



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.54

JULY 22, 2024

EFFECTIVE DATE

(07-22-2024)

PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.8.54, *Information Technology (IT) Security, Minimum Firewall Administration Requirements*.

MATERIAL CHANGES

- (1) Throughout this IRM, requirements written with “shall” verbiage updated to “must” to align with industry writing best practices.
- (2) Throughout the IRM: A leading “zero” (0) added to NIST control and control enhancement numbers as part of alignment with NIST SP 800-53 Rev 5.1.1 release. Example: “AC-1(1)” becomes “AC-01(01)”
- (3) Moved roles and responsibilities that are specific to firewall administration from 10.8.54.1.3 to new subsection 10.8.54.3 to align with Internal Control requirements. Sections were renumbered accordingly.
- (4) IRM 10.8.54.4.3.1(6) and 10.8.54.4.3.2 were revised to incorporate Interim Guidance Memorandum #IT-10-0522-0007, AU-4 Section Addition.
- (5) IRM 10.8.54.1.3, Roles and Responsibilities updated to align with Security Policy Boilerplate.
- (6) IRM 10.8.54.1.4, Program Management Review updated to align with Security Policy Boilerplate.
- (7) Exhibit 10.8.54-1 updated to align with Security Policy Boilerplate.
- (8) Exhibit 10.8.54-3 updated with additional acronyms.
- (9) Exhibit 10.8.54-4 updated IRM 10.8.50 title in accordance with IRM 10.8.1.
- (10) Exhibit 10.8.54-4 updated SRG reference with the most recent version number.
- (11) Updated Responsible Official from Kaschit Pandya to Rajiv Uppal.
- (12) Editorial changes including grammar, spelling, and minor clarifications were made throughout the IRM.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 10.8.54 dated November 3, 2023. This IRM incorporates Interim Guidance Memorandum IT-10-0522-0007, AU-4 Section Addition. This IRM supplements IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance*; and IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*.

AUDIENCE

The provisions in this manual apply to:

- a) All personnel responsible for ensuring that adequate security is provided for the Internal Revenue Service (IRS) information and systems.
- b) All employees, contractors, and vendors of the IRS who own or operate a perimeter firewall environment.

Rajiv Uppal
Chief Information Officer

Minimum Firewall Administration Requirements

10.8.54.1 Program Scope and Objectives

- #### 10.8.54.2 Risk Acceptance and Risk-Based Decisions

10.8.54.3.1	Computer Security Incident Response Center (CSIRC)
10.8.54.3.2	IT User and Network Services (UNS)
10.8.54.3.3	Information System Owner/Business and Functional Unit Owner

#

#

Exhibits

#

10.8.54-4 Related Resources

10.8.54.1
(07-22-2024)
**Program Scope and
Objectives**

- (1) **Overview:** This IRM lays the foundation to implement and manage security controls and guidance for the use of firewall administration within the IRS.
 - a. This manual 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 firewall administration.
- (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 within this manual apply to:
 - a. All offices and business, operation 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 information 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:** Cyber Threat Response & Remediation (an organization within Cybersecurity)
- (6) **Program Goals:** Cybersecurity Policy is responsible for the development and maintenance of the IRS' enterprise information technology security policies. The IRM 10.8. series provides the minimum-security requirements to protect the confidentiality, integrity, and availability of data processed on IRS systems. IRMs are developed in accordance with applicable laws, policies, federal regulations, Office of Management and Budget (OMB), the Department of the Treasury Directives (TDs), National Institute of Standards and Technology (NIST) Publications, and National Archives and Records Administration (NARA).

10.8.54.1.1
(02-23-2022)
Background

- (1) Federal Information Processing Standard (FIPS) 200 mandates the use of NIST Special Publication (SP) 800-53 as an initial set of baseline security controls for the creation of agency IT security policy.
- (2) NIST SP 800-41 Rev 1, Guidelines on Firewalls and Firewall Policy was developed under NIST statutory responsibilities by the Federal Information Security Modernization Act of 2014 (FISMA).
- (3) IRM 10.8.54 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Information Technology Cybersecurity.

10.8.54.1.2
(02-23-2022)
Authority

- (1) All IRS information systems and applications must be compliant with Executive Orders (EOs), OMB, FISMA, NIST, the Cybersecurity and Infrastructure Security Agency (CISA), the Department of the Treasury, and IRS guidelines as they apply.

10.8.54.1.3
(11-03-2023)
**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 system security, and is the authoritative source for such information.

10.8.54.1.4
(11-03-2023)
**Program Management
Review**

- (2) The supplemental roles and responsibilities identified below are specific to the implementation of firewall processes.
- (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 series and the development of technology specific 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 all of its offices. The policy 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), 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.

10.8.54.1.5
(11-03-2023)
Program Controls

- (1) Each IRM in the 10.8 series is assigned an author who reviews their IRM annually 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. Revision to security policies and checklists are reviewed by the security policy team, in collaboration with applicable stakeholders, for potential impact to the IRS operational environment.
- (2) Security Policy provides a report identifying security policies and security requirements checklists that have recently been revised or are in process of being revised.
- (3) The 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.
- (4) This IRM establishes the minimum baseline security policy and requirements for IRS firewalls to:
 - a. Protect the critical infrastructure and assets of the IRS against attacks and 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.

- (5) 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.

10.8.54.1.6
(11-03-2023)

Terms and Acronyms

- (1) Refer to Exhibit # 10.8.54-3 # for a list of terms, acronyms, and definitions.

10.8.54.1.7
(11-03-2023)

Related Resources

- (1) Refer to Exhibit 10.8.54-4 for a list of related resources and references.

10.8.54.2
(11-03-2023)

**Risk Acceptance and
Risk-Based Decisions**

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

#

- (3) Refer to IRM 10.8.1 for additional guidance on Risk Acceptance.

10.8.54.3
(07-22-2024)

**Firewall Administration
Roles and
Responsibilities**

- (1) The supplemental roles and responsibilities identified in the following sections are specific to IRS firewall administration.

10.8.54.3.1
(07-22-2024)

**Computer Security
Incident Response
Center (CSIRC)**

- (1) The Information Technology (IT) Cybersecurity, Computer Security Incident Response Center (CSIRC) must establish and manage the IRS minimum firewall administration requirements.
(2) CSIRC must oversee and approve all rule sets for the IRS network perimeter firewall environments (see CSIRC Firewall Rule Set Configuration Management section of this IRM).
(3) In conjunction with overseeing the rule sets for the perimeter firewall environments, CSIRC is a voting stakeholder for the enterprise perimeter security architecture. CSIRC must review and approve, with IT and other business units, demilitarized zone (DMZ) design and daily operations efforts. (IRM 10.8.2)
(4) CSIRC must develop and maintain an audit plan to document what traffic will be logged. (IRM 10.8.2)
(5) CSIRC must provide direction to establish and update this IRM.

10.8.54.3.2 (07-22-2024) IT User and Network Services (UNS)	<div><div>(1) IT User and Network Services (UNS) Engineering, in conjunction with CSIRC, must design the IRS network perimeter DMZs, including firewall requirements; and be responsible for firewall implementation and maintenance. (IRM 10.8.2)</div><div>(2) IT UNS Engineering must (IRM 10.8.2):<div><div>a. Administer the firewall devices comprising the perimeter firewall environment.</div><div>b. Ensure that the IRS minimum firewall requirements and policies are met.</div><div>c. Provide operation, administration and maintenance (OA&M) for the firewall devices comprising the perimeter firewall environment. This includes, but is not limited to:<div><div>-Implementing CSIRC-approved Firewall Change Requests (FCRs).</div><div>-Troubleshooting access problems.</div><div>-Applying security patches and software updates.</div><div>-Refreshing hardware.</div><div>-Securing maintenance contracts.</div></div></div><div>d. Monitor the “up/down” status of the network and firewall devices in the IRS network perimeter DMZ.</div><div>e. Ensure the appropriate placement of the approved firewall rules (rule hierarchy) to prevent conflict with existing rules, upon approval by CSIRC.</div></div></div><div>(3) The Information System Owner for IT UNS Engineering must:<div><div>a. Be responsible for notifications and routing of information to the appropriate organizational points-of-contact (POCs).</div><div>b. Notify CSIRC of any Knowledge Incident/Problem Service Asset Management (KISAM) ticket needing CSIRC’s attention.</div><div>c. Notify CSIRC for a user’s problem that originated with the Enterprise Service Desk.</div><div>d. Report suspicious activities or incidents.</div></div></div></div>
10.8.54.3.3 (07-22-2024) Information System Owner/Business and Functional Unit Owner	<div><div>(1) This IRM is to be implemented by all organizations that own or operate a perimeter firewall environment; these organizations must comply with the same requirements established for IT.</div></div>

#

#

#

#

#

#

#

#

#

#

##

#

#

[illegible]

#

#####

[illegible]

[illegible]

[illegible]

#

##

##

[illegible]

[illegible]

[illegible]

#

[illegible]

#####

[illegible][illegible]

[illegible]

#####

#

Exhibit 10.8.54-4 (07-22-2024)**Related Resources****IRS Publications**

- IRM 10.8.1, *Policy and Guidance*.
- IRM 10.8.2, *IT Security Roles and Responsibilities*.
- IRM 10.8.15, *General Platform Operating System Security Policy*.
- IRM 10.8.50, *Enterprise Incident, Vulnerability, and Security Patch Management*.
- IRM 10.8.60, *IIT Service Continuity (ITSCM) Policy and Guidance*.
- IRM 10.8.62, *Information System Contingency Plan (ISCP) and Disaster Recovery (DR) Test, Training, and Exercise (TT&E) Program*.
- IRM 10.9.1, *Classified National Security Information (CNSI)*.

The Department of the Treasury Publications

- TD P 85–01, v3.1.3 *Treasury Information Technology (IT) Security Program*, February 28, 2022.

National Institute of Standards and Technology (NIST) Publications

- NIST Special Publication (SP) 800-37 Rev 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, December 20, 2018.
- NIST Special Publication (SP) 800-41, Rev 1. *Guidelines on Firewalls and Firewall Policy*, September 28, 2009.
- NIST Special Publication (SP) 800-53 Rev 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020 (includes updates as of December 10, 2020).
- NIST Special Publication (SP) 800-53A Rev 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*, January 25, 2022.
- NIST Special Publication (SP) 800-70 Rev 4, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*, February 15, 2018.
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 1, 2004.
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 1, 2006.

Defense Information Systems Agency (DISA) Publications

- DISA, *Firewall Security Requirements Guide (SRG)*, V2R3, October 21, 2022.
- 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 Control Exhibit SharePoint site. DISA version and release for each guide is contained within each checklist. Refer to Exhibit # 10.8.54-1 # for additional information.
- DISA Security Guides are available at: <https://public.cyber.mil/stigs/>

Center for Internet Security (CIS) Publications

- CIS Benchmarks are used as a basis for producing IRS Security Requirements Checklists. The security requirements checklists are updated as CIS releases updated guidance and are posted in the IRS Security Control Exhibit SharePoint site. The CIS version for each benchmark is contained within each checklist. Refer to Exhibit # 10.8.54-1 # for additional information.
- CIS benchmarks are available at: <https://www.cisecurity.org/cis-benchmarks/>