



# MANUAL TRANSMITTAL

Department of the Treasury  
Internal Revenue Service

10.8.12

FEBRUARY 16, 2024

## EFFECTIVE DATE

(02-16-2024)

## PURPOSE

- (1) This transmits the new Internal Revenue Manual (IRM) 10.8.12, *Information Technology (IT) Security, Container Platform Security Policy*.

## MATERIAL CHANGES

- (1) This is a new security policy to the 10.8.x series to introduce software container platform security to the IRS.
- (2) This security policy incorporates guidance on software container platform from IRM 10.8.15, *Information Technology (IT) Security, General Purpose Operating System Security Policy*, dated October 19, 2023.

## EFFECT ON OTHER DOCUMENTS

Software Container Platform related guidance will be removed from IRM 10.8.15, *Information Technology (IT), General Purpose Operating System Security Policy*. Checklists related to such guidance will now be found this IRM. This IRM supplements IRM 10.8.1, *Information Technology (IT) Security Policy and Guidance* and IRM 10.8.2, *Information Technology (IT), IT Security Roles and Responsibilities*.

## AUDIENCE

IRM 10.8.12 shall be distributed to all personnel responsible for overseeing, managing, and implementing software containers.

Rajiv Uppal  
Chief Information Officer



# Container Platform Security Policy

#### 10.8.12.1 Program Scope and Objectives

[illegible]

[illegible]

---

Exhibits

10.8.12-2 Terms and Acronyms

#  
#  
#  
#  
#  
#  
  
#  
  
#



10.8.12.1  
(02-16-2024)  
**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 software container platforms within the 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 related to IRS software container platforms.
- (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 policy apply to:
  - a. All offices and 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, 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.

10.8.12.1.1  
(02-16-2024)  
**Background**

- (1) This IRM defines the security controls for the use of container platforms within the IRS.
- (2) IRM 10.8.12 is part of the Security, Privacy, and Assurance policy family, IRM Part 10 series for IRS Information Technology Cybersecurity.

10.8.12.1.2  
(02-16-2024)  
**Authority**

- (1) All IRS 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.

10.8.12.1.3  
(02-16-2024)  
**Roles and Responsibilities**

- (1) IRM 10.8.2, *Information Technology (IT), 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.

10.8.12.1.4  
(02-16-2024)  
**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, OMB guidance, Treasury Directives (TDs), NIST Publications, 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 (ECL), Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve IRS IT process and service efficiency and effectiveness.

10.8.12.1.5  
(02-16-2024)

#### Program Controls

- (1) Each IRM in the 10.8.x series is assigned an author who reviews the 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 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 (CNSI)*, for additional guidance for protecting classified information.
- (4) This IRM establishes the minimum baseline security policy and requirements for all IRS Container Platforms 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.

10.8.12.1.6  
(02-16-2024)

#### Terms and Acronyms

- (1) Refer to Exhibit 10.8.12-2 for Terms and Acronyms.

(1) Refer to Exhibit # 10.8.12-3 # for Related Resources.

- (1) Any exception to this policy requires 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 within the Risk Based Decision Standard Operating Procedures (SOP).

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

- (1) The security controls in this IRM supplement the requirements found in IRM 10.8.1.
  - a. Refer to IRM 10.8.1 for security control families and security controls not addressed within this IRM.
- (2) It is acceptable to configure settings to be more restrictive than those defined in this IRM.
- (3) To configure less restrictive requirements requires a risk-based decision. Refer to the Risk Acceptance and Risk-Based Decisions subsection within this IRM for additional guidance.

##  
##  
##  
##

##  
##  
##

#####

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

[illegible]

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

[illegible]

#

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

[illegible]

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

#####

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

#

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

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

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

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

[illegible]

#####

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

[illegible]

##  
##  
##  
##  
##

##  
##  
##  
##

[illegible]

##  
##  
##

##

##  
##  
##

#  
#

##  
##  
##  
##

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

#  
#  
#  
#

**This Page Intentionally Left Blank**

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

**Exhibit 10.8.12-2 (02-16-2024)****Terms and Acronyms**

Term	Definition or Description
Access Control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems.
Application virtualization	A form of virtualization that exposes a single shared operating system kernel to multiple discrete application instances, each of which is kept isolated from all others on the host.
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.
Base layer	The underlying layer of an image upon which all other components are added.
BEARS	Business Entitlement Access Request System
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.

**Exhibit 10.8.12-2 (Cont. 1) (02-16-2024)**  
**Terms and Acronyms**

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.
Certification and Accreditation (C&A)	See Certification or Security Assessment & Authorization.
Chief Information Officer (CIO)	See IRM 10.8.2 for a detailed description of responsibilities.
Computer Security Incident Response Center (CSIRC)	See IRM 10.8.2 for a detailed description of responsibilities.
Container	See Software Container.
Container runtime	The environment for each container; comprised of binaries coordinating multiple operating system components that isolate resources and resource usage for running containers.
Container-specific operating system	A minimalistic host operating system explicitly designed to only run containers.
Contingency Planning (CP)	A plan designed to take a possible future event or circumstance into account.
CPU	Central Processing Unit
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.

**Exhibit 10.8.12-2 (Cont. 2) (02-16-2024)****Terms and Acronyms**

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 require the approval of two, (dual) authorized individuals to execute a task.
EA	Enterprise Architecture
ESP	Enterprise Standards Profile
Filesystem virtualization	A form of virtualization that allows multiple containers to share the same physical storage without the ability to access or alter the storage of other containers.
FIPS	Federal Information Processing Standards
Fire Call Account	Local site accounts for emergency or special issues used by Enterprise Operations (EOPs) or other approved IRS personnel.
FISMA	Federal Information Security Management Act
General-purpose operating system	A host operating system that can be used to run many kinds of applications, not just applications in containers.
GMT	Greenwich Mean Time

## Exhibit 10.8.12-2 (Cont. 3) (02-16-2024)

## Terms and Acronyms

High Value Asset (HVA)	<p>Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States's national security interests, foreign relations, economy, or the public confidence, civil liberties, or public health and safety of the American people. HVA can fall into one of three categories:</p> <ul style="list-style-type: none"><li>• Informational Value - The information or information system that processes, stores, or transmits the information is of high value to the Government or its adversaries.</li><li>• Mission Essential – The agency that owns the information or information system cannot accomplish its Primary Mission Essential Functions (PMEF), as approved in accordance with Presidential Policy Directive 40 (PPD-40) National Continuity Policy, within expected timelines without the information or information system.</li><li>• Federal Civilian Enterprise Essential (FCEE) – The information or information system serves a critical function in maintaining the security and resilience of the federal civilian enterprise.</li></ul>
Host	Any computer that has full two-way access to other computers on the Internet.
Host operating system	The operating system kernel shared by multiple applications within an application virtualization architecture.
HTTP	Hypertext Transfer Protocol
IAVM	Information Assurance Vulnerability Management
Image	A package that contains all the files required to run a container.

Exhibit 10.8.12-2 (Cont. 4) (02-16-2024)

Terms and Acronyms

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.
--	--

**Exhibit 10.8.12-2 (Cont. 5) (02-16-2024)**  
**Terms and Acronyms**

Information Technology (IT)	<p>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.</p> <ol style="list-style-type: none"> <li>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 – <ol style="list-style-type: none"> <li>a. Its use; or</li> <li>b. To a significant extent, its use in the performance of a service or the furnishing of a product.</li> </ol> </li> <li>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.</li> <li>3. The term “information technology” does not include any equipment that – <ol style="list-style-type: none"> <li>a. Is acquired by a contractor incidental to a contract, or</li> <li>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.</li> </ol> </li> </ol>
-----------------------------	---

**Exhibit 10.8.12-2 (Cont. 6) (02-16-2024)****Terms and Acronyms**

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
Isolation	The ability to keep multiple instances of software separated so that each instance only sees and can affect itself.
ISSO	Information System Security Officer
Kubernetes	An open-source container-orchestration tool used for bundling and managing clusters of containerized applications.
LAN	Local Area Network
Microservice	A set of containers that work together to compose an application.
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
Operating system virtualization	A virtual implementation of the operating system interface that can be used to run applications written for the same operating system.
Orchestration	Bundling and managing clusters of containerized applications
Orchestrator	A tool that enables DevOps personas or automation working on their behalf to pull images from registries, deploy those images into containers, and manage the running containers. Orchestrators are also responsible for monitoring container resource consumption, job execution, and machine health across hosts.
OS	Operating 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

**Exhibit 10.8.12-2 (Cont. 7) (02-16-2024)****Terms and Acronyms**

Platform as a Service (PaaS)	The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.
Registry	A service that allows developers to easily store images as they are created, tag and catalog images for identification and version control to aid in discovery and reuse and find and download images that others have created.
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 considered 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 considered 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.)
Secure Socket Layer (SSL)	Provides privacy and data integrity between two communicating applications. It is designed to encapsulate other protocols, such as HTTP.
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.

**Exhibit 10.8.12-2 (Cont. 8) (02-16-2024)****Terms and Acronyms**

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
Software as a Service (SaaS)	The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
Software Container	A method for packaging and securely running an application within an application virtualization environment. Also known as an application container or a server application container.
SRG	Security Requirements Guide
SRM	Security Risk Management
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.
STIG	Security Technical Implementation Guide
System Administrator (SA)	A person who manages the technical aspects of a system. Refer to IRM 10.8.2, <i>Information Technology (IT) Security, Roles and Responsibilities</i> , for details.
Transport Layer Security (TLS)	Provides privacy and data integrity between two communicating applications. It is designed to encapsulate other protocols, such as HTTP.
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.

**Exhibit 10.8.12-2 (Cont. 9) (02-16-2024)**
**Terms and Acronyms**

UTC	Universal Time Coordinate
Virtual machine	A simulated environment created by virtualization.
Virtualization	The simulation of the software and/or hardware upon which other software runs.

#####