



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.5

OCTOBER 24, 2023

EFFECTIVE DATE

(10-24-2023)

PURPOSE

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

MATERIAL CHANGES

- (1) Subsection 10.8.5.3.18.4 SC-13 Cryptographic Protection has been updated to incorporate Zero Trust Architecture guidance from OMB memo 22-09.
- (2) Internal controls were realigned to comply with SPDER/IMD requirements;
 - a. The following subsections have been added; Program Management and Review, Program Controls, Terms and Acronyms, Related Resources.
 - b. Original 10.8.5.3 Roles and Responsibilities and subsections relocated to be new 10.8.5.1.3 Roles and Responsibilities.
 - c. Original 10.8.5.1.2 (1) text moved to the new 10.8.5.1.7 Program Controls subsection.
 - d. Original 10.8.5.1.2 (2) text moved to the new 10.8.5.1.7 Program Controls subsection.
 - e. Original 10.8.5.1.2 (3) text identified as redundant and removed.
 - f. Original 10.8.5.1.2 (4) text moved to Exhibit 10.8.5-5 Security Requirements Checklists.
 - g. Original 10.8.5.1.2 (5) text moved to the new 10.8.5.1.7 Program Controls subsection.
 - h. Original 10.8.5.1.3 (1) text incorporated with language in new 10.8.5.1.7 Program Controls subsection.
 - i. Original 10.8.5.1.3 (2) text moved to 10.8.5.4 IT Security Controls subsection.
 - j. Original 10.8.5.1.3 (2) text moved to 10.8.5.4 IT Security Controls subsection.
 - k. Original 10.8.5.1.10 Risk Acceptance and Risk-Based Decisions moved to be new 10.8.5.2 Risk Acceptance and Risk-Based Decisions subsection.
- (3) Editorial changes (including grammar, spelling and minor clarification) were made throughout the IRM.

EFFECT ON OTHER DOCUMENTS

IRM 10.8.5 dated October 1, 2021, is superseded. This IRM supersedes all prior versions of IRM 10.8.5. This IRM supplements IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance* and IRM 10.8.2, *Information Technology (IT) Security, Roles and Responsibilities*.

AUDIENCE

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

Kaschit Pandya
Acting, Chief Information Officer

#

10.8.5.1
(10-24-2023)
Program Scope and Objectives

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

10.8.5.1.1
(10-24-2023)
Background

- (1) This IRM defines the controls for the use of DNS within the IRS.
- (2) IRM 10.8.5 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Information Technology Cybersecurity.
- (3) This DNS policy provides the technical security policies and requirements for applying security concepts to systems.
- (4) This policy 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 policy, 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 TSIG (hash-based Transaction Signature) for authenticating zone updates.
- (7) This policy does not address the DNS configuration of DNS clients (i.e., the workstations, servers, and network devices that query name servers).
- (8) Each of these DNS resolver clients' security posture should be validated with the security IRM and checklists for the underlying technology or operating system.

- 10.8.5.1.2
(10-24-2023)
Authority
- (1) All IRS systems and applications shall be compliant with Executive Orders (E.O.s), Office of Management and Budget (OMB), Federal Information Security Modernization Act of 2014 (FISMA), National Institute of Standards and Technology (NIST), Cybersecurity and Infrastructure Security Agency (CISA), National Archives and Records Administration (NARA), Department of the Treasury, and IRS guidelines as they apply.
- 10.8.5.1.3
(10-24-2023)
Roles and Responsibilities
- (1) IRM 10.8.2, **Information Technology (IT) Security, IT Security Roles and Responsibilities**, defines IRS-wide roles and responsibilities related to IRS information and computer security, and is the authoritative source for such information.
- (2) The supplemental roles and responsibilities provided below are specific to the implementation of IRS DNS.
- 10.8.5.1.3.1
(10-24-2023)
Information System Owner
- (1) The Information System Owner shall be the agency official responsible for the overall procurement, development, integration, modification, and operation and maintenance of the information system as defined by IRM 10.8.2. At the IRS, the Information System Owner is the Business and Functional Unit Owner.
- (2) Business and Functional Unit Owners shall ensure that all requirements within this IRM related to their systems are implemented.
- (3) Business and Functional Unit Owners shall ensure that the planning, operation and monitoring of their DNS services are properly coordinated with User and Network Services (UNS) and Cyber Security.
- 10.8.5.1.3.2
(10-24-2023)
DNS Key Administrator
- (1) The DNS Key Administrator shall 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, Sec. 9)
- (2) The primary purpose of the role shall 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-Defined)
- (3) The DNS Key Administrator shall be responsible for ensuring the execution of the following in compliance with this IRM: (NIST SP 800-81-2, Sec. 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.

- 10.8.5.1.3.3
(10-24-2023)
DNS Zone Administrator
- (1) The DNS Zone Administrator shall:
- a. Manage the creation and modification of DNS records, but shall not manage the signing of those records.
 - b. Ensure the compliance of DNS records with this policy.
 - 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.
- 10.8.5.1.3.4
(10-24-2023)
User and Network Services (UNS)
- (1) UNS shall:
- 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 countermeasures in order to protect IRS systems.
- 10.8.5.1.4
(10-24-2023)
Program Management and Review
- (1) The IRS Security Policy Program establishes a framework of security controls to ensure the inclusion of security in the daily operations and management of IRS IT resources. This framework of security controls is provided through the issuance of security policies via the IRM 10.8.x series and the development of technology specific 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:
- a. To establish and manage an Information Security Program within all its offices. This policy provides uniform policies and guidance to be used by each office.
 - b. To 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. To protect its information resources and allow the use, access, disposition, and disclosure of information in accordance with applicable laws, policies, federal regulations, Office of Management and Budget (OMB) guidance, Treasury Directives (TDs), NIST Publications, National Archives and Records Administration (NARA) guidance, other regulatory guidance, and best practice methodologies.
 - d. To use best practices methodologies (such as Capability Maturity Model Integration (CMMI), Enterprise Life Cycle (ELC), Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve IRS IT process and service efficiency and effectiveness.

10.8.5.1.5
(10-24-2023)
Program Controls

- (1) This IRM applies to all IRS information and information systems, which include IRS production, development, test, and contractor systems. For systems that store, process, or transmit classified national security information, refer to IRM 10.9.1, **Classified National Security Information (CNSI)**, for additional guidance for protecting classified information.
- (2) In the event there is a discrepancy between this policy and IRM 10.8.1, IRM 10.8.1 takes precedence, unless the security controls/requirements in this policy are more restrictive, or, otherwise noted.
- (3) This IRM establishes the minimum baseline security policy and requirements for all DNS services in order to:
 - a. Protect the critical infrastructure and assets of the IRS against attacks that exploit IRS assets.
 - b. Prevent unauthorized access to IRS assets.
 - c. Enable IRS IT computing environments to meet the security requirements of this policy and support the business needs of the organization.

10.8.5.1.6
(10-24-2023)
Terms and Acronyms

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

10.8.5.1.7
(10-24-2023)
Related Resources

- (1) Refer to Exhibit 10.8.5-7 for a list of related resources and references.

10.8.5.2
(10-24-2023)
Risk Acceptance and Risk-Based Decisions

- (1) Any exception to this policy requires that the Authorizing Official (AO) make a Risk-Based Decision (RBD).
- (2) Users shall submit 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.

#

#

#

#

#

#

#

#

#

#

#

#

#

#

This Page Intentionally Left Blank

#

#

