



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.6

NOVEMBER 8, 2023

EFFECTIVE DATE

(11-08-2023)

PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.8.6, *Information Technology (IT) Security, Application Security and Development*.

MATERIAL CHANGES

- (1) IRM updated to align with IRM 1.11.2, **Internal Management Documents System, Internal Revenue Manual (IRM) Process** Internal Controls.
- (2) The following sections were added: 10.8.6.1.3 Roles and Responsibilities, 10.8.6.1.4 Program Management and Review, 10.8.6.1.5 Program Controls, 10.8.6.1.6 Terms and Acronyms, and 10.8.6.1.7 Related Resources.
- (3) Section 10.8.6.1.1.1 (1) and (4) moved to 10.8.6.1.5 Program Controls.
- (4) Section 10.8.6.1.1.1 (2) was removed to align with the Security Policy boilerplate.
- (5) Section 10.8.6.1.1.1 (3) moved to Exhibit 10.8.6-2 Security Requirements Checklists.
- (6) Section 10.8.6.1.1.2 (1) moved to 10.8.6.1.5 Program Controls.
- (7) Section 10.8.6.1.1.2 (2) and (3) moved to 10.8.6.1.3 IT Security Controls.
- (8) Section 10.8.6.1.8 Risk Acceptance and Risk-Based Decisions moved to renumbered section 10.8.6.2.
- (9) Editorial changes (including standardization, grammar, spelling, and minor clarifications) were made throughout the IRM.

EFFECT ON OTHER DOCUMENTS

IRM 10.8.6 dated May 27, 2022, is superseded. This IRM update supersedes all prior versions of IRM 10.8.6. This IRM supplements IRM 10.8.1, *Information Technology (IT) Security Policy and Guidance* and IRM 10.8.2, *Information Technology Security Roles and Responsibilities*.

AUDIENCE

IRM 10.8.6 shall be distributed to all personnel responsible for ensuring adequate security for developing, overseeing, managing, and implementing application security for IRS information and information systems. This IRM is not intended as a primer for novice program developers/programmers. The reader is expected to be well-versed and experienced in general systems engineering, software development, and software testing practices. The reader should have a thorough understanding of technology involved in secure application development and in-depth experience with the development of software applications and web services. The Application Security and Development Policy will consist of, but will not be limited to, agency-defined

requirements, authoritative guidance, legislative mandates, and national standards. This policy applies to all employees, contractors, and vendors of the IRS.

Kaschit Pandya
Acting, Chief Information Officer

Application Security and Development

10.8.6.1 Program Scope and Objectives

[illegible]

[illegible]

[illegible]

#

10.8.6.1
(11-08-2023)
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 applications and application development within the Internal Revenue Service (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 applications and application development.
- (2) **Purpose of the program:** Development 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 manual apply to:
 - a. All offices; including business, operating, and functional units within the IRS.
 - b. IRS Personnel and organizations having contractual arrangements with the IRS, including employees, contractors, vendors and outsourcing providers who:
 - Connect to an IRS network or system and/or
 - Operate information systems that store, process, or transmit IRS information and/or
 - Leverage automated programs
- (4) **Policy Owner:** Chief Information Officer
- (5) **Program Owner:** Cybersecurity Threat Response and Remediation
- (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), Department of the Treasury Directives (TDs), National Institute of Standards and Technology (NIST) Publications, and National Archives and Records Administration (NARA).

10.8.6.1.1
(05-27-2022)
Background

- (1) This IRM establishes comprehensive Information Technology (IT) security policies and provides guidance to all IRS organizations developing or modifying applications code for use within the IRS. This IRM shall be used in conjunction with coding guidelines found in:
 - a. IRM 2.5.3, *Systems Development, Programming and Source Code Standards*
 - b. Open Web Application Security Project (OWASP) web site at https://www.owasp.org/index.php/Main_Page
- (2) IRM 10.8.6 is part of the Security, Privacy and Assurance policy family; which consists of the IRM Part 10 series for IRS Information Technology Cybersecurity.

10.8.6.1.2
(05-27-2022)
Authority

- (1) All IRS information 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), Department of the Treasury, and IRS guidelines as they apply.

10.8.6.1.3
(11-08-2023)
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.

10.8.6.1.4
(11-08-2023)
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 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.

10.8.6.1.5
(11-08-2023)
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.

10.8.6.1.6
(11-08-2023)

Terms and Acronyms

- (1) Refer to Exhibit 10.8.6-4 for a list of terms, acronyms, and definitions.

10.8.6.1.7
(11-08-2023)

Related Resources

- (1) Refer to Exhibit 10.8.6-5 for a list of related resources and references.

10.8.6.2
(11-08-2023)

Risk Acceptance and Risk-Based Decisions

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

#

#

#

#

#

#

#####

#

[illegible]

#

#

#####

#

##

#

#

#

#

#

#

#

#

[illegible]

#

#

#

##

#

[illegible]

#

#

#

[illegible]

#

[illegible]

#

##

#

[illegible]

#

#

#

##

#

#

This Page Intentionally Left Blank

#

#

#

[illegible]

#####

##

[illegible]

[illegible]

#####

[illegible][illegible]

#####

[illegible][illegible]

[illegible]

##

[illegible]

page 50 10.8 Information Technology (IT) Security

[illegible]

##

Exhibit 10.8.6-5 (05-27-2022)**Related Resources****IRS Publications**

- IRM 2.5.3 – *Systems Development, Programming and Source Code Standards.*
- IRM 10.8.1 – *Information Technology (IT) Security, Policy and Guidance.*
- IRM 10.8.2 – *Information Technology (IT) Security, IT Security Roles and Responsibilities.*
- IRM 10.8.50 – *Information Technology (IT) Security, Service-wide 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.*

Department of the Treasury Publications

- TD P 85-01, v3.1.2 *Treasury Information (IT) Security Program*, November 3, 2020

National Institute of Standards and Technology (NIST) Publications

- FIPS 140-3: *Security Requirements for Cryptographic Modules*, March 22, 2019.
- 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
- 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 800-28 Rev 2, *Guidelines on Active Content and Mobile Content*, March 2008.
- NIST SP 800-53 Rev 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020 (includes updates as of December 10, 2020).
- NIST SP 800-53A Rev 4, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations*, December 18, 2014.

Defense Information Systems Agency (DISA) Publications

- Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG): *Application Security and Development V5R1*, October 23, 2020.
- 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/>

Other Publications

- Open Web Application Security Project (OWASP):
 - OWASP Testing Guide:
https://www.owasp.org/index.php/OWASP_Testing_Project#tab=New_OWASP_Testing_Guide
 - OWASP Developer Cheat Sheets:
https://www.owasp.org/index.php/Cheat_Sheets
 - Application Security Desk Reference (ASDR): <https://www.owasp.org/index.php/ASDR>
- AJAX and other “Rich” Interface Technologies:
https://www.owasp.org/index.php/Ajax_and_Other_%22Rich%22_Interface_Technologies

Exhibit 10.8.6-5 (Cont. 1) (05-27-2022)**Related Resources**

- Information Assurance Technology Analysis Center (IATAC) Software Security Assurance State of the Art Report (SOAR) , July 31, 2007.
- Java Community of Practice SharePoint site:
<https://program.ds.irsnet.gov/sites/ADJCOP/Standards/Site%20Pages/Standards-Processes.aspx>

