MANUAL TRANSMITTAL

10.8.22

Department of the Treasury
Internal Revenue Service

NOVEMBER 3, 2023

EFFECTIVE DATE

(11-03-2023)

PURPOSE

(1) This transmits revised IRM 10.8.22, *Information Technology (IT) Security, Web Server Security Policy.*

MATERIAL CHANGES

(1) IRM 10.8.22.1 updated to align with IRM 1.11.2, Internal Management Documents System, Internal Revenue Manual (IRM) Process Internal Controls.

(2) Editorial changes (including grammar, spelling, and minor clarifications) were made throughout the IRM.

EFFECT ON OTHER DOCUMENTS

IRM 10.8.22 dated February 08, 2022, is superseded. This IRM supplements IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance and IRM 10.8.2 Information Technology (IT) Security, Security Roles and Responsibilities.

AUDIENCE

IRM 10.8.22 shall be distributed to all IRS personnel responsible for ensuring that adequate security is provided for IRS information and systems. This policy applies to all employees, contractors, and vendors of the IRS.

Kaschit Pandya
Acting, Chief Information Officer

10.8.22
Web Server Security Policy

Table of Contents

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

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

Exhibits

10.8.22.1
(11-03-2023)
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 web servers within the Internal Revenue Service (IRS).

a. This manual is supplements IRM 10.8.1, *Information Technology (IT) Security*, *Policy and Guidance*, and augments the existing requirements identified in IRM 10.8.1, as they relate to IRM web servers.

(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 businesses, 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.

(4) **Policy Owner**: Chief Information Officer

(5) **Program Owner**: Cybersecurity Threat Response & Remediation (an organization within Cybersecurity)

(6) **Program Goals**: Cybersecurity Policy is responsible for the development and maintenance of IRS's enterprise information technology security policies. The IRM 10.8.X 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), Treasury Directives (TDs), National Institute of Standards and Technology (NIST) Publications, and National Archives and Records Administration (NARA).

10.8.22.1.1
(02-08-2022)
Background

(1) Web servers provide data via an internally or publicly-exposed interface and are well-known targets for exploitation. Unprotected Web servers provide an avenue for malicious activity such as theft or the denial of service to IRS resources. An improperly implemented server can be attacked directly and be used as a staging area to obtain unauthorized access to IRS internal resources.

a. This policy defines the security controls for Web servers.
b. This IRM provides the security configuration standards required to ensure Web server software is integrated and used appropriately for all IRS systems.

(2) IRM 10.8.22, is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Information Technology Cybersecurity.

10.8.22.1.2
(02-08-2022)
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), Department of Homeland Security (DHS), Treasury, and IRS guidelines as they apply.

10.8.22.1.3
(11-03-2023)
Roles and Responsibilities

(1) IRM 10.8.2, *Information Technology (IT) Security Roles and Responsibilities*, defines IRS-wide roles and responsibilities related to IRS information and information system security, and is the authoritative source for such information.

10.8.22.1.4
(11-03-2023)
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 of 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 resouces 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.

10.8.22.1.5
(11-03-2023)
Program Controls

(1) Each IRM in the 10.8.x 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, DISA) for potential revisions to security policies and security requirement 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 requirement checklists that have recently been revised or are in the process of being revised.

(3) 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 (NSI), for additional guidance for protecting classified information.

(4) This IRM establishes the minimum baseline security policy and requirements for IRS application security and development 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.

(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.

10.8.22.1.6
(11-03-2023)
Terms and Acronyms

(1) Refer to Exhibit 10.8.22-2 for a list of terms, acronyms, and definitions.

10.8.22.1.7
(11-03-2023)
Related Resources

(1) Refer to Exhibit 10.8.22-3 for a list of related resources and references.

10.8.22.1.8
(02-08-2022)
Risk Acceptance and Risk-Based Decisions

(1) Any exception to this policy requires the Authorizing Official (AO) to make a Risk-Based Decision.

(2) Users shall submit RBD requests in accordance with Cybersecurity's Security Risk Management (SRM) Risk Acceptance Process within the Risk-Based Decision (RBD) Standard Operating Procedure (SOP).

#
#
#
#

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

10.8.22.2
(02-08-2022)
IT Security Controls

#
#

#
#

#
#
#

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

#
#
#

#
#
#
#

#

#
#
#

#

#
#
#
#
#
#
#

#
#
#
#
#
#
#

#
#

#

#
#
#
#
#
#
#

#

#
#
#

#
#
#
#
#

#
#
#
#

#

#
#
#
#
#
#
#
#
#
#

#

#

#
#
#
#
#
#
#
#
#

#
#

#
#
#
#
#
#
#
#
#
#

#

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

#
#
#

#
#

#
#
#
#

#
#

#
#
#

#
#
#

#
#

#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#

#
#
#

#

#
#
#
#
#
#
#

#
#

#
#
#

#
#
#

#
#
#
#
#

#
#
#
#

#
#
#

#
#
#
#
#
#
#

#
#
#

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

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#

#
#
#

#
#
#
#

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

#
#
#
#
#
#
#

#
#
#

#
#

#

#
#
#
#

#
#
#
#
#
#
#
#

#

#
#
#
#
#
#

#
#

#
#
#

#
#
#

#
#

#
#
#

#
#

#
#
#
#
#
#
#

#
#
#
#

#
#

#

#
#
#
#
#
#
#
#

#

#
#
#
#
#
#
#

#
#

#
#
#
#
#
#
#
#

#
#
#
#
#
#
#

#
#
#

#
#

#

#
#
#
#

#
#
#

#
#

#
#
#

#

This Page Intentionally Left Blank

Exhibit 10.8.22-1 (02-08-2022)
Security Requirements Checklists

#
#
#
#
#
#

a. Select the appropriate IRM folder.
b. Security Checklists are available for the following:

- General Web Server
- Apache HTTP Server
- Microsoft Intranet Information Server (IIS)

2. Security Checklists shall be effective immediately. Vulnerabilities shall be remediated in accordance with IRM 10.8.50 remediation timelines table. The source's publication date can be found in the external reference row of the checklist. (Typically row 10)
3. Checklists for technologies that are no longer supported by either DISA or CIS won't receive further updates. These checklists will be removed from the active checklist and moved to an Archive folder during the next checklist update cycle.
4. Evaluate system configurations and implement controls while system functionality.

Exhibit 10.8.22-2 (02-08-2022)
Glossary and Acronyms

Term	Definition or description
Authentication	The process of verifying the identity or location of a user, service or application. Authentication is performed using at least one of three mechanisms: “something you have”, “something you know” or “something you are”. The authenticating application may provide different services based on the location, access method, time of day, etc.
Authorization	The determination of what resources a user, service or application has permission to access. Accessible resources can be URLs, files, directories, servlets, databases, execution paths, etc.
Authorizing Official (AO)	See IRM 10.8.2 for a detailed description of an AO’s responsibilities.
Basic Authentication	A simple form of client-side authentication supported in HTTP. The http-client sends a request header to the web server containing a Base64 encoded username and password. If the username/password combination is valid, the web server grants the client access to the requested resource.
CA	Certification Authority
Cipher Suite	A named combination of authentication, encryption, and message authentication code algorithms use to negotiate the security settings for a network connection using a network protocol.
Common Gateway Interface (CGI)	Programming standard for software to interface and execute applications residing on web servers.
Compiler	A computer program that translates a high-level programming language into machine readable language. The compiler usually converts the high-level language into assembly language first, and then translates the assembly language into machine language. The program fed into the compiler is called the source program; the generated machine language program is called the object program.
CRL	Certificate Revocation List
CTL	Certificate Trust List
DoS	Denial of Service
EA	Enterprise Architecture

Exhibit 10.8.22-2 (Cont. 1) (02-08-2022)
Glossary and Acronyms

Enterprise Architecture (EA) Enterprise Standards Profile (ESP)	The authoritative repository for IRS approved products and standards.
Enterprise Life Cycle (ELC)	Enterprise architecture is the dynamic, iterative process of changing the enterprise overtime by incorporating new business processes, new technology, and new capabilities, as well as maintenance, disposition and disposal of existing elements of the enterprise.
File Transfer Protocol (FTP)	A client/server protocol for exchanging files with a host computer.
Federal Information Processing Standards (FIPS)	A set of standards that describe document processing, encryption algorithms and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies.
Federal Information Security Management (FISMA)	A framework for managing information security that must be followed for all information systems used or operated by a U.S. federal government agency in the executive or legislative branches, or by a contractor or other organization on behalf of a federal agency in those branches.
GMT	Greenwich Mean Time
HyperText Transfer Protocol (HTTP)	A protocol scheme used on the World Wide Web. HTTP describes the way a web-client requests data and how a web server responds to those requests.
HyperText Transfer Protocol Secure (HTTPS)	A secure form of communication over a computer network by layering HTTP on top of the SSL/TLS protocol.
Internet Information Services (IIS)	Formerly known as Internet Information Server, is a web server product by Microsoft and is used with Microsoft operating systems.
Internet Protocol (IP)	The principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries.
Internet Server Application Program Interface (ISAPI)	An API for Microsoft's Internet Information Server (IIS) Web server. ISAPI enables programmers to develop Web-based applications running faster than conventional CGI programs.
IT	Information Technology

Exhibit 10.8.22-2 (Cont. 2) (02-08-2022)
Glossary and Acronyms

Internal Web Server	A private server with a private IP address and is not visible to the Internet (i.e. irweb.irs.gov).
Metabase	A repository for most Internet Information Services (IIS) configuration values. The metabase is a plaintext XML file and can be edited manually or programmatically. The metabase is efficiently extensible. As IIS deployment grows, so does the metabase.
MIME	Multipurpose Internet Mail Extensions
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.
Public Web Server	A server that is configured with a public IP address and is completely visible to the Internet (i.e. irs.gov).
SA&A	Security Assessment and Authorization
SBU	Sensitive But Unclassified
Secure Sockets Layer (SSL)	An industry standard public-key protocol used to create encrypted tunnels between two network-connected devices.
Session ID	A string of data provided by the web server, normally stored within a cookie or URL. A Session ID tracks a user's session, or perhaps just his current session, as he traverses the web site.
Script	A program run on a Web server, in response to input from a browser.
Scripting language	A programming language that allows control of one or more applications and makes the compiler of the language part of the language runtime, and as a result, enables code to be generated dynamically. ″Scripts″ are distinct from the core code of the application, as they are usually written in a different language and are often created or at least modified by the end-user.
Transport Layer Security (TLS)	An authentication and security protocol widely implemented in browsers and Web servers.
Universal Resource Locator (URL)	A standard way of specifying the location of an object, normally a web page, on the Internet.
UTC	Coordinated Universal Time

Exhibit 10.8.22-2 (Cont. 3) (02-08-2022)
Glossary and Acronyms

WebDAV	Web Distributed Authoring
Web Server	A general-purpose software application that handles and responds to HTTP requests. A web server may utilize a web application for dynamic web page content.
Web Service	A software application that uses Extensible Markup Language (XML) formatted messages to communicate over HTTP. Typically, software applications interact with web services rather than normal users.

Exhibit 10.8.22-3 (02-08-2022)
References

IRS Publications

- IRM 1.4.6 - *Resource Guide for Managers, Managers Security Handbook*
- IRM 1.15.x series - Records and Information Management
- IRM 10.2.x - Physical Security Program
- IRM 10.8.1 – *Information Technology (IT) Security, Policy and Guidance*
- IRM 10.8.2 – *Information Technology (IT) Security, Security Roles and Responsibilities*
- IRM 10.8.6 - Information Technology (IT) Security, Application Security and Development
- IRM 10.8.50 - Information Technology (IT) Security, Servicewide Security Patch Management
- IRM 10.8.52 - Information Technology (IT) Security, PKI Security Policy
- IRM 10.8.60 - Information Technology (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance
- IRM 10.9.1 - Classified National Security Information (NSI)

Note: IRS IRMs are available on IRM Online at *http://irm.web.irs.gov/*.

Department of the Treasury Publications

- TD P 85–01, Version 3.1.2 *Treasury Information Technology (IT) Security Program*, November 3, 2020

National Institute of Standards and Technology (NIST) Publications

- NIST FIPS 199: *Standards for Security Categorization of Federal Information and Information Systems*
- NIST FIPS 200: *Minimum Security Requirements for Federal Information and Information Systems*
- NIST SP 800-37 Rev 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, September 20, 2018
- NIST SP 800-52 Rev 2, Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations, August 2019
- NIST SP 800-53 Rev 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, April 2013 (includes updates as of January 22, 2015)
- NIST SP 800-53A Rev 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*, December 2014 (includes updates as of December 18, 2014)

Defense Information Systems Agency (DISA) Publications

- Web Server SRG V2R2, October 23, 2015
- Security Technical Implementation Guides (STIGS) are used as a basis for producing IRS Exhibit Checklists. The security checklists are updated as DISA releases updated guidance and are posted on the IRS Security Control Exhibit SharePoint site. The DISA version and release for each guide is contained within each checklist. Refer to the Security Requirements Checklists exhibit for additional information.
- DISA security guides are available at: *https://public.cyber.mil/stigs/*

Center for Internet Security Publications

- CIS Benchmarks are used as a basis for producing IRS Security Requirements Checklists. The security 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 the Security Requirements Checklists exhibit for additional information.
- CIS benchmarks are available at: *https://www.cisecurity.org/cis-benchmarks/*