



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.15

OCTOBER 19, 2023

EFFECTIVE DATE

(10-19-2023)

PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.8.15, *Information Technology (IT) Security, General Platform Operating System Security Policy*.

MATERIAL CHANGES

- (1) IRM 10.8.15.1(1)a, Program Scope and Objectives - Updated to align with Security Policy boilerplate.
- (2) IRM 10.8.15.1(5), Program Scope and Objectives - Updated to align with Security Policy boilerplate.
- (3) IRM 10.8.15.1(6), Program Scope and Objectives - Updated to align with Security Policy boilerplate.
- (4) IRM 10.8.15.1.1.1, Scope - Section removed; content relocated elsewhere in the document or removed to align with Security Policy boilerplate.
- (5) IRM 10.8.15.1.1.2, Objectives - Section removed; content relocated elsewhere in the document.
- (6) IRM 10.8.15.1.2(1), Authority - Updated to align with Security Policy boilerplate.
- (7) IRM 10.8.15.1.3, Roles and Responsibilities - Moved section from 10.8.15.2 to align with SPDER Internal Controls.
- (8) IRM 10.8.15.1.4, Program Management and Review - Section created to align with SPDER Internal Controls.
- (9) IRM 10.8.15.1.5, Program Controls - Section created to align with SPDER Internal Controls.
- (10) IRM 10.8.15.1.5(4), Program Controls - Text moved from now deleted Objectives section.
- (11) IRM 10.8.15.1.5(5), Program Controls - Text moved from now deleted Scope section.
- (12) IRM 10.8.15.1.6, Terms and Acronyms - Section created to align with SPDER Internal Controls.
- (13) IRM 10.8.15.1.7, Related Resources - Section created to align with SPDER Internal Controls.
- (14) IRM 10.8.15.2, Risk Acceptance and Risk-Based Decisions - Renumbered section from 10.8.15.1.3.
- (15) IRM 10.8.15.2(2), Risk Acceptance and Risk-Based Decisions - Updated URL to Cyber SRM RBD Application website.
- (16) IRM 10.8.15.3(3), IT Security Controls - Text moved from now deleted Scope section
- (17) IRM 10.8.15.3(4)&(5), IT Security Controls - Text moved from now deleted Objectives section.
- (18) IRM 10.8.15.3.1.3.1, Least Privilege - Web Browsers - Incorporated section from IG Memo # IT-10-1221-0014.
- (19) IRM 10.8.15.3.18.5(4), SC-8 Transmission Confidentiality and Integrity - Citation update from IG Memo # IT-10-0522-0006.
- (20) Exhibit 10.8.15-1(1), Security Requirements Checklists - Text moved from now deleted Scope section

- (21) Exhibit 10.8.15-1(2), Security Requirements Checklists - Updated URL to Security Policy SharePoint.
- (22) Exhibit 10.8.15-1(2)b, Security Requirements Checklists - Incorporated checklist topics from IG Memo # IT-10-1221-0014.
- (23) Exhibit 10.8.15-2, Terms and Acronyms - Section renamed to align with SPDER Internal Controls.
- (24) Exhibit 10.8.15-3, Related Resources - Section title updated to "Related Resources" to align with SPDER internal controls.
- (25) Exhibit 10.8.15-3, Related Resources - Updated date and version for Treasury TD P 85-01.
- (26) Exhibit 10.8.15-3, Related Resources- Updated date and version for General Purpose Operating System SRG to match currently published date and version from DISA.
- (27) Exhibit 10.8.15-3, Related Resources- Changed text "Exhibit 10.8.15-1" to "Security Requirements Checklists exhibit" in second bullet point to align with Security Policy boilerplate.
- (28) Exhibit 10.8.15-3, Related Resources - Added entry for CIS Benchmarks to align with Security Policy boilerplate.
- (29) Editorial changes made throughout the IRM for clarity. Reviewed and updated plain language, grammar, titles, website addresses, legal references and IRM references.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes the prior version of IRM 10.8.15 dated December 16, 2021. 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*. This IRM incorporates Interim Guidance Memorandum IT-10-1221-0014, Policy Updated Internal Revenue Manual (IRM) 10.8.15, Information Technology (IT), General Platform Operating System, dated 02-23-2022 and Interim Guidance Memorandum IT-10-0522-0006, SC-8 requirement citation update, dated 06-15-2022.

AUDIENCE

IRM 10.8.15 shall be distributed to all personnel responsible for securing operating systems. This policy applies to all employees, contractors, and vendors of the IRS.

Kaschit Pandya
Acting, Chief Information Officer

General Platform Operating System Security Policy

10.8.15.1 Program Scope and Objectives

[illegible]

[illegible]

#

#

#

#

#

#

#

Exhibits

#

10.8.15-2 Terms and Acronyms

#

10.8.15.1
(10-19-2023)
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 operating systems 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 operating systems.
- (2) **Purpose of the Program:** Develop and publish security 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. Individuals 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:** 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.

10.8.15.1.1
(11-27-2019)
Background

- (1) This IRM defines the security controls for the use of operating systems within the IRS.
- (2) Federal Information Processing Standards (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.
- (3) IRM 10.8.15, *Information Technology (IT) Security, General Platform Operating System Security Policy* provides policy and guidance to be used by the IRS to carry out their representative responsibilities in information systems security regarding workstations and servers.
- (4) IRM 10.8.15 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Information Technology Cybersecurity.

10.8.15.1.2
(10-19-2023)
Authority

- (1) All IRS information systems and applications shall be compliant with Executive Orders (EOs), 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.

10.8.15.1.3
(10-19-2023)
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.

10.8.15.1.4
(10-19-2023)
**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.

10.8.15.1.5
(10-19-2023)
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. 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 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 all IRS operating systems 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.

10.8.15.1.6
(10-19-2023)

- (1) Refer to Exhibit 10.8.15-2 for a list of terms, acronyms, and definitions.

Terms and Acronyms

10.8.15.1.7
(10-19-2023)

- (1) Refer to Exhibit 10.8.15-3 for a list of related resources and references.

Related Resources

10.8.15.2
(10-19-2023)

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

Risk Acceptance and Risk-Based Decisions

#

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

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

page 6

10.8 Information Technology (IT) Security

##

#

##

[illegible]

##

##

##

#

[illegible]

#

[illegible]

[illegible]

#

#

##

#####

#

#

This Page Intentionally Left Blank

[illegible]

Exhibit 10.8.15-2 (10-19-2023)**Terms and Acronyms****A**

Access Control - Process of granting access to information system resources only to authorized users, programs, processes, or other systems.

Active Directory (AD) - A directory service implemented by Microsoft for Windows domain networks. It is included in most Windows Server operating systems and runs as a Windows service. An AD domain controller authenticates and authorizes all users and computers in a Windows domain type network-assigning and enforcing security policies for all computers and installing or updating software.

Assessment, Authorization, and Monitoring – (Formerly known as Security Assessment & Authorization (SA&A)) – Assessment, Authorization, and Monitoring (AA&M) is a testing and evaluation process with a resulting authorization based on the NIST Special Publication 800-series; specifically, SP 800-37 and SP 800-53. The new AA&M process and terminology replaces the Security Assessment & Authorization process, which were based on earlier NIST SP 800 guidance.

Authorizing Official (AO) - Official with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals. Accountable for the security risks associated with information system operations. Previously known as the Designated Approving Authority.

Authentication - Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's identity.

B

BEARS – Business Entitlement Access Request System

C

Center for Internet Security (CIS) - A 501c3 nonprofit organization focused on enhancing the cybersecurity readiness and response of public and private sector entities, with a commitment to excellence through collaboration. CIS provides resources that help partners achieve security goals through expert guidance and cost-effective solutions.

Certification - A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of the security authorization process, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Security control assessment is included within the certification process.

Chief Information Officer (CIO)/Chief Technology Officer (CTO) - Refer to IRM 10.8.2 for a detailed description of responsibilities.

Configuration Management (CM) - A systems engineering process for establishing and maintaining consistency of a product's performance, functional and physical attributes with its requirements, design and operational information throughout its life.

Contingency Planning (CP) - A plan designed to take a possible future event or circumstance into account.

CPU – Central Processing Unit

Exhibit 10.8.15-2 (Cont. 1) (10-19-2023)**Terms and Acronyms****D**

Defense Information Systems Agency (DISA) - A U.S. combat support agency that connects the U.S. military and government through IT and communications support. Originally known as the Defense Communications Agency (DCA).

Denial of Service (DoS) – A cyber-attack where the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

Department of Defense (DoD) - The executive department of the government of the United States charged with coordinating and supervising all agencies and functions of the government concerned directly with national security and the United States Armed Forces.

Department of Homeland Security (DHS) - A cabinet department of the United States federal government, with the primary responsibilities of protecting the United States and its territories (including protectorates) from and responding to terrorist attacks, man-made accidents, and natural disasters.

Dual Authorization – In the absence of an automatic process, a rule that requires the approval of two, (dual) authorized individuals to execute a task.

E

EA – Enterprise Architecture

ESP – Enterprise Standards Profile

F

FIPS – Federal Information Processing Standards

Fire Call Account – Local site accounts for emergency or special issues used by Enterprise Operations (EOPs) or other approved organizations.

FISMA – Federal Information Security Management Act

G

GMT - Greenwich Mean Time

H

Host – Any computer that has full two-way access to other computers on the Internet.

Host Server – The physical machine that uses a hypervisor to manage the virtual machine(s).

HTTP - Hypertext Transfer Protocol

Hypervisor – The virtualization component that manages the guest OS on a host and controls the flow of instructions between the guest OS and the physical hardware. Also described as software that allows a single host to run one or more guest operating systems. The hypervisor is basically a high-speed scheduler that issues out the physical resources such as CPU, disk space and RAM to the guest operating systems, (virtual machines). Can be referred to as a virtual machine manager.

Exhibit 10.8.15-2 (Cont. 2) (10-19-2023)**Terms and Acronyms****I**

Information System Contingency Plan (ISCP) - Established procedures created and maintained by IRS Information Technology organization and system owners for the assessment and recovery of a system following a system disruption. The ISCP provides key information needed for system recovery, including roles and responsibilities, inventory information, assessment procedures, detailed recovery procedures, and testing of a system. The ISCP differs from DR plan primarily in that the information system contingency plan procedures are developed for recovery of the system regardless of site or location. An ISCP can be activated at the system's current location or at an alternate site. In contrast, a DR plan is primarily a site-specific plan developed with procedures to move operations of one or more information systems from a damaged or uninhabitable location to a temporary alternate location. Once the DR plan has successfully transferred an information system site would then use its respective ISCO to restore, recover, and test systems, and put them in operation.

Information Technology (IT) – IT is defined as any service or equipment or the personnel that support any part of the lifecycle of those services or equipment, or interconnected system(s) or subsystem(s) of equipment, that are used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the agency.

1. For purposes of this definition, equipment is used by an agency if the equipment is used by the agency directly or issued by a contractor under a contract with the agency that require –
 - a. Its use; or
 - b. To a significant extent, its use in the performance of a service or the furnishing of a product
2. The term “*information technology*” includes computers, ancillary equipment (including imaging peripherals, input, output, and storage devices necessary for security and surveillance), peripheral equipment designed to be controlled by the central processing unit of a computer, software, firmware and similar procedures, services (including support services and cloud computing), and related resources.
 - a. Is acquired by a contractor incidental to a contract, or
 - b. Contains imbedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. For example, HVAC (heating, ventilation, and air conditioning) equipment, such as electronic thermostats or temperature control devices, and medical equipment where information technology is integral to its operation, is not information technology.

Information Technology Contingency Plan (ITCP) - Support plans designed to ensure continuity of general support systems and major systems following a disruption.

Internet Protocol (IP) -The principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries.

Internet Protocol Security (IPSec) - A protocol suite for securing Internet Protocol communications by authenticating and encrypting each IP packet of a communication session.

IRM – Internal Revenue Manual

ISSO – Information System Security Officer

L

LAN- Local Area Network

Exhibit 10.8.15-2 (Cont. 3) (10-19-2023)

Terms and Acronyms

N

NIST – National Institute of Standards and Technology

NSA – National Security Agency

O

OMB – Office of Management and Budget

OS – Operating System

P

PDS – Protected Distribution System

Permissions – The access controls of a file or directory in the form of read, write, and execute for each of the three groups; file owner, same group member, and everyone else.

PKI – Public Key Infrastructure

R

Risk Based Decision (RBD) – Decision made by individuals responsible for ensuring security by utilizing a wide variety of information, analysis, assessment, and processes. The type of information taken into account 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.)

S

Security Risk Management (SRM) - The management of security risks applies the principles of risk management to the management of security threats. It consists of identifying threats (or risk causes), assessing the effectiveness of existing controls to face those threats, determining the risks' consequence(s), prioritizing the risks by rating the likelihood and impact, classifying the type of risk, and selecting an appropriate risk option or risk response.

Security Technical Implementation Guide (STIG) - A methodology for standardized secure installation and maintenance of computer software and hardware. The term was coined by DISA which creates configuration documents in support of the United States Department of Defense (DoD). The implementation guidelines include recommended administrative processes and span the devices' lifecycle.

Sensitive But Unclassified (SBU) Information - Any information that requires protection due to the risk and magnitude of loss or harm to the IRS or the privacy to which individuals are entitled under 5 U.S.C. § 552a (the Privacy Act), which could result from inadvertent or deliberate disclosure, alteration, or destruction.

SP – Special Publication

SRG – Security Requirements Guide

Standard Operating Procedure (SOP) – A set of step-by-step instructions compiled by an organization to help workers carry out routine operations. SOPs aim to achieve efficiency, quality output and uniformity of performance, while reducing miscommunication and failure to comply with industry regulations.

Exhibit 10.8.15-2 (Cont. 4) (10-19-2023)**Terms and Acronyms**

STIG – Security Technical Implementation Guide. A cybersecurity methodology for standardizing security protocols within networks, servers, computers, and logical designs to enhance overall security.

System Administrator (SA) – A person who manages the technical aspects of a system. Refer to IRM 10.8.2, **Information Technology (IT) Security, Roles and Responsibilities**, for details.

T

Treasury Directive (TD) - Documents signed by the appropriate senior Treasury officials that: may further delegate authority from the most senior officials to other Treasury officials; and provide processes for implementing legal obligations and Departmental policy objectives.

U

UTC – Universal Time Coordinate

V

Virtualization – The simulation of the software and/or hardware upon which other software runs by creating an abstracted layer from the actual hardware creating a unique instance of a physical system, but running independently in software or “virtual” state.

#

