199 impact-level low
(M)	Applies to systems categorized as FIPS 199 impact-level moderate
(H)	Applies to systems categorized as FIPS 199 impact-level high
(CIP)	Overlay - Applies to systems identified as cyber critical infrastructure assets.
(HVA)	Overlay - Applies to systems identified as Cyber High Value Assets
(P)	Overlay - 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:

*Below is a list of citations used within the IRM and examples.*

<u>Citation</u>	<u>Example</u>
NIST Control	[NIST: SP 800-53, AC-02]
Treasury Control	[Treasury: TD P 85-01, AC-03_T.002]
Treasury Publication	[Treasury: TD P 15-71]
Federal	[Federal: P.L. 113-283]
U.S. Code	[USC: 44 USC 3551]
Executive Order	[EO: 14028]
OMB Memorandum	[OMB: M-22-09] or [OMB: M-22-09 (III)(D)(5)]
CISA	[CISA: BOD-23-01]
NIST Publication	[NIST: SP 800-40] or [NIST: SP 800-40, Section 3.5]
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: HVA]

**Note:** Citations correlate to a reference listed in Exhibit 10.8.15-3, 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 policy and IRM 10.8.1, IRM 10.8.1 has precedence, unless the security controls/requirements in this policy are more restrictive.

10.8.21.1.6  
(09-02-2025)

#### Terms and Acronyms

(1) Refer to Exhibit 10.8.21-2 Terms and Acronyms, for a list of terms, acronyms, and definitions.

10.8.21.1.7  
(11-09-2023)  
Related Resources

(1) In addition to the federal guidance cited throughout this IRM, this IRM incorporates IRS-defined policy, regulatory and mandated guidance, and policy from other sources. Refer to Exhibit # 10.8.21-3 # Related Resources for a list of related resources and references.

10.8.21.2  
(09-02-2025)  
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).

#

#

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

10.8.21.3  
(09-02-2025)  
IT Security Roles and Responsibilities

(1) The following roles and responsibilities are specific to the implementation of databases:

a. Application Developer: The application developer role is used to assign required privileges to developer accounts on a development database. Application developers must not be permitted access to production databases, except as specified within IRM 10.8.1 and the security requirements checklists for this IRM.

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

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

[illegible]

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

##  
##

##  
##  
##  
##  
##

##  
##  
##

##  
##  
##

##  
##

##  
##  
##  
##



[illegible]

```
## ## ##
## ##
## ## ## ## ##
## ##
## ## ## ## ## ## ## ## ## ## ## ##
## ##
## ## ## ## ## ## ## ## ## ## ## ##
## ## ##
## ## ## ## ## ## ## ## ## ## ## ##
```

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

[illegible]

[illegible]

#  
#  
#  
#  
#

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

[illegible]



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

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

[illegible]

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

[illegible]

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

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

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



[illegible]

**Exhibit 10.8.21-2 (11-09-2023)**  
**Terms and Acronyms**

Term	Definition or description
AO	Authorizing Official
Application Developers	Refer to Developers
Authorized or Unauthorized Personnel	Applies to all IRS personnel being authorized or not authorized to perform a particular action.
CA	Certification Authority
CIS	Center for Internet Security
CRL	Certificate Revocation List
CSIRC	Computer Security Incident Response Center
DASD	Direct Access Storage Device
DBA	Database Administrator
DBMS	Database Management System
Developers or Application Developers	Refers to “Program Developers/Programmers” and “Web Developers” as defined in IRM 10.8.2. Note: This does not refer to database administrators (DBAs), who may assist Developers.
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
Discretionary Access Control (DAC)	A means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).
DML	Data Manipulation Language
EA	Enterprise Architecture
ESAT	Enterprise Security Audit Trails
ESP	Enterprise Standards Profile
FIFO	First-In-First-Out
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Modernization Act
GMT	Greenwich Mean Time
HTML	Hypertext Markup Language

**Exhibit 10.8.21-2 (Cont. 1) (11-09-2023)**  
**Terms and Acronyms**

IBM	International Business Machines
IP	Internet Protocol
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
ISSO	Information System Security Officer
IT	Information Technology
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSI	National Security Information
OCSP	Online Certificate Status Protocol
OS	Operating System
OMB	Office of Management and Budget
OUO	Official Use Only
PII	Personally Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RBD	Risk Based Decision
RIM	Records and Information Management
Risk Based Decisions	Decision made by individuals responsible for ensuring security by utilizing a wide variety of information, analysis, assessment, and processes. The type of information taken into account when making a risk-based decision may change based on life cycle phase and decision is made taking entire posture of the system into account. Some examples of information taken into account are formal and informal risk assessments, risk analysis, assessments, recommended risk mitigation strategies, and business impact. (This list is not intended to be all inclusive).
SA	System Administrator
SBU	Sensitive But Unclassified
SOP	Standard Operating Procedure
SP	Special Publication
SRG	Security Requirements Guide

**Exhibit 10.8.21-2 (Cont. 2) (11-09-2023)****Terms and Acronyms**

SRM	Security Risk Management
SSP	System Security Policy
STIG	Security Technical Implementation Guide
TD	Treasury Directive
Unauthorized Personnel	Refer to Authorized Personnel
UTC	Coordinated Universal Time
XML	Extensible Markup Language

[illegible]

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