



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.5

MAY 12, 2025

EFFECTIVE DATE

(05-12-2025)

PURPOSE

- (1) This transmits revised IRM 10.8.5, *Information Technology (IT) Security, Domain Name System (DNS) Security Policy*.

MATERIAL CHANGES

- (1) Throughout the IRM, Changed instances of "shall" to "must" where appropriate.
- (2) Throughout the IRM, Changed instances of "this policy" to "this IRM".
- (3) Throughout the IRM, Added a leading zero to single digit NIST controls. Example: AC-2 is now AC-02.
- (4) Throughout the IRM, Revised source citation and baseline indicator formatting.
- (5) Throughout the IRM, Updated references to IRM 10.8.1 to include a reference to IRM 10.8.24.
- (6) 10.8.5.1 Program Scope and Objectives:
 - (1) Removed acronyms IRM and IRS definitions.
 - (1)a) Updated IRM 10.8.1 title; added on-premises and off-premises language.
 - (3)c) Added new subpart to clarify applicability of IRM to systems and their NIST impact levels.
 - (4) Added CIO acronym.
 - (6) Changed "information systems" to "systems" to align with NIST SP 800-53 Rev5.
- (7) 10.8.5.1.1 Background: (2) Clarified 10.8 series language.
- (8) 10.8.5.1.3 Roles and Responsibilities: Updated IT security roles references.
- (9) 10.8.5.1.3.1 Information System Owner: Subsection moved to new 10.8.5.3.1.
- (10) 10.8.5.1.3.2 DNS Key Administrator: Subsection moved to new 10.8.5.3.2.
- (11) 10.8.5.1.3.3 DNS Zone Administrator: Subsection moved to new 10.8.5.3.3.
- (12) 10.8.5.1.3.4 User and Network Services (UNS): Subsection moved to new 10.8.5.3.4.
- (13) 10.8.5.1.4 Program Management and Review: (2)d) Removed ELC as an example.
- (14) 10.8.5.1.5 Program Controls:
 - (1) Revised language for clarification.
 - New (2) Added informative language.
 - New (3) IRM 10.9.1 reference relocated from paragraph (1).
 - New (5) Added guidance on baseline and overlay indicators attached to requirements within the IRM.
 - New (6) Added guidance on citations attached to requirements within the IRM.
 - Original (2) moved to the end of the subsection as paragraph (7).
- (15) 10.8.5.1.6 Terms and Acronyms: Added Exhibit 10.8.5-6 title.

- (16) 10.8.5.1.7 Related Resources: Added Exhibit 10.8.5-7 title.
- (17) 10.8.5.2 Risk Acceptance and Risk-Based Decisions (RBD):
 - (1) Updated language to clarify that a risk acceptance decision is made, not an RBD is created.
 - (2) Updated URL.
- (18) 10.8.5.3 IT Roles and Responsibilities: New subsection added.
- (19) 10.8.5.3.1 System Owner:
 - 10.8.5.1.3.1 Information System owner subsection relocated to this new subsection.
 - (3) Change “UNS” to “EOps”.
- (20) 10.8.5.3.2 DNS Key Administrator: 10.8.5.1.3.2 DNS Key Administrator subsection relocated to this new subsection.
- (21) 10.8.5.3.3 DNS Zone Administrator: 10.8.5.1.3.3 DNS Zone Administrator subsection relocated to this new subsection.
- (22) 10.8.5.3.4 User and Network Services (UNS):
 - 10.8.5.1.3.4 User and Network Services (UNS) subsection relocated to this new subsection.
 - Changed subsection title to “Enterprise Operations (EOps)”.
 - (1) Changed “UNS” to “EOps”.
- (23) 10.8.5.4 IT Security Controls:
 - Original (2) Removed as it was deemed duplication of language in each IT control subsection.
 - Original (4) Added subsection number to reference and updated title of referenced subsection.
- (24) 10.8.5.4.1 AC - Access Control:
 - Removed AC-2 from list due to AC-2 requirements being added to the IRM.
 - Add AC-04 to list due to the subsection no longer having requirements.
- (25) 10.8.5.4.1.1 AC-02 Account Management: New subsection and requirements SRG-APP-000700-DNS-000100 and SRG-APP-000705-DNS-000110 added from the SRG.
- (26) 10.8.5.4.1.2 AC-04 Information Flow Control: Subsection removed due to requirements being removed from the SRG.
- (27) 10.8.5.4.3 AU - Audit and Accountability: Removed AU-6 from the list due to AU-6 requirements being added to the IRM.
- (28) 10.8.5.4.3.2 AU-06 Audit Record Review, Analysis, and Reporting: New subsection and requirement SRG-APP-000745-DNS-000120 added from the SRG.
- (29) 10.8.5.4.3.3 AU-09 Protection of Audit Information: Added new requirement SRG-APP-000795-DNS-000130 from the SRG.
- (30) 10.8.5.4.3.4 AU-10 Non-repudiation: Removed requirement SRG-APP-000176-DNS-000076 due to it no longer in the SRG.
- (31) 10.8.5.4.3.5 AU-12 Audit Record Generation: Removed requirement SRG-APP-000353-DNS-000045 due to it no longer in the SRG.

-
- (32) 10.8.5.4.5 CM - Configuration Management: Removed CM-5 Access Restrictions for Change and CM-14 Signed Components from the list due to CM-5 and CM-14 requirements being added to the IRM.
- (33) 10.8.5.4.5.1 CM-05 Access Restrictions for Change: New subsection and requirement SRG-APP-000805-DNS-000140 being added from the SRG.
- (34) 10.8.5.4.5.2 CM-06 Configuration Settings:
- Original (2) relocated to the SI-13 subsection to align with SRG CCI mapping.
 - Original (3) relocated to the AU-10 subsection to align with SRG CCI mapping.
 - Original (5) relocated to the AU-10 subsection to align with SRG CCI mapping.
 - Original (8) relocated to the SC-20 subsection to align with SRG CCI mapping.
 - Original (9) relocated to the SC-20 subsection to align with SRG CCI mapping.
 - (37) Corrected requirement by replacing CTO with IRS and Treasury policies.
- (35) 10.8.5.4.5.5 CM-14 Signed Components: New subsection and requirement SRG-APP-000810-DNS-000150 being added from the SRG.
- (36) 10.8.5.4.7 IA - Identification and Authentication: IA-11 Re-Authentication and IA-13 Identity Providers and Authorization Servers due to the SRG not having any requirements for them.
- (37) 10.8.5.4.7.1 IA-02 Identification and Authentication (Organizational Users):
- (1) New requirement SRG-APP-000815-DNS-000160 added from the SRG.
 - (2) New requirement SRG-APP-000820-DNS-000170 added from the SRG.
 - (3) New requirement SRG-APP-000825-DNS-000180 added from the SRG.
- (38) 10.8.5.4.7.3 IA-05 Authenticator Management:
- (8) New requirement SRG-APP-000830-DNS-000190 added from the SRG.
 - (9) New requirement SRG-APP-000835-DNS-000200 added from the SRG.
 - (10) New requirement SRG-APP-000840-DNS-000210 added from the SRG.
 - (11) New requirement SRG-APP-000845-DNS-000220 added from the SRG.
 - (12) New requirement SRG-APP-000850-DNS-000230 added from the SRG.
 - (13) New requirement SRG-APP-000855-DNS-000240 added from the SRG.
 - (14) New requirement SRG-APP-000860-DNS-000250 added from the SRG.
 - (15) New requirement SRG-APP-000865-DNS-000260 added from the SRG.
 - (16) New requirement SRG-APP-000870-DNS-000270 added from the SRG.
 - (17) New requirement SRG-APP-000875-DNS-000280 added from the SRG.
- (39) Original 10.8.5.4.7.4 IA-11 Re-Authentication: Removed subsection and its requirements due to requirements being removed from the SRG.
- (40) 10.8.5.4.9.1 MA-04 Non-Local Maintenance: (2) New requirement SRG-APP-000880-DNS-000290 added from the SRG.
- (41) 10.8.5.4.15 PT - Personally Identifiable Information Processing and Transparency: Replaced IRM 10.8.1 reference with reference to IRM 10.5.1.
- (42) 10.8.5.4.17.2 SA-04 Acquisition Process: (1)a) Changed “UNS” to “EOps”.
- (43) 10.8.5.4.18 SC - System and Communications Protection: Removed SC-17 Public Key Infrastructure (PKI) Certificates and SC-45 System Time Synchronization from the list due to requirements being added from the SRG to the IRM.
- (44) 10.8.5.4.18.3 SC-08 Transmission Confidentiality and Integrity: Corrected subsection title.

- (45) 10.8.5.4.18.5 SC-17 Public Key Infrastructure (PKI) Certificates: New subsection and requirement SRG-APP-000910-DNS-000300 added from the SRG.
- (46) 10.8.5.4.18.6 SC-20 Secure Name/Address Resolution Service (Authoritative Source):
- - New (5) added requirement SRG-APP-000420-DNS-000053, which was relocated from 10.8.5.4.1 (8).
 - - New (6) added requirement SRG-APP-000421-DNS-000054, which was relocated from 10.8.5.4.1 (9).
- (47) 10.8.5.4.18.9 SC-28 Protection of Information at Rest: New requirement SRG-APP-000915-DNS-000310 added from the SRG.
- (48) 10.8.5.4.18.10 SC-45 System Time Synchronization: New subsection added.
- - (1) New requirement SRG-APP-000920-DNS-000320 added from the SRG.
 - - (2) New requirement SRG-APP-000925-DNS-000330 added from the SRG.
- (49) 10.8.5.4.19 SI - System and Information Integrity: SI-13 Predictable Failure Prevention removed from the list due to requirements being added to the subsection.
- (50) 10.8.5.4.19.3 SI-13 Predictable Failure Prevention:
- New subsection added.
 - - (1) Added requirement SRG-APP-000268-DNS-000039, which was relocated from 10.8.5.4.5.1 (2).
- (51) 10.8.5.4.20 SR- Supply Chain Risk Management Policy and Procedures: New subsection added.
- (52)
- Exhibit 10.8.5-5 Security Requirements Checklists:
 - - 2) Updated URL.
 - - 3) Updated IRM 10.8.50 title.
 - - 4) Defined EA ESP acronym.
- (53) Exhibit 10.8.5-6 Terms and Acronyms:
- - Added the following acronyms: AO, CIO, CISA, CMMI, DAC, DRP, EFC, EO, IETF, ISCP, IT, ITIL, LSS, NSA, RBD, SA&A, SBU, SOP, SP, SRM, STIG, and TD.
 - Removed the following acronyms no longer in the IRM: HINFO, LOC
 - Added the following terms: RBD, Risk Acceptance Decision.
 - Updated the following terms: Authentication Chain and External System Service Provider.
- (54) Exhibit 10.8.5-7 Related Resources:
- - Added the following publications: IRM 10.8.24, IRM 10.9.1, FIPS 140-3, FIPS 200, NIST SP 800-53, NIST SP 800-53A, and NIST SP 800-53B.
 - - Updated the following publications: IRM 10.5.1, TD P 85-01, FIPS 140-2, FIPS 180-4, FIPS 198-1, FIPS 199, NIST SP 800-37, NIST SP 800-57 Part 1, NIST SP 800-57 Part 2, NIST SP 800-90A, NIST SP 800-81-2, NIST SP 800-123, RFC 4033, CISA ED 19-01, OMB M-08-03, and OMB M-22-09.
 - - Replaced FIPS 186-4 with FIPS 186-5.
 - - Replaced DISA DNS SRG V2R4 with DISA DNS SRG V4R1.
 - Added URL to where Treasury publications are available.
 - Added URL to where NIST publications are available.
 - Added URL to where DISA publications are available.

- (55) Editorial changes (including grammar, spelling and minor clarification) were made throughout the IRM.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 10.8.5 dated October 24, 2023. This IRM supplements IRM 10.8.1, *Information Technology (IT) Security, Security Policy*, and IRM 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy* (as applicable).

AUDIENCE

IRM 10.8.5 must be distributed to all personnel responsible for ensuring security is provided for the design, operation and configuration of DNS systems. This IRM applies to all employees, contractors, and vendors of the IRS.

Rajiv Uppal
Chief Information Officer

Domain Name System (DNS) Security Policy

10.8.5.1 Program Scope and Objectives

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

10.8.5.3.1	System Owner
10.8.5.3.2	DNS Key Administrator
10.8.5.3.3	DNS Zone Administrator
10.8.5.3.4	Enterprise Operations (EOps)

#

[illegible]

Exhibits

- 10.8.5-6 Terms and Acronyms
- 10.8.5-7 Related Resources

#

10.8.5.1
(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 Domain Name Systems (DNS) 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 DNS 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 DNS 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 external system service providers, which use or operate systems that store, process, or transmit IRS Information or connect to an IRS network or system.
 - c. All systems regardless of their NIST impact-level (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 systems.

10.8.5.1.1
(05-12-2025)
Background

- (1) This IRM defines the controls for the use of DNS within the IRS.
- (2) IRM 10.8.5 is part of the IRM 10.8, Information Technology (IT) Security series for IRS IT Cybersecurity.
- (3) This IRM provides the technical security policies and requirements for applying security concepts to systems.
- (4) This IRM details DNS security guidance applicable to all IRS name servers, including authoritative and recursive servers.
- (5) The requirements are relevant to all name servers connected to the IRS enterprise.
- (6) Within this IRM, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-81 rev2 is used as a basis for DNS deployment best practices, encryption algorithms, guidelines on using DNS Security Extensions (DNSSEC) digital signatures for DNS query/response and hash-based transaction signature (TSIG) for authenticating zone updates.
- (7) This IRM does not address the DNS configuration of DNS clients (i.e., the workstations, servers, and network devices that query name servers).

- (8) DNS resolver clients' security postures are validated with the security IRM and checklists for the underlying technology or operating system.

10.8.5.1.2
(05-12-2025)

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

10.8.5.1.3
(05-12-2025)

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, *IT Security Roles and Responsibilities*.
- (2) Supplemental roles and responsibilities specific to the implementation of DNS (if any) are in the IRM 10.8.5.3, *IT Roles and Responsibilities* subsection of this IRM.

10.8.5.1.4
(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 technology specific security requirement 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), Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve IRS IT process and service efficiency and effectiveness.

10.8.5.1.5
(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, 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 on protecting classified information.
- (4) This IRM establishes the minimum baseline security policy and requirements for all IRS DNS services.
- (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 Information Processing Standards (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.

Example: 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.
 - 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

10.8 Information Technology (IT) Security

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.

- g. Indicators and their applicability:

Indicator	Applicability
(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)	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 as well. 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: 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]
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

Citation	Example
NIST Baseline	[Baseline: P, L, M, H, O]

c. Overlay

Citation	Example
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 10.8.5-7, *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/requirements in this IRM are more restrictive.

10.8.5.1.6
(05-12-2025)
Terms and Acronyms

- (1) Refer to Exhibit 10.8.5-6, *Terms and Acronyms*, for a list of terms, acronyms, and definitions.

10.8.5.1.7
(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 10.8.5-7, *Related Resources*, for a list of related resources and references.

10.8.5.2
(05-12-2025)

**Risk Acceptance and
Risk-Based Decisions
(RBD)**

- (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 (RBD) Standard Operating Procedures (SOP).

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

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

10.8.5.3
(05-12-2025)

**IT Roles and
Responsibilities**

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

10.8.5.3.1
(05-12-2025)

System Owner

- (1) The system owner must be the agency official responsible for the overall procurement, development, integration, modification, and operation and maintenance of the system as defined by IRM 10.8.2.

Note: Within the IRS, the system owner may be the business and functional unit owner.

- (2) The system owner must ensure that all requirements within this IRM related to their systems are implemented.
- (3) The system owner must ensure that the planning, operation and monitoring of their DNS services are properly coordinated with Enterprise Operations (EOps) and Cybersecurity.

10.8.5.3.2
(05-12-2025)

DNS Key Administrator

- (1) The DNS key administrator must be responsible for the creation, distribution and implementation of the public and private keys used in conjunction with the operation of DNSSEC. [NIST: SP 800-81-2, Section 9]
- (2) The primary purpose of the DNS key administrator must be to create a separation of duty of the signing of DNS records from the creation and alteration of the content of DNS records. [IRS: IRS-Defined]
- (3) The DNS key administrator must ensure the execution of the following in compliance with this IRM: [NIST: SP 800-81-2, Section 11]
 - a. The secure creation of keys using compliant processes with the required key strength.
 - b. The secure storage of private keys.
 - c. The secure transfer of keys from the point of creation to the location of implementation.
 - d. The configuration of DNS servers as it relates to the use of keys.

- e. The implementation of the signing of DNS records with keys using manual or automated methods.
- f. The tracking of key expiration periods requiring the need for new key generation.
- g. The implementation of emergency key rollover procedures when required and approved.
- h. The resolution of key verification errors through investigation and auditing of logs or other applicable information.

10.8.5.3.3
(05-12-2025)

DNS Zone Administrator

(1) The DNS zone administrator must:

- a. Manage the creation and modification of DNS records but must not manage the signing of those records.
- b. Ensure the compliance of DNS records with this IRM.
- c. Review the contents of data entered into DNS records to ensure only allowable information is made available via DNS services.
- d. Process requests for the creation of or changes to DNS records that are not updated dynamically.

10.8.5.3.4
(05-12-2025)

**Enterprise Operations
(EOps)**

(1) EOps must:

- a. Oversee and guide the architectural planning and interoperability of the IRS DNS solution.
- b. Serve as the central point of communication for issues related to the modification and operation of DNS services.
- c. Provide a list of approved DNS software and related tools.
- d. Maintain a library to track the deployment and use of approved software.
- e. Establish and update operational policy for DNS management that complies with this IRM.
- f. Review and provide an approval process for emergency key roll overs.
- g. Monitor threat and vulnerability information related to DNS services and tools to determine the need for software updates or temporary counter-measures to protect IRS systems.

#

#####

#

#

[illegible]

#

#

[illegible]

[illegible]

#

#

#

[illegible]

#

[illegible]

#

[illegible]

##

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

#

#

#

#

#

#

Exhibit 10.8.5-6 (05-12-2025)**Terms and Acronyms****A****ACL** - Access Control List

Authentication Chain: An alternating sequence of DNS public key (DNSKEY) RRsets and Delegation Signer (DS) RRsets forms a chain of signed data, with each link in the chain vouching for the next. A DNSKEY RR is used to verify the signature covering a DS RR and allows the DS RR to be authenticated. The DS RR contains a hash of another DNSKEY RR, and this new DNSKEY RR is authenticated by matching the hash in the DS RR. This new DNSKEY RR, in turn, authenticates another DNSKEY RRSet and, in turn, some DNSKEY RR in this set may be used to authenticate another DS RR, and so forth until the chain finally ends with a DNSKEY RR whose corresponding private key signs the desired DNS data. For example, the root DNSKEY RRSet can be used to authenticate the DS RRSet for “example.” The “example.” DS RRSet contains a hash that matches some “example.” DNSKEY, and this DNSKEY’s corresponding private key signs the “example.” DNSKEY RRSet. Private key counterparts of the “example.” DNSKEY RRSet sign data records such as “www.example.” as well as DS RRs for delegations such as “subzone.example.”

Authentication Key: A public key that a DNSSEC-aware resolver has verified and uses to authenticate data. A DNSSEC-aware resolver can obtain authentication keys in three ways:

- The resolver generally is configured to recognize at least one public key; this configured data usually is either the public key itself or a hash of the public key as found in the DS RR (see trust anchor).
- The resolver may use an authenticated public key to verify a DS RR and the DNSKEY RR to which the DS RR refers.
- The resolver may be able to determine that a new public key has been signed by the private key corresponding to another public key that the resolver has verified.

Authoritative Name Server: A name server that is authoritative for a DNS zone. It provides the definitive answer to a DNS query for a record in the zone. This could be either a master or a slave server.

Authoritative RRSet: Within the context of a particular zone, an RRSet (RRs with the same name, class, and type) is authoritative if and only if the owner name of the RRSet lies within the subset of the name space that is at or below the zone apex and at or above the cuts that separate the zone from its children. RRs of type NSEC, RRSIG, and DS are examples of RRsets at a cut that are authoritative at the parent side of the zone cut, and not the delegated child side.

AO - Authorizing Official**C****Chain of Trust:** See authentication chain**Chained Secure Zone:** A DNS zone in which there is an authentication chain from the zone to a trust anchor.**CISA** - Cybersecurity and Infrastructure Security Agency**CMMI** - Capability Maturity Model Integration**CIO** - Chief Information Officer**CISA** - Cybersecurity and Infrastructure Security Agency**CVVS** - Common Vulnerability Scoring System

Exhibit 10.8.5-6 (Cont. 1) (05-12-2025)**Terms and Acronyms****D**

DAC - Discretionary Access Control

Delegation Point: The name at the parental side of a zone cut. That is, the delegation point for “finance.irs.gov” would be the finance.irs.gov node in the “.irs.gov” zone.

Demilitarized Zone (DMZ): A network zone created using firewalls creating a buffer between the internal domain and the public domain where higher risk servers requiring access by the public are placed.

DLV - DNSSEC Lookaside Validation

DMZ - Demilitarized Zone

DNS - Domain Name System

DNSSEC - Domain Name System Security Extensions

DNSSEC-Aware Name Server: An entity acting in the role of a name server that understands the DNS security extensions as defined in NIST SP 800-81.

DNSSEC-Aware Recursive Name Server: An entity that acts in both the DNSSEC-aware name server and DNSSEC-aware resolver roles.

DNSSEC-Aware Resolver: An entity that sends DNS queries, receives DNS responses, and understands the DNSSEC specification, although incapable of performing validation.

DNSSEC-Aware Stub Resolver: An entity acting in the role of a stub resolver that has an understanding of the DNS security extensions. DNSSEC-aware stub resolvers may be either “validating” or “nonvalidating”.

DNS-Notify: A protocol defined by RFC 1996 whereby a master server sends a Notify Request to slave servers when a change has occurred in the master zone file. The slave responds with a Notify Response and queries the SOA record. If the serial number has changed, a zone transfer is initiated by the slave server.

DoS - Denial of Service

DRP - Disaster Recovery Plan

DS - Delegation Signer

DSS - Digital Signature Standard

Dynamic Updating: A name server which uses an automated method of populating information in resource records within the zone for which it is authoritative. An example would be a name server that uses DHCP records to update information on workstations within a zone.

E

ED - Emergency Directive

EFC - Enterprise FISMA Compliance

EO - Executive Order

External System Service Provider - A provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business part-

Exhibit 10.8.5-6 (Cont. 2) (05-12-2025)**Terms and Acronyms**

nerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. [CNSSI: 4009]

F

FIPS - Federal Information Processing Standards

FQDN - Full Qualified Domain Name

FISMA- Federal Information Security Modernization Act of 2014#

H

Hidden Master Authoritative: An authoritative DNS server whose IP address does not appear in the name server set for a zone. If the master authoritative name server is "hidden", a secondary authoritative name server may reside on the same network as the hidden master.

Hidden Master: An authoritative name server that does not accept DNS queries and is not listed in the NS records for the zone. It performs zone transfers to slave servers that then respond to DNS queries within the zone.

HIDS - Host Intrusion Detection System

HMAC - Hash-Based Message Authentication Code

I

IETF - Internet Engineering Task Force

IPS - Intrusion Prevention System

Island of Security: A signed, delegated zone that does not have an authentication chain from its delegating parent. That is, there is no DS RR containing a hash of a DNSKEY RR for the island in its delegating parent zone. An island of security is served by DNSSEC-aware name servers and may provide authentication chains to any delegated child zones. Responses from an island of security or its descendants can be authenticated only if its authentication keys can be authenticated by some trusted means out of band from the DNS protocol.

ISCP - Information System Contingency Plan

IT - Information Technology

ITIL - Information Technology Infrastructure Library

K

Key Rollover: The process of generating and using a new key (symmetric or asymmetric key pair) to replace one already in use. Rollover is done because a key has been compromised or is vulnerable to compromise as a result of use and age.

Key Signing Key (KSK): An authentication key that corresponds to a private key used to sign one or more other authentication keys for a given zone. Typically, the private key corresponding to a key signing key will sign a zone signing key, which in turn has a corresponding private key that will sign other zone data. See also .zone signing key.

L

Exhibit 10.8.5-6 (Cont. 3) (05-12-2025)**Terms and Acronyms**

LAN - Local Area Network

LSS - Lean Six Sigma

M

MAC - Message Authentication Code

N

NARA- National Archives and Records Administration

NIDS - Network Intrusion Detection System

NIST - National Institute of Standards and Technology

Nonvalidating DNSSEC-Aware Stub Resolver: A stub resolver that understands DNSSEC responses but depends on a DNS server to perform any validation of DNSSEC signed records.

NS - Name Server

NSA - National Security Agency

NSEC - Next Secure: This record is used in “negative answers” to prove that a name does not exist. Each name in a zone has an NSEC record added when signed to allow both positive (this name exists) answers and negative answers (this name does not exist) to be cryptographically secure.

NTP - Network Time Protocol

O

OMB - Office of Management and Budget

OS - Operating System

P

Parent Domain: The next higher domain in a DNS hierarchy. For example, the parent server for accounting.finance.irs.gov would be finance.irs.gov.

Parent Server - A name server that belongs to the parent domain (see Parent Domain).

PKI - Public Key Infrastructure

R

RFC - Request for Comments

RBD - Risk-Based Decision - Decision made by individuals responsible for ensuring security by utilizing a wide variety of information, analysis, assessment and processes. The type of information considered 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).

Risk Acceptance Decision - A decision in which the AO determines if they’re going to accept the risk.

Exhibit 10.8.5-6 (Cont. 4) (05-12-2025)**Terms and Acronyms**

RP - Responsible Person

RR - Resource Record

RRSet - Resource Record Set: A complete set of resource records of the same type. That is, all NS records for a given name, or all DNSKEY records.

RRSIG - Resource Record Signature: These records hold the signatures for a specific record type. For instance, you will see an RRSIG for NS records, one for DNSKEY records, etc. One RRSIG record will be generated per ZSK, typically, and for certain records one for each KSK as well. Note that there is one signature per-key per-RRSET, not per RR.

RSA - Rivest Shamir Adelman

S

SA&A - Security Assessment and Authorization

SBU - Sensitive But Unclassified

Secure Entry Point: See Trust Anchor.

SHA - Secure Hash Algorithm

SHS - Secure Hash Standard

Signed Zone: A zone whose RRsets are signed and which contains properly constructed DNSKEY, RRSIG, NSEC, and (optionally) DS records.

SOA - Start of Authority

SOP - Standard Operating Procedure

SP - Special Publication

SRM - Security Risk Management

STIG - Security Technical Implementation Guide

Subdomain: The next lower domain in a DNS hierarchy (see Parent Domain).

T

TD - Treasury Directive

TCP - Transmission Control Protocol

TLD - Top-Level Domain

Transaction Signature (TSIG) Key: A string used to generate the message authentication hash stored in a TSIG RR and used to authenticate an entire DNS message. This is not the same as signing a message, which involves a cryptographic operation. TSIG keys are used for securing zone transfers.

Trust Anchor: A configured DNSKEY RR or DS RR hash of a DNSKEY RR. A validating DNSSEC-aware resolver uses this public key or hash as a starting point for building the authentication chain to a signed DNS response. In general, a validating resolver will need to obtain the initial values of its trust anchors via some

Exhibit 10.8.5-6 (Cont. 5) (05-12-2025)**Terms and Acronyms**

secure or trusted means outside the DNS protocol. The presence of a trust anchor also implies that the resolver should expect the zone to which the trust anchor points to be signed. This is sometimes referred to as a secure entry point.

TTL - Time to Live

TXT - Text

U

UDP - User Datagram Protocol

UNS - User and Network Services

Unsigned Zone - A zone that is not signed.

V

Validator - A component that validates DNSSEC signatures. Usually not a separate component but part of a DNSSEC-aware recursive server (sometimes referred to as a validating resolver or validating recursive server).

W

Whitelist - A list that contains allowed entities such as users, IP addresses, servers, etc.

Z

Zone Apex - The node of the DNS namespace that is at the top of the zone. See also delegation point.

Zone File - The file which contains all the DNS resource records for a specific DNS zone.

Zone Signing Key (ZSK) - An authentication key that corresponds to a private key used to sign a zone. Typically a zone signing key will be part of the same DNSKEY RRSset as the key signing key whose corresponding private key signs this DNSKEY RRSset, but the zone signing key is used for a slightly different purpose and may differ from the KSK in other ways, such as validity lifetime. Designating an authentication key as a zone signing key is purely an operational issue: DNSSEC validation does not distinguish between zone signing keys and other DNSSEC authentication keys, and it is possible to use a single key as both a key signing key and a zone signing key (See also key signing key).

Zone Transfer - The process of copying the zone file containing all DNS resource records for a zone from one server to another.

Exhibit 10.8.5-7 (05-12-2025)**Related Resources****IRS Publications**

- IRM 1.15.6, *Records and Information Management, Managing Electronic Records*.
- IRM 10.5.1, *Privacy and Information Protection, Privacy Policy*.
- IRM 10.8.1, *Information Technology (IT) Security, Security Policy*.
- IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*.
- IRM 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy*.
- IRM 10.9.1, *Classified National Security Information (CNSI)*.

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.
- Treasury publications are available on the *Treasury Cybersecurity Policy* site.

National Institute of Standards and Technology (NIST) Publications

- 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).
- FIPS 140-3: Federal Information Processing Standards Publication 140-3, “*Security Requirements for Cryptographic Modules*,” issued March 22, 2019.
- FIPS 180-4, Federal Information Processing Standards Publication 180-4, “*Secure Hash Standard (SHS)*,” issued August 04, 2015.
- FIPS 186-5: Federal Information Processing Standards Publication FIPS 186-5, “*Digital Signature Standard (DSS)*,” issued February 2, 2023.
- FIPS 198-1, Federal Information Processing Standards Publication 198-1, “*The Keyed-Hash Message Authentication Code (HMAC)*,” issued July 16, 2008.
- FIPS 199: Federal Information Processing Standards Publication 199, “*Standards for Security Categorization of Federal Information and Information Systems*,” issued February 01, 2004.
- FIPS 200: Federal Information Processing Standards Publication 200, “*Minimum Security Requirements for Federal Information and Information Systems*,” issued March 01, 2006.
- 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, “*Assessing Security and Privacy Controls in Information Systems and Organizations*,” issued January 25, 2022.
- SP 800-53B: NIST Special Publication 800-53B, “*Control Baselines for Information Systems and Organizations*,” issued as December 10, 2020.
- SP 800-57: NIST Special Publication 800-57, “*Recommendation for Key Management – Part 1: General (Revised)*,” issued May 04, 2020.
- SP 800-57: NIST Special Publication 800-57, “*Recommendation for Key Management – Part 2: Best Practices for Key Management Organization*,” issued May 23, 2019.
- SP 800-90A: NIST Special Publication 800-90A, “*Recommendation for Random Number Generation Using Deterministic Random Bit Generators*,” issued June 24, 2015.
- SP 800-81-2: NIST Special Publication 800-81-2, “*Secure Domain Name System (DNS) Deployment Guide*,” issued September 18, 2013.
- SP 800-123: NIST Special Publication 800-123, “*Guide to General Server Security*,” issued July 25, 2008.
- NIST publications are available on the *NIST Computer Security Resource Center Publications* site

Exhibit 10.8.5-7 (Cont. 1) (05-12-2025)**Related Resources****Defense Information Systems Agency (DISA)**

- SRG: DISA Domain Name System (DNS) Security Requirements Guide (SRG) V4R1, issued 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 Security Requirements Checklists SharePoint site. The DISA version and release for each guide is contained within each checklist. Refer to Exhibit # 10.8.5-5 #, *Security Requirement Checklists*, for additional information.
- DISA security guides are available on the *DISA STIGs Document Library* site.

Other Publications

- RFC: 4033: RFC 4033, “*DNS Security Introduction and Requirements*,” issued March 1, 2005.
- CISA: ED-19-01: Cybersecurity and Infrastructure Security Agency (CISA) Emergency Directive 19-01, “*Migrating DNS Infrastructure Tampering*,” issued January 22, 2019.
- OMB: M-08-03: Office of Management and Budget Memorandum 08-03, “*Securing the Federal Government’s Domain Name System Infrastructure*,” issued August 22, 2008.
- OMB: M-22-09: Office of Management and Budget Memorandum 22-09, “*Moving the US Government Toward Zero Trust Cybersecurity Principles*,” issued January 26, 2022.

