



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.11

SEPTEMBER 19, 2024

EFFECTIVE DATE

(09-19-2024)

PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.8.11, *Information Technology (IT) Security, Application Security Policy*. The purpose of this IRM is to provide guidance and establish requirements necessary to implement and manage IT security for applications within the IRS.

MATERIAL CHANGES

- (1) Updated the Chief Information Officer.
- (2) Removed Scope 10.8.11.1.1 and Objectives 10.8.11.1.1.2.
- (3) IRM 10.8.11.1.4, Program Management and Review - Updated to align with IRM 1.11.2 requirements.
- (4) IRM 10.8.11.1.5, Program Control - Updated to align with IRM 1.11.2 requirements.
- (5) IRM 10.8.11.2, IT Security Controls - Replaced the word shall with must throughout the IRM to align with IRM 1.11.2.
- (6) IRM 10.8.11.2, IT Security Controls - Updated control identifiers throughout the IRM to add leading zeros to align with NIST SP 800-53 Rev 5.1.1 (e.g., instead of AC-1, the control identifier is now AC-01).
- (7) IRM 10.8.11.2, IT Security Controls - Removed the control identifier for all of the -1 controls throughout the IRM to align with NIST SP 800-53 Rev 5.
- (8) Editorial changes made throughout the IRM for clarity and alignment with Security Policy Boilerplate 2 July 2024. Reviewed and updated plain language, grammar, titles, website addresses, legal references and IRM references.

EFFECT ON OTHER DOCUMENTS

This IRM supplements 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 IRM 10.8.11, dated November 3, 2023 is superseded.

AUDIENCE

IRM 10.8.11 must be distributed to all personnel responsible for overseeing, managing, and implementing application security for IRS information and information systems. The Application Security Policy IRM 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.

Rajiv Uppal
Chief Information Officer

Application Security Policy

10.8.11.1 Program Scope and Objectives

- [illegible]

[illegible]

[illegible]

#

#

#

10.8.11.1
(09-19-2024)
Program Scope and Objectives

- (1) **Overview:** This IRM lays the foundation to implement and manage security controls and guidance for the use of applications 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 relate to IRS applications.
- (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, that 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, Cybersecurity Threat Response and Remediation
- (6) **Program Goals:** To protect the confidentiality, integrity, and availability of IRS information and information systems.

10.8.11.1.1
(09-19-2024)
Background

- (1) IRM 10.8.11 defines security controls for application programs. An application is a software program that is hosted by an information system and is designed to perform a specific function directly for the user or, in some cases, for another application. Application programs can be executed without access to system control, monitoring, or administrative privileges.
- (2) IRM 10.8.11 is part of the Security, Privacy, and Assurance policy family, IRM Part 10 Series for IRS IT Cybersecurity.

10.8.11.1.2
(09-19-2024)
Authority

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

10.8.11.1.3
(09-19-2024)
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 system security, and is the authoritative source for such information.

10.8.11.1.4
(09-19-2024)
**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 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 its organizations. This policy provides uniform policies and guidance to be used by each organization.
 - 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, National Archives and Records Administration (NARA) guidance, other regulatory guidance, and best practice methodologies.
 - d. Use best practices methodologies (such as Capability Maturity Model Integration (CMMI), enterprise lifecycle (ELC), Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve IRS IT process and service efficiency and effectiveness.

10.8.11.1.5
(09-19-2024)
Program Control

- (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, DISA) for potential revisions to security policies and security requirements 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 weekly report identifying security policies and security requirements 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 applications IT assets 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.

Note: IRM 10.8.1 applies to on-premises systems, including on-premises cloud models. For off-premises cloud models, refer to IRM 10.8.24, Information Technology (IT) Security, Cloud Computing Security Policy.

- #### 10.8.11.2.1

#

[illegible]

#

[illegible]

#

#

[illegible]

#

#

##

#

#

```
# #  
# #  
# #  
# #  
# #  
# #  
# #  
# #  
# #  
# #  
# #  
  
# #  
# #  
# #  
  
# #  
# #  
# #  
# #  
# #  
  
# #  
# #  
# #  
# #  
# #
```


#

[illegible]

#

#

#

#

#

#

#

#

#

[illegible]

#

#

#

This Page Intentionally Left Blank

#

Exhibit 10.8.11-2 (09-19-2024)**Terms and Acronyms**

Term	Definition or Description
Application	An application is a software program hosted by an information system that is designed to perform a specific function directly for users/applications and can be executed without access to system control, monitoring, or administrative privileges.
AO	Authorizing Official
Contractor	Contractors are individuals or other legal entities that are, directly or indirectly, awarded government contracts. Contractors conduct business, or reasonably may be expected to conduct business, with the Government as an agent or representative of another contractor.
CIS	Center for Internet Security
CISA	Cybersecurity Infrastructure Security Agency
CNSI	Classified National Security Information
Cybersecurity	Cybersecurity is the ability to protect or defend the use of cyberspace from cyber attacks.
DAC	Discretionary access control is a means of restricting access to objects (e.g., files, data entities) based on the identity and need-to-know of subjects (e.g., users, processes) and/or groups to which the object belongs. The controls are discretionary in the sense that a subject with certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject (unless restrained by mandatory access control).
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
DoS	The prevention of authorized access to resources or the delaying of time-critical operations. (Time-critical may be milliseconds or it may be hours, depending upon the service provided).
EA	Enterprise Architecture
EFC	Enterprise FISMA Compliance
EO	Executive Order
ESP	Enterprise Standards Profile
FIPS	Federal Information Processing Standards (FIPS) are publicly announced standards developed by the National Institute of Standards and Technology for use in computer systems by non-military American government agencies and government contractors.

Exhibit 10.8.11-2 (Cont. 1) (09-19-2024)**Terms and Acronyms**

Term	Definition or Description
FISMA	The Federal Information Security Modernization [FISMA] of 2014 requires federal agencies to identify and provide information security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of an agency; or information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency.
Honeypot	Honeypot is a name given to a system (e.g., a web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders and has no authorized users other than its administrators.
IDS	Intrusion detection system is a hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations.)
IP	Internet protocol is a standard protocol for transmission of data from source to destinations in packet-switched communications networks and interconnected systems of such networks.
IPSEC	IP Security (IPSec) is a suite of protocols for securing Internet Protocol (IP) communications at the network layer, layer 3 of the OSI model by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for cryptographic key establishment.
IRM	Internal Revenue Manual
ISSO	Information System Security Officer
NARA	National Archives and Records Administration
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OMB	Office of Management and Budget
Outsourcing Provider	An outsourcing provider is a provider of external information system services to an organization through a variety of consumer-producer relationships including but not limited to: joint ventures; business partnerships; outsourcing arrangements (i.e., through contracts, interagency agreements, lines of business arrangements); licensing agreements; and/or supply chain exchanges. (NIST SP 800-161 from NIST SP 800-53 Rev. 5)
PKI	Public key infrastructure (PKI) is 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. Class 3 PKI certificates are used for servers and software signing rather than for identifying individuals. Class 4 certificates are used for business-to-business transactions.

Exhibit 10.8.11-2 (Cont. 2) (09-19-2024)**Terms and Acronyms**

Term	Definition or Description
RBD	Risk-based decision (RBD) is a 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).
SA	System Administrator
SOA	Service Oriented Architecture
SOP	Standard Operating Procedures
SP	Special Publications
SRG	Security Requirements Guide
SRM	Security Risk Management
SSL	Secure socket layer (SSL) is a protocol used for protecting private information during transmission via the Internet. Note: SSL works by using a public key to encrypt data that's transferred over the SSL connection. Most web browsers support SSL, and many web sites use the protocol to obtain confidential user information, such as credit card numbers. By convention, URLs that require an SSL connection start with "https:" instead of "http:".
SSP	System Security Plan
STIG	Security Technical Implementation Guide
TCP	Transmission Control Protocol (TCP) is a standard that defines how to establish and maintain a network conversation via which application programs can exchange data. TCP works with the Internet Protocol (IP), which defines how computers send packets of data to each other.
TD	Treasury Directive
TLS	TransportLayer Security is an authentication and security protocol widely implemented in browsers and web servers.
URL	A uniform resource locator (URL) , previously universal resource locator) - usually pronounced by sounding out each letter, but sometimes pronounced "earl," is the unique address for a file that is accessible on the Internet. A common way to get to a Web site is to enter the URL of its home page file in your web browser's address line. However, any file within that web site can also be specified with a URL. Such a file might be any web (HTML) page other than the home page, an image file, or a program such as a common gateway interface application or Java applet. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

Exhibit 10.8.11-2 (Cont. 3) (09-19-2024)**Terms and Acronyms**

Term	Definition or Description
Vendor	Vendors are commercial suppliers of software or hardware (NISTIR 4734). More specifically, vendors create or manufacture products for government organizations or contractors.
VPN	Virtual private network is a virtual network, built on top of existing physical networks, that provides a secure communications tunnel for data and other information transmitted between networks.
Web Service	A web service is a software system that supports interoperable machine-to-machine interaction over a network and fulfills a specific task or a set of tasks. It has an interface described in a machine - processable format (specifically, web service definition language, or WSDL). A web service is described using a standard, formal XML notion, called its service description, that provides all details necessary to interact with the service, including message formats (that detail the operations), transport protocols, and location.

#