



MANUAL TRANSMITTAL

Department of the Treasury
Internal Revenue Service

10.8.55

NOVEMBER 3, 2023

EFFECTIVE DATE

(11-03-2023)

PURPOSE

- (1) This transmits revised Internal Revenue Manual (IRM) 10.8.55, *Information Technology (IT) Security, Network Security Policy*.

MATERIAL CHANGES

- (1) The following sections have been added, updated, and removed from this version of the IRM:
 - a. Added the following sections:
 - IRM updated to align with IRM 1.11.2, Internal Management Documents System, Internal Revenue Manual (IRM) Process Internal Controls
 - added - 10.8.55.1.3 Roles and Responsibilities.
 - added - 10.8.55.1.4 Program Management and Review.
 - added - 10.8.55.1.5 Program Controls.
 - added - 10.8.55.1.6 Terms and Acronyms.
 - added - 10.8.55.1.7 Related Resources.
 - b. Modified the following sections:
 - Effects on Other Documents.
 - Exhibit 10.8.55-2 renamed Terms and Acronyms.
 - Exhibit 10.8.55-3 renamed Related Resources.
 - 10.8.55.1.3 Roles and Responsibilities moved from 10.8.55.3
 - 10.8.55.1.8 Risk Acceptance and Risk-Based Decisions moved to 10.8.55.2
 - moved #10.8.55.3.1 Computer Security Incident Response Center (CSIRC)# from 10.8.55.4.1
 - moved #10.8.55.3.2 User and Network Services (UNS)# from 10.8.55.4.2
 - moved #10.8.55.3.2.1 Network Security Management Standard# from 10.8.55.42.1
- (2) This IRM supplements IRM 10.8.1, *Information Technology (IT) Security Policy and Guidance*.
- (3) Exhibit sections have been updated, including Terms and Acronyms.
- (4) Editorial changes (including grammar, spelling, and minor clarification) were made throughout this IRM.

EFFECT ON OTHER DOCUMENTS

IRM 10.8.55 dated May 04, 2022 is superseded. This IRM supersedes all prior versions of IRM 10.8.55. Additionally, This IRM supplements IRM 10.8.1, *Information Technology (IT) Security, Policy and Guidance* and IRM 10.8.54, *Information Technology (IT) Security, Minimum Firewall Administration Requirements*.

AUDIENCE

IRM 10.8.55 shall be distributed to all personnel responsible for ensuring that adequate security is provided for IRS information and information systems. This policy applies to all employees, contractors, and vendors of the IRS.

Kaschit Pandya
Acting, Chief Information Officer

10.8.55

Network Security Policy

Table of Contents

10.8.55.1 Program Scope and Objectives

10.8.55.1.1 Background

10.8.55.1.1.1 Scope

10.8.55.1.1.2 Objectives

10.8.55.1.2 Authority

10.8.55.1.3 Roles and Responsibilities

10.8.55.1.4 Program Management and Review

10.8.55.1.5 Program Controls

10.8.55.1.6 Terms and Acronyms

10.8.55.1.7 Related Resources

10.8.55.2 Risk Acceptance and Risk-Based Decisions

#

#

#

10.8.55.4 IT Security Controls

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

[illegible]

Exhibits

#

10.8.55-2 Terms and Acronyms

10.8.55-3 Related Resources

10.8.55.1
(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 network devices 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 network security.
- (2) **Purpose of the program:** Develop and publish policies to protect the IRS IT infrastructure 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 and business, 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.

10.8.55.1.1
(05-04-2022)
Background

- (1) This IRM establishes a comprehensive policy to implement the minimum security controls to safeguard network devices within the IRS organization.
- (2) IRM 10.8.55 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Information Technology Cybersecurity.
- (3) Federal Information Processing Standards (FIPS) 200 mandates the use of the NIST Special Publication (SP) 800-53 as the baseline for the creation of agency IT security policy.
- (4) This IRM is based on:
 - a. Guidance provided in the NIST SP 800-53, Rev 5, Security and Privacy Controls for Federal Information Systems and Organizations.
 - b. Requirements from the Defense Information Systems Agency (DISA) Network Security Requirement Guides (SRGs).
 - c. Industry best practices.

10.8.55.1.1.1
(11-03-2023)
Scope

- (1) This IRM applies to all IRS information and information systems, which include IRS production, development, test, and contractor systems. For information systems that store, process, or transmit classified national security information, please refer to IRM 10.9.1 *Classified National Security Information (NSI)*, for additional guidance for classified information.
- (2) This IRM covers the minimum-Security controls and guidance for safeguarding network devices within the IRS.
- (3) Security Requirements Checklists:

- a. Security Requirements Checklists (if accompanying this IRM) serve as the secure configuration baseline and are developed in accordance with NIST SP 800-70, *National Checklist Program for IT Products: Guidelines for Checklist Users and Developers*.
- b. IRMs with accompanying checklists contain a checklist with general security requirements (e.g., Defense information Systems Agency (DISA) Security Requirements Guide (SRG), as well as checklists with platform or technology specific requirements (e.g., Security Implementation Guides (STIGs), Center for Internet Security (CIS) Benchmarks). In the event a platform or technology specific checklist is not available, the general security requirements checklists shall be used (e.g., Database (General), Operating Systems (General), Router (General)).
- c. Security Requirement Checklists shall be used in addition to the requirements within the IRM body. This allows for IRS and Treasury defined requirements contained within the IRM body to be captured in the secure configuration baseline.
- d. In the event of a conflict between a checklist and the IRM body, the requirement(s) from the checklist shall be used.

Note: The order of precedence only applies when there is a conflict between the IRM body and one of its accompanying checklists, and does not apply when there is a discrepancy with IRM 10.8.1.

- e. Implementation of Security Requirement Checklists is required (CM-6).
 - f. Refer to the Security Requirements Checklist exhibit for additional guidance.
- (4) 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 or otherwise noted.

10.8.55.1.1.2
(11-03-2023)
Objectives

- (1) The IRM establishes the minimum baseline security policy and requirements for all IRS network and network related assets 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.
- (2) It is acceptable to configure settings to be more restrictive than those defined in this IRM.
- (3) To configure less restrictive requirements, a risk-based decision is required. Refer to the Risk Acceptance and Risk-Based Decisions section within this IRM for additional guidance.

10.8.55.1.2
(05-04-2022)
Authority

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

10.8.55.1.3
(11-03-2023)
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 information system security, and is the authoritative source for such information.
- (2) The supplemental roles and responsibilities provided below are specific to the implementation of security patch management.

10.8.55.1.4
(11-03-2023)
Program Management and Review

- (1) The IRS Cybersecurity 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.

10.8.55.1.5
(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. 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.

10.8.55.1.6
(11-03-2023)
Terms and Acronyms

- (1) Refer to Exhibit 10.8.50-4 for a list of terms, acronyms, and definitions

10.8.55.1.7
(11-03-2023)
Related Resources

- (1) Refer to Exhibit 10.8.50-5 for a list of related resources and references

10.8.55.2
(11-03-2023)
Risk Acceptance and Risk-Based Decisions

- (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 about risk acceptance and risk-based decision.

#

10.8.55.3
(05-04-2022)

#

10.8.55.4
(05-04-2022)
IT Security Controls

- (1) The security controls within this IRM supplement the requirements defined in IRM 10.8.1.
- (2) Refer to IRM 10.8.1 for security control families not addressed within this IRM.
- (3) There may, on occasion, be redundancy in requirements that appear in the security controls within this IRM and potentially other subordinate IRMs. This overlap in requirements is intended to reinforce the security requirements from the perspective of multiple controls and/or enhancements.

- ##

##

[illegible]

#

#

#

#

#

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

#

#

#

#

##

#

#

#

[illegible]

[illegible]

[illegible]

[illegible]

#

#

#

[illegible]

[illegible]

Exhibit 10.8.55-2 (11-03-2023)**Terms and Acronyms****A**

Access Control - The process of granting or denying specific requests:

- 1) For obtaining and using information and related information processing services.
- 2) To enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).

AES- Advanced Encryption Standard

AS - Autonomous System

Asset - A major application, general support system, high impact program, physical plant, mission critical system, personnel, equipment, or a logically related group of systems.

Audit - An independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit Trail - A chronological record of system activities that is sufficient to enable the reconstruction, review, and examination of each event in a transaction from inception to output of final results.

Authentication - The act of identifying or verifying the eligibility of a station, originator, or individual to access specific categories of information. Typically, a measure designed to protect against fraudulent transmissions by establishing the validity of a transmission, message, station, or originator. The process of identifying an individual is usually based on a username and password, but can also be done through other means, such as tokens, access cards, and biometrics. Authentication ensures that the individual is who he or she claims to be, but says nothing about the access rights of the individual.

Authenticator - The means used to confirm the identity of a user, processor, or device (e.g., user password, token, PKI certificate, biometric, or key card).

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.

Authorized User Any appropriately cleared individual with a requirement to access a IRS information system in order to perform or assist in a lawful and authorized governmental function.

Availability - The ability to access information system resources in a timely manner as required by an authorized user; one of the fundamental components of information security.

Awareness - Activities which seek to focus attention on information security or set of issues. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. Awareness relies on reaching broad audiences with attractive packaging techniques.

B

BGP - Border Gateway Protocol

Exhibit 10.8.55-2 (Cont. 1) (11-03-2023)**Terms and Acronyms**

Bogon/Martian - A bogon route or martian address is a type of packet that should never be routed inbound through the perimeter device. Bogon routes and martian addresses are commonly found as the source addresses of DDoS attacks. By not having a policy implemented to keep these addresses up to date, the network will run the risk of allowing illegitimate traffic into the network or even blocking legitimate traffic. Also, if there are rulesets with "any" as the source address then Bogons/Martians must be applied.

Bridge Protocol Data Unit (BPDU) – Frames that contain information about the spanning tree protocol. A switch sends BPDUs using a unique source MAC address from its origin port to a multicast address with destination MAC

C

CCMP- Counter Mode with Cipher Block Chaining Message Authentication Protocol

CD - Compact disc

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 certification.

Channel Service Unit/Data Service Unit (CSU/DSU) - A hardware device about the size of an external modem that converts a digital data frame from the communications technology used on a LAN into a frame appropriate to a WAN and vice versa.

CIA - Confidentiality, Integrity, and Availability

CIO- Chief Information Officer

Client Agent- Configures how often client computers retrieve the policy that gives them their basic configuration settings. For example, after you configure the other client agent settings, Configuration Manager puts those settings into policy and sends them to the management point, and client computers poll for them on the schedule that you configure. This agent also controls settings that are common to several Configuration Manager features, for example, how often users are prompted with reminders about client operations and what customized organization names users see with the reminders

Configuration Control - Process for controlling modifications to hardware, firmware, software, and documentation to ensure the information system is protected against unauthorized or improper modifications prior to, during, and after system implementation.

Continuous Monitoring - Per NIST SP 800-137, continuous monitoring is maintaining an ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. The objective is to conduct ongoing monitoring of the security of an organization's networks, information, and systems, and respond by accepting, avoiding/rejecting, transferring/sharing, or mitigating risk as situations change.

CRL- Certificate Revocation List

Cryptography - The discipline that embodies the principles, means, and methods for the transformation of data in order to hide semantic content, prevent unauthorized use, or prevent undetected modification.

CSIRC - Computer Security Incident Response Center

Exhibit 10.8.55-2 (Cont. 2) (11-03-2023)**Terms and Acronyms****D**

DISA - Defense Information Systems Agency

Dynamic Host Configuration Protocol (DHCP) - A protocol used by network devices (clients) to obtain various parameters necessary for the clients to operate in an Internet Protocol (IP) network. By using this protocol, system administration workload greatly decreases, and devices can be added to the network with minimal or no manual configurations.

Denial of Service (DoS) - Action(s) that strive to make a computer resource unavailable to authorized users, generally consisting of the concerted efforts of a person or persons to prevent an information resource from functioning efficiently or at all, temporarily or indefinitely.

Deep Packet Inspection - An inspection engine that analyzes data at the application layer, typically layers 5 through 7 of the OSI model.

Demilitarized Zone (DMZ) - An interface on a routing firewall that is similar to the interfaces found on the firewall's protected side. Traffic moving between the DMZ and other interfaces on the protected side of the firewall still goes through the firewall and can have firewall protection policies applied. A host or network segment inserted as a "neutral zone" between an organization's private network and the Internet. Perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

Designated Router (DR) - Router selected to receive other router's link-state advertisements. Each multi-access network has a DR, which performs two main functions; originate network link advertisements on behalf of the network and establish adjacencies with all routing devices on the network, thus participating in the synchronizing of the link-state databases.

DVD - Digital Video Disc

E

EA - Enterprise Architecture

EAP - Extensible Authentication Protocol

Encryption - The reversible transformation of data from the original (the plaintext) to a difficult-to-interpret format (the ciphertext) as a mechanism for protecting its confidentiality, integrity and sometimes its authenticity. Encryption uses an encryption algorithm and one or more encryption keys.

F

Federal Information Processing Standard (FIPS) - A standard for adoption and use by federal departments and agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability.

Federal Information Security Management Act (FISMA) - Title III of the E-Government Act requiring each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Annual security reviews of programs and systems are to be conducted and the results reported to the Office of Management and Budget (OMB).

Exhibit 10.8.55-2 (Cont. 3) (11-03-2023)**Terms and Acronyms****G**

Group Master Key (GMK) - An auxiliary key that may be used to derive a group temporal key.

GSP - Guideline, Standard and Procedure

H

HIGH Impact System - An information system in which at least one security objective (e.g., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of HIGH.

HTTP - Hypertext Transfer Protocol

HTTPS - Hypertext Transfer Protocol Secure

I

ICMP- Internet Control Message Protocol

IEEE 802.11- A family of IEEE standards that extend the common wired Ethernet local network standard into the wireless domain using the 5 GHz and 2.4 GHz public spectrum bands. It specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. It is commonly referred to as “Wi-Fi” because the “Wi-Fi Alliance” provides certification for 802.11 products.

Information at Rest - Data in computer storage (e.g., on hard disk drives, CDs/DVDs, floppy disks, thumb drives, PDAs, cellphones, other removable storage media, etc.) while excluding data that is traversing in a network (data in transit) or temporarily residing in computer memory to be read or updated (data in use).

Information Security - The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide CIA.

Information System - A discrete set of information resources organized for the collection, processing, maintenance, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual.

Interior Gateway Protocol (IGP) - A type of protocol used in exchanging routing information between gateways (commonly routers) within an autonomous system (for example, a system of corporate local area networks). This routing information can then be used to router network-layer protocols like IP.

Intermediate Distribution Frame (IDF) - A distribution frame that cross-connects the user cable media to individual line circuits and may serve as a distribution point for multipair cables from the main distribution frame or combined distribution frame to individual cables connected to equipment in areas remote from these frames.

Internet Group Management Protocol (IGMP) - A communication protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships.

Intrusion Detection System (IDS) - Software and/or hardware designed to detect unwanted attempts to access, manipulate, and/or disable computer systems, mainly through a network, such as the Internet.

Intrusion Detection and Prevention System (IDPS) - Software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

Intrusion Prevention System (IPS) - System(s) which can detect an intrusive activity and can also attempt to stop the activity, ideally before it reaches its targets.

Exhibit 10.8.55-2 (Cont. 4) (11-03-2023)**Terms and Acronyms**

ISSO - Information System Security Officer

K

Key Management - The activities involving the handling of cryptographic keys and other related security parameters during the entire life cycle of the keys, including their generation, storage, establishment, entry and output, and zeroization.

Keyed-Hash Message Authentication Code (HMAC) - A specific type of message authentication code involving a cryptographic hash function and a secret cryptographic key. It may be used to simultaneously verify both the data integrity and the authentication of a message.

L

Label Distribution Protocol (LDP) - A protocol in which routers capable of MPLS exchange label mapping information. Two routers with an established session are called LDP peers and the exchange of information is bi-directional.

LAN- Local Area Network

Least Privilege - The security principle that requires each subject to be granted the most restrictive set of privileges necessary to carry out their assigned duties and functions.

M

MFA- Multi-factor Authentication

MSDP - Multicast Source Discovery Protocol

Multicast Listener Discovery (MLD) - Used by IPv6 routers for discovering multicast listeners on a directly attached link, much like IGMP is used in IPv4.

Multifactor Authentication - Requires the use of two or more different factors to achieve authentication. The factors are defined as: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (e.g., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Multifactor solutions that require devices separate from information systems gaining access include, for example, hardware tokens providing time-based or challenge-response authenticators and smart cards such as the U.S. Government PIV card and the DoD common access card.

Multi-Protocol Labeled Switching (MPLS) - A type of data-carrying technique for high-performance telecommunications network.

N

Network Access - Access to an information system by a user (or a process acting on behalf of a user) communicating through a network (e.g., local area network, wide area network, Internet).

Network Address Translation – Protocol Translation (NAT-PT) - An IPv6-to-IPv4 translation mechanism, as defined in RFC 2765 and RFC 2766, which allows IPv6-only devices to communicate with IPv4-only devices and vice versa.

Network Elements - Any Multiplexers, Routers, CSU/DSUs, Channel Compression Devices, and/or Trunk Encryption that is in the route or path that connects IRS Switches, non-IRS Users, and/or IP Devices.

NIST - National Institute of Standards and Technology

Exhibit 10.8.55-2 (Cont. 5) (11-03-2023)**Terms and Acronyms**

NSA - National Security Agency

NTP - Network Time Protocol

Non-repudiation - Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the information.

O

OFDM- Orthogonal Frequency Division Multiplexing

OMB - Office of Management and Budget

OCSP- Online Certificate Status Protocol

Operating System (OS) - A collection of software that manages computer hardware resources and provides common service for computer programs.

Out of Band Management Network (OOB/OOBM)- This is the dedicated management network. It utilizes encrypted connections (Transport Layer Security [TLS] and Internet Protocol Security [IPSec]) between the user and the hosting site to provide management capability for servers, applications and network devices. It also provides transport of monitoring and reporting devices.

P

Pairwise Master Key (PMK) - A key established between the wireless station and the access point. This key is typically generated using 802.1X, which is authentication of the user to a RADIUS or other authentication server using Extensible Authentication Protocol. Both the station and RADIUS server derive identical keys and the RADIUS server returns that key to the access point.

Path Maximum Transmission Unit (PMTU)Discovery - A standardized technique in computer networking for determining the MTU size on the network path between two IP hosts, usually with the goal of avoiding IP fragmentation. Originally intended for routers in IPv4, in IPv6 this function has been explicitly delegated to the end points of a communication session. See RFC 119 for additional guidance on PMTU Discovery.

PIM - Protocol Independent Multicast

PIV - Personal Identity Verification

Plan of Action and Milestones (POA&M) - A key document of an information system's security authorization package describing the specific measures that are planned: (i) to correct weaknesses or deficiencies noted in the security controls during the security control assessment; and (ii) to address known vulnerabilities in the information system. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

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.

Q

Quality of Service (QoS) - The description or measurement of the overall performance of a service, such as telephony or computer networking service, particularly the performance seen by the users of the network. Cisco defines as the set of techniques to manage network resources.

Exhibit 10.8.55-2 (Cont. 6) (11-03-2023)**Terms and Acronyms****R**

Remediation - The act of correcting a vulnerability or eliminating a threat through activities such as installing a patch, adjusting configuration settings, or uninstalling a software application.

Remote Access - Access to an organizational information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

Remote Access Server (RAS) - A server, normally equipped with one or more modems, which allows remote users to dial in and establish temporary connections to a network.

Remote Authentication Dial-In User Service (RADIUS) - A client/server protocol and software that enables remote access servers to communicate with a central server to authenticate dial-in users and authorize their access to the requested system or service.

Risk Assessment - The process of determining risks; that is, determining the extent to which an entity is threatened by potential, adverse circumstances or events. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF). Risk assessment for information system-related security risks includes assessment of the susceptibility to adverse impacts through information (e.g., consideration of dependence on information, vulnerabilities in mission and business processes, and effectiveness of risk mitigations) and assessment of the threat environment with regard to causing such impacts. Synonymous with risk analysis.

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). To document risk-based determinations, IT Cybersecurity has created an SOP and associated Form 14201.

Robust Security Network (RSN) - A protocol for establishing secure communications over an 802.11 wireless network.

S

SA – System Administrator

Security Authorization - The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation, based on the implementation of an agreed-upon set of security controls.

Security Authorization Boundary - All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected.

Security Requirements Guide (SRG) - General statements and recommendations on how to secure a type of technology, without calling out a specific flavor or vendor.

Security Technical Implementation Guide (STIG) - A methodology for standardized secure installation and maintenance of computer software and hardware.

SNMP - Simple Network Management Protocol

Exhibit 10.8.55-2 (Cont. 7) (11-03-2023)**Terms and Acronyms**

Spanning Tree Protocol (STP) – A network protocol that builds a loop-free logical topology for Ethernet networks. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. STP also allows a network design to include backup links providing fault tolerance if an active link fails.

Standard Operating Procedure (SOP) - established or prescribed methods to be followed routinely for the performance of designated operations or in designated situations

T

Terminal Access Controller Access Control System (TACACS) - An authentication protocol common to UNIX networks that allows a remote access server to forward a user's logon password to an authentication server to determine whether access can be allowed to a given system.

TCP/IP - Transmission Control Protocol/Internet Protocol

TCP/UDP - Transmission Control Protocol-User Datagram Protocol

Treasury Directive Publication (TD-P) - Documents that provide IT security requirements and supporting guidance that apply to the Department of the Treasury bureaus, Departmental Offices (DO), Office of the Inspector General (OIG), and the Treasury Inspector General for Tax Administration (TIGTA), hereafter referred to collectively as bureaus.

TTL – Time-to-Live

Technical Controls - The security controls (e.g., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software, or firmware components of the system.

U

UUFB - Unknown Unicast Flood Blocking

US-CERT - United States Computer Emergency Readiness Team

User Account - An operating system data object containing information identifying a user to an operating system. A user account, for example typically contains a user's name and password, the user account's group memberships, and the user's rights and permissions for accessing an information system and its resources.

V

VLAN – Virtual Local Area Network

VLAN Trunk Protocol (VTP) - A Cisco proprietary protocol that propagates the definition of VLANs on the whole local area network.

Voice over Internet Protocol (VoIP) - A methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks.

VPN - Virtual Private Network

Vulnerability - Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Assessment - Formal description and evaluation of the vulnerabilities in an information system.

Exhibit 10.8.55-2 (Cont. 8) (11-03-2023)**Terms and Acronyms**

Vulnerability Scanning - The process of proactively identifying vulnerabilities of an information system in order to determine if and where a system can be exploited and/or threatened. Employs software that seeks out security flaws based on a database of known flaws, testing systems for the occurrence of these flaws and generating a report of the findings that an individual or an enterprise can use to tighten the network's security.

W

Waiver - A process utilized by IRS's Enterprise Architecture (EA) organization. System Owners can request a Waiver for system(s) that cannot meet the infrastructure configuration management requirements established by the EA.

Wide Area Network (WAN) - A network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, or national boundaries) using private or public network transports.

Wi-Fi Protected Access (WPA) - A security protocol and security certification program developed by the Wi-Fi Alliance to secure wireless computer networks.

WPA2 - Wi-Fi Protected Access II

WIDS- Wireless Intrusion Detection System

Wireless Local Area Network (WLAN) - Links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), and usually providing a connection through an access point to the wider Internet.

Exhibit 10.8.55-3 (11-03-2023)**Related Resources****IRS Publications**

- IRM 10.8.1 – *Information Technology (IT) Security, Policy and Guidance*
- IRM 10.8.2 – *Information Technology (IT) Security, Roles and Responsibilities*
- IRM 10.9.1 – *Classified National Security Information (NSI)*

Department of the Treasury Publications

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

National Institute of Standards and Technology (NIST) Publications

- NIST FIPS 140-3: *Security Requirements for Cryptographic Modules*, March 22, 2019
- 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*, December 2018
- NIST SP 800-53 Rev 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, December 10, 2020
- 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)
- NIST SP 800-57 Rev 5, *Recommended for Key Management – Part 1 General*, May 04, 2020
- NIST SP 800-97, *Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*, February 7, 2007
- NIST SP 800-98, *Guidelines for Securing Radio Frequency Identification (RFID) Systems*, April 2007
- NIST SP 800-131A Rev 2, *Transitioning the Use of Cryptographic Algorithms and Key Lengths*, March 2019
- NIST SP 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs)* February 2012
- NIST SP 800-175B Rev 1, *Guideline for Using Cryptographic Standards in the Federal Government: Cryptographic Mechanisms*, March 2020

Defense Information Systems Agency (DISA) Publications

- Network Device Management SRG V4R1, April 27, 2021
- Layer 2 Switch SRG V2R1, May 21, 2021
- Router SRG V4R2, April 27, 2021
- 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 Requirements Checklists exhibit for additional information.
- DISA security guides are available at: <https://public.cyber.mil/stigs/>

