MANUAL TRANSMITTAL

10.8.1

Department of the Treasury
Internal Revenue Service

DECEMBER 12, 2023

EFFECTIVE DATE

(12-12-2023)

PURPOSE

(1) This transmits revised Internal Revenue Manual (IRM) 10.8.1, *Information Technology (IT) Security, Policy and Guidance.*

MATERIAL CHANGES

(1) Throughout this IRM, requirements written with “shall” verbiage updated to “must” to align with industry writing best practices.

(2) Throughout the IRM: A leading “zero” (0) added to NIST control and control enhancement numbers as part of alignment with NIST SP 800-53 Rev5.1.1 release. Example: “AC-1(1)” becomes “AC-01(01)”.

(3) IRM 10.8.1 has been revised to align with IRM 1.11.2 as a part of the Publications Management & Resource Services (PMRS) Internal Controls data call.

(4) 10.8.1.1 Program Scope and Objectives - Updated to align with Security Policy Boiler Plate and PMRS.

(5) Original 10.8.1.1.1.1, Scope - Removed to align with IRM 1.11.2 as a part of the PMRS data call.

(6) Original 10.8.1.1.1.1 (1) Scope - Requirements incorporated into new 10.8.1.1.5 Program Controls.

(7) Original 10.8.1.1.1.1 (2) Scope - Requirements incorporated into new 10.8.1.1.5 Program Controls.

(8) Original 10.8.1.1.1.1 (3) Scope - Requirements incorporated into 10.8.1.3 General Policy.

(9) Original 10.8.1.1.1.1 (4) Scope - Requirements incorporated into 10.8.1.4 Security and Privacy Controls, Enhancements, and Supplemental Guidance.

(10) Original 10.8.1.1.1.1 (5) Scope - Requirements incorporated into new 10.8.1.1.5 Program Controls.

(11) Original 10.8.1.1.1.1 (6) Scope - Requirements incorporated into new 10.8.1.1.6 Terms and Acronyms.

(12) Original 10.8.1.1.1.2 Objectives - Removed to align with IRM 1.11.2 as a part of the PMRS data call.

(13) Original 10.8.1.1.1.2 (1) Objectives - Requirements incorporated into new 10.8.1.1.5 Program Controls.

(14) Original 10.8.1.1.1.2 (2) Objectives - Requirements incorporated into 10.8.1.4 Security and Privacy Controls, Enhancements, and Supplemental Guidance.

(15) Original 10.8.1.1.1.2 (3) Objectives - Requirements incorporated into 10.8.1.4 Security and Privacy Controls, Enhancements, and Supplemental Guidance.

(16) Original 10.8.1.1.1.2 (4) Objectives - Requirements incorporated into 10.8.1.1.4 Program Management and Review.

(17) 10.8.1.1.4 Program Management and Review - Added to align with IRM 1.11.2 as a part of the PMRS data call.

(18) 10.8.1.1.5 Program Controls - Added to align with IRM 1.11.2 as a part of the PMRS data call.

(19) 10.8.1.1.5 Program Controls - Note for on-premise and off-premise systems added.

(20) 10.8.1.1.6 Terms and Acronyms - Added to align with IRM 1.11.2 as a part of the PMRS data call.

(21) Original 10.8.1.1.6 Risk Acceptance and Risk-Based Decisions - Relocated to 10.8.1.2.

(22) Original 10.8.1.1.6.1 Risk Acceptance Request - Relocated to 10.8.1.2.1.

(23) Original 10.8.1.1.6.2 Exceptions to Treasury Requirements - Relocated to 10.8.1.2.2.

(24) Original 10.8.1.1.7 Roles and Responsibilities - Relocated to 10.8.1.1.3.

(25) 10.8.1.1.7 References - Added to align with IRM 1.11.2 as a part of the PMRS data call.

(26) 10.8.1.2 Risk Acceptance and Risk-Based Decisions - Relocated from original 10.8.1.1.6.

(27) 10.8.1.2 Risk Acceptance and Risk-Based Decisions - URL updated.

(28) 10.8.1.2.1 Risk Acceptance Request - Relocated from original 10.8.1.1.6.1.

(29) 10.8.1.2.1 Risk Acceptance Request - Removed TD P 85-01 S-CVM.18 requirement.

(30) 10.8.1.2.2 Exceptions to Treasury Requirements - Relocated from original 10.8.1.1.6.2.

(31) 10.8.1.2.2 Exceptions to Treasury Requirements - Updated Exceptions language to align with TD P 85-01.

(32) 10.8.1.3 General Policy - Updated with language from the old Scope and Objectives.

(33) 10.8.1.3.1 Zero Trust and Zero Trust Architecture - Updated with language from OMB Memo M-22-09.

(34) 10.8.1.4 Security and Privacy Control, Enhancements and Supplements - Updated with language from original 10.8.1.1.1.1 Scope and original 10.8.1.1.1.2 Objectives.

(35) 10.8.1.4.1.1.1 Administrator Account - Language corrected for clarification.

(36) 10.8.1.4.1.1.8 Access to Sensitive Information - OMB guidance relocated from 10.8.1.4.1.2 inserted to subsection.

(37) 10.8.1.4.1.1.10 Non-IRS Access - Updated ″viruses″ to ″viruses/malicious code″ for consistency throughout the IRM.

(38) 10.8.1.4.1.1.10 Non-IRS Access - Replaced outdated unescorted (staff-like) access guidance with reference to IRM 10.2.18.

(39) 10.8.1.4.1.2 AC-03 Access Enforcement - Updated with language from OMB Memo M-22-09.

(40) 10.8.1.4.1.5 AC-06 Least Privilege (InTC) - Requirement to document developer access added.

(41) 10.8.1.4.1.7 AC-08 System-Use Notifications - ″SATE programs″ changed to ″security awareness and training programs″.

(42) 10.8.1.4.1.17 AC-18 Wireless Access - Note updated with reference to the *FMSS Classified Information Security Team mailbox.

(43) 10.8.1.4.1.18.2 Video and Photographic Technologies - Reference to IRM 10.2.24 for physical security photography guidance added.

(44) 10.8.1.4.1.21 AC-22 Publicly Accessible Content - Reference to IRM 10.5.1 for additional publicly accessible content guidance added.

(45) 10.8.1.4.3.1 AU-02 Event Logging - Updated with language from OMB Memo M-22-09.

(46) 10.8.1.4.4.1 CA-02 Control Assessment - Updated with language from OMB Memo M-22-09.

(47) 10.8.1.4.4.5.2 FISMA Reporting Requirements - Updated with language from OMB Memo M-23-03.

(48) 10.8.1.4.4.6 CA-07 Continuous Monitoring (InTC) - Independent assessor guidance updated to align with TD P 85-01 App A language.

(49) 10.8.1.4.5.7 CM-08 System Component Inventory - Note added to CISA BOD 23-01 guidance for clarification.

(50) 10.8.1.4.5.7 CM-08 System Component Inventory - Updated with language from OMB Memo M-22-09 and CISA BOD 23-01.

(51) 10.8.1.4.7.1 IA-02 Identification and Authentication (Organization Users) - Updated with language from OMB Memo M-22-09.

(52) 10.8.1.4.7.2 IA-03 Device Identification and Authentication - Updated with language from OMB Memo M-22-09.

(53) 10.8.1.4.7.4 IA-05 Authenticator Management - Updated with language from OMB Memo M-22-09.

(54) 10.8.1.4.7.4.1 Application and Operating System (OS) Password Policies - Title changed to Application and Operating System (OS) Password Policies for Non-MFA Systems as part of OMB Memo M-22-09 update.

(55) 10.8.1.4.7.4.1 Application and Operating System (OS) Password Policies for Non-MFA Systems - Updated with language from OMB Memo M-22-09.

(56) 10.8.1.4.7.7 IA-08 Identification and Authentication (Non-organizational Users) - Updated with language from OMB Memo M-22-09.

(57) 10.8.1.4.8.3 IR-04 Incident Handling - Changed impact level.

(58) 10.8.1.4.8.5 IR-06 Incident Reporting - Updated URL.

(59) 10.8.1.4.11 PE-01 Physical and Environmental Protection Policy & Procedures - Limited areas guidance removed and language referring readers to 10.2 series for restricted security access areas guidance added.

(60) 10.8.1.4.13 Program Management Control - Updated OMB A-130 updated with title.

(61) 10.8.1.4.13.5 PM-05 System Inventory - Updated with language from OMB Memo M-22-09 and Memo M-23-02.

(62) 10.8.1.4.13.6 PM-06 Measures of Performance - Updated with language from OMB Memo M-22-09.

(63) 10.8.1.4.13.12 PM-12 Insider Threat Program - Clarified authority for the security control requirement.

(64) 10.8.1.4.16.9 RA-10 Threat Hunting - Added Threat Hunting requirements to the IRS baseline per TIGTA’s recommendation.

(65) 10.8.1.4.17.3 SA-04 Acquisition Process - Updated with language from OMB Memo M-22-18.

(66) 10.8.1.4.17.3 SA-04 Acquisition Process - Notes for SA-04_T.189 revised to clarify they are informative in nature and not requirements.

(67) 10.8.1.4.17.8 SA-09 External System Services - Updated to align with current Federal CIO guidance and to remove impact and overlay designations.

(68) 10.8.1.4.18 SC-01 System and Communications Protection Policy and Procedures - Removed URL for IPv6 Transition PMO Portal that is inaccessible to IRS employees.

(69) 10.8.1.4.18.6.2.4 Multi-Function Devices (MFDs) - Updated MFD protection guidance and reference to IRM 10.2.14.

(70) 10.8.1.4.18.7 SC-08 Transmission Confidentiality and Integrity - Removed IRM 10.2 Physical Security series references not relevant to the requirements they’re associated with.

(71) 10.8.1.4.18.19 SC-20 Secure Name/Address Resolution (Authoritative Source) - Updated with language from OMB Memo M-22-09 and Memo M-23-10.

(72) 10.8.1.4.18.27 SC-28 Protection of Information at Rest - Updated the impact levels.

(73) 10.8.1.4.19.1 SI-02 Flaw Remediation - Updated with language from OMB Memo M-22-09, Memo M-22-01, Memo M-21-31, CISA BOD 23-01, CISA Cloud Security Technical Reference and NSA Adversary Emulation Guidance.

(74) 10.8.1.4.19.2 SI-03 Malicious Code Protection - Removed the Linux exception.

(75) 10.8.1.4.19.3 SI-04 System Monitoring (InTC) - Grammar corrected.

(76) 10.8.1.4. 20.5 SR-06 Supplier Assessment and Review - Updated with language from OMB Memo M-22-18.

(77) Exhibit 10.8.1-1 Glossary and Acronym Lists - Title changed to Terms and Acronyms.

(78) Exhibit 10.8.1-1 Terms and Acronyms - A&I acronym remove.

(79) Exhibit 10.8.1-1 Terms and Acronyms - Controlled Area definition added.

(80) Exhibit 10.8.1-1 Terms and Acronyms - DRP acronym remove.

(81) Exhibit 10.8.1-1 Terms and Acronyms - EDR acronym added.

(82) Exhibit 10.8.1-1 Terms and Acronyms - Limited Area definition updated.

(83) Exhibit 10.8.1-1 Terms and Acronyms - SATE acronym removed.

(84) Exhibit 10.8.1-1 Terms and Acronyms - Security Area definition added.

(85) Exhibit 10.8.1-1 Terms and Acronyms - SOAR acronym added.

(86) Exhibit 10.8.1-1 Terms and Acronyms - US-CERT acronym removed.

(87) Exhibit 10.8.1-2 References - Title changed to Related Resources.

(88) Exhibit 10.8.1-2 Related Resources - IRM 2.5 series added.

(89) Exhibit 10.8.1-2 Related Resources - IRM 2.7.1 added.

(90) Exhibit 10.8.1-2 Related Resources - IRM 2.16.1 added.

(91) Exhibit 10.8.1-2 Related Resources - IRM 2.25 series added.

(92) Exhibit 10.8.1-2 Related Resources - IRM 2.149 series added.

(93) Exhibit 10.8.1-2 Related Resources - IRM 2.150.2 added.

(94) Exhibit 10.8.1-2 Related Resources - IRM 3.10 series added.

(95) Exhibit 10.8.1-2 Related Resources - IRM 6.610.1 added.

(96) Exhibit 10.8.1-2 Related Resources - IRM 6.751.1 added.

(97) Exhibit 10.8.1-2 Related Resources - IRM 6.752 series added.

(98) Exhibit 10.8.1-2 Related Resources - IRM 10.2 series added.

(99) Exhibit 10.8.1-2 Related Resources - IRM 10.8.24 added.

(100) Exhibit 10.8.1-2 Related Resources - IRM 10.23.1 added.

(101) Exhibit 10.8.1-2 Related Resources - IRM 10.23.2 added.

(102) Exhibit 10.8.1-2 Related Resources - IRM 10.23.3 added.

(103) Exhibit 10.8.1-2 Related Resources - IRM 11.3.1 added.

(104) Exhibit 10.8.1-2 Related Resources - Policy Statement P-1-144 updated to Policy Statement 2-90.

(105) Exhibit 10.8.1-2 Related Resources - Executive Order 13960 added.

(106) Exhibit 10.8.1-2 Related Resources - OMB Memo M-19-13 added.

(107) Exhibit 10.8.1-2 Related Resources - OMB Memo M-22-01 added.

(108) Exhibit 10.8.1-2 Related Resources - OMB Memo M-22-18 added.

(109) Exhibit 10.8.1-2 Related Resources - OMB Memo M-23-02 added.

(110) Exhibit 10.8.1-2 Related Resources - OMB Memo M-23-03 added.

(111) Exhibit 10.8.1-2 Related Resources - OMB Memo M-23-10 added.

(112) Exhibit 10.8.1-2 Related Resources - OMB Memo M-23-16 added.

(113) Throughout this IRM, defined acronyms the first time used.

(114) Throughout this IRM, replaced ″§″ with ″Section″ to align with the IRS Style Guide.

(115) Throughout this IRM, updated ″US-CERT″ to ″CISA″.

(116) Editorial changes made throughout the IRM for clarity. Reviewed and updated plain language, grammar, titles, website addresses, legal references and IRM references.

(117) The following Interim Guidance Memorandums (IG Memos) are incorporated into this IRM:

a. Interim Guidance Memo # IT-10-0323-0003 - Interim Guidance (IG) - Policy Update Internal Revenue Manual (IRM) 10.8.1, OMB Memos and NSA Adversary Emulation Study for Zero Trust Architecture (ZTA) Updates, dated July 5, 2023.
b. Interim Guidance Memo # IT-10-0523-0006 - Interim Guidance (IG) - Policy Update Internal Revenue Manual (IRM) 10.8.1, Removal of SI-3 Malicious Code Protection Exceptions, dated June 27, 2023.

c. Interim Guidance Memo # IT-10-1122-0027 - Interim Guidance (IG) - Policy Update Internal Revenue Manual (IRM) 10.8.1, Software Supply Chain Attestation – OMB M-22-18, dated January 25, 2023.
d. Interim Guidance Memo # IT-10-1022-0012 - Interim Guidance (IG) - Policy Update Internal Revenue Manual (IRM) 10.8.1, IA-5 Password Complexity - OMB M-22-09, dated December 07, 2022.

(118) All content within this IRM is being released as guidance to facilitate implementation of the numerous updates to the aforementioned.

EFFECT ON OTHER DOCUMENTS

This IRM supersedes IRM 10.8.1 dated December 13, 2022. Additionally, this IRM was updated to incorporate Interim Guidance Memoranda listed in the material changes section.

AUDIENCE

The provisions in this manual 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, volunteers and outsourcing providers, which use or operate systems that store, process, or transmit IRS information or connect to an IRS network or system.

Kaschit Pandya
Acting, Chief Information Officer

10.8.1
Policy and Guidance

Table of Contents

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

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

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

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

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

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

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

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

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

#

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

Exhibits

10.8.1.1 (12-12-2023) Program Scope and Objectives

(1) **Overview:** This Internal Revenue Manual (IRM) lays the foundation to implement and manage security for systems within the Internal Revenue Service (IRS). It provides guidance on all aspects of security for the protection of Information Technology (IT) resources.

a. This guidance establishes the IT security framework for the development of security control specific implementations defined in subordinate IRMs, IRS publications (e.g., IRS Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies*; IRS Pub 4812, *Contractor Security & Privacy Controls -– Handling and Protecting Information or Information Systems*), and subordinate procedural guidance (e.g., Standard Operating Procedures (SOPs), Desk Procedures).
b. This IRM provides the minimal security requirements for IRS IT systems based on data classification. Subordinate IRM sections of the 10.8 series provide platform and technology specific security requirements and may have vendor specific hardening security requirements checklists associated with them. In the event there is a conflict between IRM 10.8.1 and subordinate IRM sections (and their checklists), the more restrictive setting must be implemented and documented.
c. Subordinate procedural guidance (e.g., SOPs) must be used to provide detailed guidance for implementing and complying with the requirements within this IRM.
d. Binding Operational Directives (BOD) and Emergency Directives issued by Cybersecurity and Infrastructure Security Agency (CISA) at the Department of Homeland Security (DHS) are effective immediately and are incorporated into IRS Security Policies. If there is a conflict with or variance between the CISA guidance and IRS security guidance, the more restrictive guidance takes precedence.

(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.

10.8.1.1.1 (12-12-2023) Background

(1) Federal Information Processing Standards (FIPS) Publication 200, *Minimum Security Requirements for Federal Information and Information Systems* mandates the use of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 as baseline for the creation of agency IT security policy.

(2) IRM 10.8.1 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Information Technology Cybersecurity.

10.8.1.1.2 (12-13-2022) **Authority**

(1) This IRM covers IT controls from NIST SP 800-53 Rev 5, **Security and Privacy Controls for Information Systems and Organizations**, Department of the Treasury policy, IRS-defined policy, regulatory and mandated guidance, and other sources (refer to IRM 10.8.1.1.7 Related Resources subsection within this IRM).

(2) Per FIPS 200, **Minimum Security Requirements for Federal Information and Information Systems**:

a. Policies and procedures play an important role in the effective implementation of enterprise-wide information security programs within the Federal Government and the success of the resulting security measures employed to protect federal information and information systems. Thus, organizations must develop and promulgate formal, documented policies and procedures governing the minimum security requirements set forth in this standard and must ensure their effective implementation.
b. SPs are developed and issued by NIST as recommendations and guidance documents. For other than national security programs and systems, federal agencies must follow those NIST SPs mandated in FIPS. FIPS 200 mandates the use of Special Publication 800-53, as amended. In addition, Office of Management and Budget (OMB) policies (including OMB Reporting Instructions for *Federal Information Security Modernization Act of 2014* (FISMA) and Agency Privacy Management) state that for other than national security programs and systems, federal agencies must follow certain specific NIST SPs.
c. While federal agencies are required to follow certain specific NIST SPs in accordance with OMB guidance, agencies have flexibility in how to apply the guidance. Federal agencies apply the security concepts and principles articulated in the NIST SPs in accordance with and in the context of the agency's missions, business functions, and environment of operation. Consequently, the application of NIST guidance by federal agencies can result in different security solutions that are equally acceptable, compliant with the guidance, and meet the OMB definition of adequate security for federal systems.

(3) IRM 10.8.1 is issued under the authority of Treasury Directive Publication (TD P) 85-01, *Treasury Information Technology (IT) Security Program*.

(4) In accordance with OMB's FISMA guidelines for non-national security programs and systems, agencies must follow NIST standards and guidance. Non-national security systems must provide adequate, risk-based protection in the control areas defined in FIPS 200 by using the appropriate NIST SP 800-53 baseline security controls for the designated FIPS 199 impact level, as augmented and scoped by the Department of the Treasury, bureau, and system owner (to the extent authorized).

10.8.1.1.3 (12-12-2023) **Roles and Responsibilities**

(1) The IRS must implement security roles in accordance with federal laws and IT security guidelines (e.g., FISMA, NIST, OMB) that are appropriate for their specific operations and missions.

(2) 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.

10.8.1.1.4
(12-12-2023)
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 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 manual 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, Department of the 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.

10.8.1.1.5
(12-12-2023)
Program Controls

(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, 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 policy delineates the security management structure, assigns responsibilities, and lays the foundation necessary to measure progress and compliance. The requirements within this policy are organized to follow the order in which security and privacy controls are presented within NIST SP 800-53 Rev 5.

a. In an effort to reference the origin of a requirement (NIST, Treasury, etc.), a requirement may have its origin referenced in parenthesis at the end of the requirement; such as (CA-01), (AC-03_T.001), or (IRS-defined).
b. Use of the term ″system″ in this policy is expanded to include Cloud technology, Web 2.0, and successor technologies and is applicable to all non-national security systems. (TD P 85-01, 1.3)

(4) 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, *National Security Information, Classified National Security Information (NSI)*, for additional guidance for protecting classified information.

(5) Cybersecurity documents and publishes controls (IRM 10.8 series) for the IRS Information Technology Environment/Resources.

a. Authorizing Officials (AOs) are required to develop and maintain additional operational documentation (e.g., action and implementation plans, SOPs), necessary for implementation of the security controls delineated in the IRM 10.8 series.
b. The AO is responsible for implementation of security policy. These responsibilities include the documentation and procedures for how the systems are managed, administered, and monitored.

(6) This IRM establishes the minimum baseline security policy and requirements for all IRS 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 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*.

10.8.1.1.6
(12-12-2023)
Terms and Acronyms

(1) Refer to Exhibit 10.8.1-1, Terms and Acronyms, for a list of terms, acronyms, and definitions. (L, M, H)

(2) For the purpose of this IRM, the following terms apply:

a. IRS personnel or users, which includes: Employees, Consultants, Detailees, Temporary Employees, Interns, IRS Contractors, Non-Person Entity (NPE) also referred to as Robotic Process Automation (RPA), Bots, Artificial Intelligence (AI) Workers, Digital Assistants etc.
b. Authorized or Unauthorized personnel applies to all IRS personnel being authorized or not authorized to perform a particular action.
c. "Developers" or "Application Developers" refers to "Program Developers/ Programmers" and "Web Developers" as defined in IRM 10.8.2.

Note: The requirement in part "c" does not refer to Database Administrators (DBAs), who may assist Developers.

10.8.1.1.7
(12-12-2023)
Related Resources

(1) Refer to Exhibit 10.8.1-2, Related Resources, for a list of related resources and references. (L, M, H)

10.8.1.2
(12-12-2023)

Risk Acceptance and Risk-Based Decisions

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

(2) Users must submit RBD requests in accordance with Cybersecurity's Security Risk Management (SRM) Risk Acceptance Process documented in the Risk Based Decision Standard Operating Procedures (SOP).

#
#
#
#
#

10.8.1.2.1
(12-12-2023)

Risk Acceptance Request

(1) Security vulnerabilities can be discovered at any point in a system's lifecycle and by many different means. The most common actions that lead to the discovery of vulnerabilities are system configuration scans, penetration tests, vulnerability scans, and FISMA Control Assessment processes.

(2) Acceptable reasons for an RBD are:

a. Meeting the requirement is technically not possible;
b. Meeting the requirement is cost prohibitive; and
c. Meeting the requirement is operationally not feasible and would cause an undue burden to the system and/or seriously hinder its capability to accomplish its mission.

(3) An RBD must be documented in the pertinent system's security documentation (e.g., System Security Plan).

a. The AO's decision to accept the risk associated with an identified vulnerability and not remediate it is required to be tracked (e.g., Online RBD tool).
b. The AO's decision to remediate the risk associated with an identified vulnerability, but the remediation cannot be performed immediately, must be documented in a Plan of Action and Milestones (POA&M).

Note: The AO's decision guidance above aligns with CA-05 Plan of Action and Milestones, PL-11 Baseline Tailoring, RA-07 Risk Response, and NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*.

(4) IRS RBDs are not permanent.

(5) Prior to an RBD expiring, steps must be taken to either renew the RBD or implement mitigation to address the weakness.

a. If an RBD is dependent on a policy adjustment, the RBD must remain in effect until either the policy has been adjusted or the RBD expires (whichever comes first).
b. When an RBD expires, the requestor must be notified of the expiration.

(6) Refer to the Cybersecurity Risk Acceptance - Risk based Decision web site for guidance on the RBD process (e.g., SOP, Requirements, Business Entitlement Access Request System (BEARS) Access, Online RBD, Roles).

10.8.1.2.2
(12-12-2023)
Exceptions to Treasury Requirements

(1) Per TD P 85-01 Appendix A, IRS-wide exceptions to Treasury requirements shall be managed differently than system tailoring.

a. Documentation of exception requests to Treasury requirements must include operational justification, risk acceptance, and risk mitigation measures. Such requests must be submitted to and approved by the Chief Information Officer (CIO), in consultation with the IRS CISO. An approved exception must be signed by the individuals in these roles and held by the IRS, with a copy submitted to the Treasury CIO via the Treasury CISO for review.
b. This exception policy applies to the following:
i. Treasury parameters within NIST controls;
ii. Treasury controls; and
iii. Treasury policy located within TD P 85-01.

10.8.1.3
(12-12-2023)
General Policy

(1) In accordance with FISMA, the IRS must develop, document, and implement a service-wide information security program supporting the operations and assets of this agency.

a. Requirements contained within this IRM must not be grandfathered.
b. Requirements contained within this IRM must not be based on past practices.

(2) Systems approved for the processing of classified information must not be connected to any system not approved for classified operation. Systems approved for classified processing must not share peripherals with unclassified processing equipment except for switching devices approved by National Security Agency (NSA). Approval for the use of switching devices must be included in the security authorization documentation.

(3) The IRS Information Security Program must:

a. Ensure the objectives of applicable laws, policies, federal regulations, OMB guidance, TDs, NIST Publications, and other regulatory guidance are met by establishing and ensuring compliance with security requirements, procedures, and guidelines to properly implement security controls.

Note: In situations where regulatory guidance has been released outside of the annual update cycle for IRS requirement documents, the requirements within the regulatory guidance will be met through the issuance of interim guidance.

b. Ensure that systems used by the IRS provide appropriate protection for the confidentiality, integrity, and availability (CIA) of IRS information, through the use of security controls.
c. Implement policies, standards, and procedures which are consistent with government-wide policies, standards, and procedures issued by OMB, Department of Commerce, General Services Administration (GSA), Office of Personnel Management (OPM), and Department of the Treasury. Different or more stringent requirements for securing National Security Information (NSI) must be incorporated into agency programs as required by appropriate national security directives.
d. Provide for the protection of critical infrastructure by identifying critical assets and individual, proprietary, financial, tax, mission critical, or

otherwise sensitive information in accordance with Executive Order (EO) 13800, Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure.

e. Review each interdependency analysis and provide updates at least every three (3) years or whenever there has been a significant change to the critical asset or an impact to its environment.
f. Ensure the ability to maintain processing during and following an emergency.
g. Ensure the auditability of all systems.
h. Ensure management is responsible for designating the sensitivity of information, providing for the implementation of security controls, and certifying adequacy of these controls.
i. Ensure management accountability for resources entrusted to them in accomplishing IRS objectives.
j. Ensure individual accountability for the data, information, and other IT resources to which individuals have access.

Note: Implementation of the security controls defined within this IRM address the IRS Information Security Program requirements explicitly or implicitly.

(4) The IRS Information Security Program must include:

a. Risk assessments that consider internal and external threats to the CIA of systems and data supporting critical operations and assets.
b. Policies and procedures that address the risk assessments associated with the operations and assets for programs and systems by cost effectively reducing information security risks to an acceptable level, and ensuring compliance with prescribed policies and procedures.
c. Security Awareness Training to inform personnel of information security risks, procedures designed to reduce such risks, and their personal impact/responsibilities for both.
d. Management testing and evaluation of the effectiveness of information security policies and procedures.
e. A process for ensuring remedial action is defined for addressing deficiencies.
f. Procedures for detecting, reporting, and responding to incidents; mitigation of risks associated with such incidents before substantial damage occurs; notification/consultation with appropriate law enforcement officials and other offices/authorities.
g. Appropriate reporting to proper authorities of weaknesses and remedial actions.

(5) The IRS must implement the provisions of FISMA to include the guidelines outlined in NIST publications, OMB guidance, and FIPS.

(6) All IRS systems that generate, store, process, transfer, display, or communicate non-national security information must be protected at a level commensurate with the potential impact of a loss of confidentiality, integrity, or availability on IRS operations, assets, or individuals.

(7) Systems in a Development and Testing Environment must adhere to the security requirements within this IRM based on an assessment of risk and the system’s assigned FIPS 199 categorization level.

a. Refer to IRM 10.8.1.4.16.2 # RA-03 Risk Assessment and IRM 10.8.1.4.16.1 # Security Categorization within this IRM for guidance on conducting an assessment of risk and defining security categorization levels.

(8) Unless approved by the CIO, given the associated security challenges, lack of security solutions and high implementation cost, the use of emerging technologies that have not been evaluated by the federal government for their national security impacts is prohibited. (EO 13960 Sec 2 (c), Sec 3 (b); 44 USC 3551 Purposes (6))

Note: IRS Enterprise Architecture (EA) Enterprise Standards Profile (ESP) is the authoritative repository for IRS approved products and standards.

(9) This IRM and all Security Policy IRMs (10.8 series) must be evaluated a minimum of annually to ensure consistency with the IRS mission, functions, and associated laws, directives, regulations, and standards.

Note: Implementation of the security controls defined within this IRM address the IRS Information Security Program requirements explicitly or implicitly.

10.8.1.3.1
(12-12-2023)
Zero Trust and Zero Trust Architecture

(1) The IRS must: (EO 14028, Sec. 3(b)) (L, M, H)

a. Update existing agency plans to prioritize resources for the adoption and use of cloud technology as outlined in relevant OMB guidance;
b. Develop a plan to implement Zero Trust Architecture (ZTA), which must:
i. Incorporate, as appropriate, the migration steps that NIST has outlined in standards and guidance (e.g., NIST SP 800-207, *Zero Trust Architecture*);
ii. Describe any such steps that have already been completed;
iii. Identify activities that will have the most immediate security impact; and
iv. Include a schedule to implement them.
v. Include submission of implementation plan to OMB and CISA for FY 2022 - FY 2024 for OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles concurrence and a budget estimate for FY 2024, by March 27, 2022. (OMB M-22-09 (III)) (L, M, H)
c. Provide a report to the Director of OMB and the Assistant to the President and National Security Advisor (APNSA) discussing the plans required pursuant to sub-parts (1)a. and (1)b. above.

Note: The implementation of Zero Trust (ZT) and ZTA is pending further guidance from the Department of the Treasury.

(2) As the IRS continues to use cloud technology, they must do so in a coordinated, deliberate way that allows the Federal Government to prevent, detect, assess, and remediate cyber incidents. To facilitate this approach, the migration to cloud technology must adopt ZTA, as practicable. (EO 14028, Sec. 3(c)) (L, M, H)

(3) The IRS must: (EO 14028, Sec. 3(d)) (L, M, H)

a. Adopt multi-factor authentication and encryption for data at rest and in transit, to the maximum extent consistent with Federal records laws and other applicable laws.

(4) Privileged Access Management (PAM) solutions must not be used as a general purposed substitute for multi-factor authentication or for routine single-sign-on access to legacy systems in place of needed modernization of those systems. (OMB M-22-09 (III)(A)(2)) (L, M, H)

Note: When ZTA is not available for implementation, PAM solutions may be an iterative step that provides ephemeral single-factor credentials for human access to a system.

a. The IRS must integrate and enforce multi-factor authentication across applications involving authenticated access to Federal systems by IRS staff, contractors, and partners.
b. Refer to IRM 10.8.1.4.7.4 # IA-05 Authenticator Management for exceptions.

(5) Refer to NIST SP 800-207 for guidance on Zero Trust Architecture. (L, M, H)

10.8.1.3.2 (12-12-2023) **Critical Software**

(1) The IRS must comply with OMB and NIST guidance outlining security measures for the procurement of critical software, software supply chain security, and software verification. (EO 14028, Sec. 4(i)(j)).

(2) Refer to the NIST EO 14028, Improving the Nation’s Cybersecurity web site at *https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity* for guidance. (L, M, H)

#
#
#
#
#
#
#
#

#
#
#

#
#
#

#
#
#
#

#
#
#

#
#
#

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

#
#
#
#
#
#
#
#
#

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

#
#

#
#
#
#
#
#
#
#

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

#
#

#
#
#
#
#
#
#

#
#
#

#
#

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

#
#
#
#
#

#
#

#
#
#
#
#

#
#
#

#
#

#
#

#

#
#

#
#
#
#
#
#

#
#
#

#
#
#
#

#

#
#

#
#
#

#
#
#

#
#
#
#
#
#
#
#

#
#

#
#

#
#

#
#
#

#
#

#
#

#
#
#

#
#
#
#
#
#

#
#
#
#
#
#
#

#
#

#
#
#

#
#
#

#
#
#
#

#
#
#

#
#

#
#
#
#

#
#

#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#

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

#
#

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

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

#

#
#
#
#

#
#
#
#

#
#
#

#
#
#
#
#
#

#
#
#
#

#
#
#

#
#
#

#
#
#

#
#
#
#
#

#
#
#
#
#
#
#
#
#

#
#
#

#
#

#
#

#
#

#
#
#
#
#
#
#

#
#
#

#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#

#
#

#
#
#

#
#
#
#
#

#
#

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

#
#
#
#

#
#
#

#
#
#

#
#
#
#
#
#
#
#

#

#
#
#
#
#
#
#
#
#
#

#
#
#

#
#
#

#
#
#
#

#
#

#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#

#
#

#
#

#
#
#
#
#
#
#
#

#
#

#
#
#
#
#

#
#

#
#
#
#
#
#

#
#

#
#
#
#
#
#
#

#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#

#
#
#

#
#

#

#
#
#
#
#

#
#
#

#
#
#
#
#

#
#
#
#

#

#
#
#
#

#
#
#
#

#
#
#
#
#

#
#
#
#

#
#
#

#
#

#
#
#

#
#

#
#

#
#
#
#
#

#
#
#

#

#
#
#
#
#
#
#
#
#

#
#
#

#
#
#
#

#
#
#

#
#
#

#
#

#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#

#
#

#
#
#
#
#

#
#
#
#

#
#

#

#
#
#
#

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

#
#
#
#

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

#
#
#
#
#

#
#
#

#
#
#
#

#
#

#
#
#
#
#
#
#
#

#
#
#
#

#
#
#

#
#

#
#

#
#
#
#
#
#
#
#

#
#
#
#
#

#
#

#
#
#

#
#

#
#

#
#

#
#

#

#
#
#

#

#
#
#
#
#
#

#
#

#
#
#
#
#
#
#
#
#

#
#

#
#

#
#
#

#
#
#

#
#
#
#

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

#
#

#
#
#
#
#

#
#
#
#
#
#
#

#
#
#
#

#
#

#
#
#

#

#
#
#
#
#
#
#
#

#
#
#

#
#

#

#
#
#

#
#
#
#
#
#

#
#

#
#
#

#
#

#

#
#
#

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

#
#
#

#

#
#
#
#

#
#
#
#

#
#
#
#
#
#
#

#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#

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

#
#

#
#

#
#

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

#
#
#

#
#
#
#
#
#
#

#
#
#

#
#
#
#

#
#
#
#
#
#
#

#
#
#

#
#

#
#

#
#

#
#
#
#

#
#

#
#

#
#
#

#
#
#
#

#
#

#
#

#
#

#
#
#
#
#
#

#
#
#

#

#
#

#
#

#
#
#

#
#

#
#
#
#
#

#

#
#

#
#
#

#
#

#
#
#
#
#

#
#
#

#
#
#
#

#
#
#

#
#

#
#
#
#

#
#

#
#
#

#
#
#
#

#
#
#
#
#
#
#
#

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

#
#
#
#
#

#
#
#

#
#
#
#
#

#
#

#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#

#
#
#

#
#
#
#
#

#
#
#

#
#

#
#

#
#
#
#

#

#
#
#
#

#
#
#

#
#
#

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

#
#

#
#
#
#
#

#
#

#
#
#

#
#
#
#
#
#
#
#
#
#

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

#
#
#

#
#
#
#
#

#
#

#
#
#
#
#
#
#
#

#
#

#
#
#

#
#
#

#
#
#
#

#
#
#

#
#
#
#

#
#

#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#

#
#

#
#
#
#
#
#
#
#

#
#
#
#

#
#

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

#
#

#
#
#
#
#
#
#
#

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

#
#

#
#
#
#

#
#
#

#
#
#

#
#

#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

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

#
#
#
#

#
#
#
#

#
#
#
#

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

#
#
#

#
#
#

#

#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#

#
#
#

#
#

#
#
#

#
#

#
#
#

#
#
#

#
#
#

#
#

#
#
#
#

#
#

#
#
#

#
#

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

#
#
#

#
#
#
#
#
#
#
#
#
#

#

#
#
#
#
#
#

#
#
#
#
#
#
#
#

#
#

#
#
#
#
#

#

#
#
#

#
#

#
#
#

#
#

#

#
#
#
#
#
#

#
#
#

#
#
#
#

#

#
#
#

#
#
#

#
#
#
#
#

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

#
#
#

#
#
#

#
#

#
#

#
#
#

#

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

#
#
#
#
#
#
#

#
#
#
#
#
#

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

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

#
#
#
#

#
#
#
#

#
#

#
#
#
#
#
#

#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#

#
#
#

#
#
#
#

#

#
#
#
#
#

#
#
#
#
#
#
#
#

#
#

#
#
#
#
#
#
#

#
#
#
#
#

#
#
#

#
#
#

#
#
#

#
#
#
#
#

#
#
#
#
#

#
#
#
#
#
#

#
#
#
#
#

#
#

#
#

#
#
#

#
#
#
#

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

#
#
#

#
#
#
#
#
#

#
#
#
#
#
#

#
#
#

#
#
#
#
#

#
#
#
#
#
#

#
#
#

#
#
#
#

#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#

#
#
#
#
#
#
#
#

#
#
#

#
#

#
#

#
#
#
#
#

#
#

#
#
#
#
#
#

#
#
#

#
#
#
#
#

#
#

#
#

#
#
#
#
#
#
#

#
#
#
#
#

#
#
#
#
#
#
#
#
#

#
#
#
#
#

#
#
#
#
#
#
#
#

#

#

#
#
#
#
#

#
#
#
#
#

#
#
#

#
#
#
#

#
#
#
#
#

#
#
#

#

#
#
#
#

#
#
#

#
#
#

#
#
#
#
#
#
#

#
#
#
#
#
#
#
#

#

#
#
#

#
#
#
#
#

#
#
#

#
#

#
#
#
#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#
#
#

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

#
#
#

#
#
#

#
#
#
#
#
#
#

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

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

#
#
#
#
#
#

#
#

#
#
#
#
#
#
#

#
#
#

#

#
#
#
#
#

#
#
#
#
#

#
#
#
#
#

#
#
#

#
#
#

#
#
#
#

#
#
#
#
#

#
#

#
#
#

#
#
#

#
#
#
#

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

#
#

#
#
#
#
#

#
#

#
#
#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#
#

#
#
#
#
#

#
#

#

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

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

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

#
#
#
#

#
#
#

#
#
#
#
#

#
#
#

#
#
#
#
#
#

#
#
#
#

#
#
#

#
#

#
#
#
#

#
#
#
#
#

#
#
#
#
#
#
#

#
#
#
#
#
#

#

#
#
#
#
#
#
#

#
#

#
#
#
#
#

#
#

#
#

#
#

#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#

#
#
#

#
#

#
#
#

#
#
#
#
#
#
#

#
#
#
#
#
#
#

#
#

#
#

#

#
#
#
#

#
#
#
#
#
#
#

#
#

#
#
#
#
#
#
#

#
#
#
#
#
#
#

#
#

#
#
#

#
#
#
#
#

#
#

#
#
#
#
#
#

#
#

#
#

#
#
#
#
#

#
#
#

#
#

#
#

#
#
#
#

#
#
#
#
#
#

#
#
#

#
#

#
#

#
#
#

#

#
#
#
#
#
#
#
#
#

#
#
#

#
#
#
#
#

#
#
#
#

#
#
#

#
#

#
#

#

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

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

#
#

#
#

#
#
#
#

#
#

#
#
#

#
#

#
#
#
#
#
#
#

#
#
#

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

#
#
#
#
#
#
#

#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#

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

#
#
#
#

#
#
#
#
#
#
#

#
#
#

#
#

#
#
#

#
#
#
#
#
#
#

#
#
#
#

#
#

#
#

#

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

#
#

#
#

#
#

#
#
#

#
#
#

#
#
#
#
#

#
#
#
#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#

#
#

#
#
#
#
#
#
#
#

#
#
#
#
#
#
#

#
#
#
#
#

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

#
#
#

#
#
#

#
#
#

#
#

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

#
#

#

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

#
#

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

#
#
#
#

#
#
#
#
#
#

#
#

#
#

#
#
#
#
#

#
#
#

#

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

#
#

#
#
#

#

#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#

#
#

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

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

#

#
#
#
#
#
#
#
#
#
#

#
#

#
#
#
#
#
#
#
#
#
#
#

#
#

#
#

#
#
#
#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#
#
#
#

#
#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#
#
#
#

#
#

#
#

#
#
#

#

#
#
#

#
#
#
#

#
#
#

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

#
#
#
#

#
#

#
#

#
#
#
#

#
#
#

#

#
#
#
#
#
#
#
#
#

#
#
#

#
#

#
#
#
#

#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#

#

#
#

#
#
#
#

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

#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#

#
#
#
#
#
#

#

#
#
#
#
#
#

#
#
#
#

#
#
#

#
#
#

#
#
#
#
#
#

#
#

#
#
#
#

#
#
#
#
#
#

#
#

#

#
#

#

#
#
#
#
#

#
#

#
#
#
#
#

#
#

#

#
#
#
#
#
#
#

#

#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

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

#
#

#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#

#
#
#

#
#
#

#
#

#
#
#

#

#
#
#
#
#
#
#
#

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

#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#

#
#
#
#

#
#

#
#
#
#
#
#
#
#
#

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

#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#

#
#
#
#
#

#
#

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

#
#
#
#
#
#
#
#

#

#
#
#

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

#
#
#
#
#

#
#
#

#
#
#

#
#
#
#

#
#
#

#
#
#
#
#
#
#
#

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

#
#
#

#
#
#
#

#
#
#
#

#
#
#
#
#

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

#
#
#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

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

#
#
#
#

#
#
#

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

#
#
#
#
#
#
#
#

#
#

#
#
#
#
#

#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#

#
#
#
#
#
#

#
#
#
#

#
#
#
#
#

#
#
#
#

#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#

#
#

#
#
#

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

#
#
#
#

#
#

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

#
#
#
#
#
#

#
#

#
#
#
#
#
#

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

#
#

#
#
#
#
#

#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#

#
#

#
#
#
#
#
#
#
#
#
#

#
#

#
#
#
#
#
#

#
#
#

#
#

#
#
#
#

#
#

#
#
#

#
#
#

#
#
#
#
#
#
#
#

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

#
#

#
#
#
#
#
#
#

#
#
#

#
#
#

#
#
#
#
#
#
#
#

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

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

#
#
#

#
#
#
#

#
#
#

#
#
#

#
#
#

#
#
#
#

#
#
#
#
#

#
#
#

#
#
#
#

#
#

#
#
#

#
#

#
#
#
#
#
#

#
#
#
#
#

#
#
#
#
#

#

#
#
#
#
#
#
#

#
#
#

#
#
#

#
#
#
#
#
#
#
#
#

#

#
#
#
#
#
#

#
#
#
#
#
#
#
#

#
#

#
#

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

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

#
#

#
#

#
#
#

#
#
#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#
#
#
#
#

#
#

#
#

#
#
#
#
#
#
#
#

#
#

#
#
#
#
#

#
#
#
#
#
#
#
#
#

#
#
#
#
#

#
#

#
#
#

#
#
#
#
#

#
#

#
#
#
#
#

#
#
#

#
#
#
#

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

#
#
#

#
#
#

#
#
#

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

#
#
#
#
#
#
#
#
#

#
#

#
#
#
#
#
#
#
#
#
#

#
#
#

#
#

#
#
#
#
#

#
#

#
#

#
#
#

#
#

#
#
#
#

#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#

#
#
#
#
#
#
#
#

#
#
#
#
#
#

#
#
#

#
#

#
#
#

#
#
#
#
#
#
#

#
#

#
#
#
#

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

#
#
#

#
#
#
#

#
#

#
#
#
#
#
#

#
#
#
#
#
#
#

#
#
#

#
#
#

#
#

#
#
#
#
#

#

#
#
#
#

#

#
#
#
#
#
#

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

#
#
#
#
#

#

#
#
#
#

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

#
#
#
#
#
#
#
#
#
#

#
#
#
#

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

#
#

#
#

#
#

#
#
#

#
#
#

#
#

#
#
#
#
#
#

#
#

#

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

#
#
#
#
#
#
#

#
#

#
#
#

#
#
#

#
#
#

#
#
#
#

#
#

#
#

#
#

#
#

#
#
#
#

#
#
#
#

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

#
#

#
#

#
#
#
#
#

#

#
#

#
#
#
#
#
#
#
#

#
#

#
#
#

#
#
#
#
#
#
#

#
#
#
#

#
#

#
#
#
#
#
#

#
#

#
#
#

#
#
#
#

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

#
#

#
#
#
#

#
#
#
#
#

#
#
#
#
#
#

#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#

#
#
#
#
#
#

#
#

#
#
#
#
#
#
#
#
#

#
#

#
#
#

#
#
#
#
#
#
#
#
#

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

#
#
#

#
#
#

#
#
#

#

#
#
#
#
#
#
#

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

#
#

#
#
#
#
#

#
#
#

#
#

#
#
#

#

#
#
#
#
#
#
#
#
#

#
#
#

#
#

#
#
#
#

#

#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

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

#
#

#
#
#

#
#
#
#

#
#
#
#
#
#
#
#
#

#
#

#
#
#
#

#
#
#

#
#
#
#
#
#
#

#
#
#

#
#
#

#
#
#
#

#
#
#
#
#
#
#
#

#
#
#
#

#

#
#
#
#
#
#
#
#
#

#
#

#
#
#

#
#

#
#
#
#
#

#

#
#
#
#
#
#
#
#
#

#
#
#
#
#

#
#
#
#

#
#
#

#
#

#
#
#
#
#

#
#

#
#

#
#
#
#
#

#

#
#

#
#
#
#
#

#
#
#
#

#

#

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

#
#

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

#
#
#

#
#
#

#
#
#

#

#
#

#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#

#

#
#
#
#
#
#
#
#

#
#

#
#

#
#
#
#

#

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

#
#
#
#
#
#
#
#
#

#
#
#

#

#
#
#
#

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

#
#
#

#
#
#

#
#

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

#
#

#
#
#
#
#
#

#
#
#
#

#
#
#
#
#
#
#

#

#
#
#
#
#

#
#
#

#
#

#
#
#

#
#
#
#
#
#
#

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

#
#

#
#
#
#
#

#
#

#
#
#
#

#
#

#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#

#
#
#
#
#
#
#
#
#

#
#
#
#
#

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

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

#

#
#
#
#
#
#
#
#
#

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

#
#
#

#
#
#

#

#
#
#
#

#
#
#
#
#
#

#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#

#
#

#
#

#
#
#
#
#

#
#
#
#
#
#

#
#
#

#
#

#
#
#
#

#
#

#
#

#
#
#
#
#
#
#
#
#

#
#
#

#
#
#
#
#
#

#
#

#
#
#
#
#

#
#
#

#
#
#
#
#

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

#
#
#
#

#
#
#
#
#
#
#
#

#
#

#
#

#
#
#
#
#
#
#
#
#

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

#
#

#
#
#
#

#
#
#

#
#

#
#
#
#
#

#
#

#
#
#
#
#
#
#
#
#

#
#

#
#

#
#
#

#
#

#
#
#

#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#

#
#
#
#

#
#
#
#
#
#

#
#
#

#
#
#

#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#

#
#
#
#
#
#

#
#
#
#
#
#

#
#

#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#

#
#

#
#
#

#
#
#
#
#
#
#
#

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

#
#
#

#

#

#
#
#

#

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

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

#
#
#
#
#
#
#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

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

#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#

#
#

#
#
#
#
#
#

#
#

#
#

#
#
#
#

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

#
#
#

#
#
#

#
#
#
#
#

#
#
#

#

#
#

#
#

#
#
#
#
#

#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#

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

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

#
#
#

#
#
#

#
#
#
#
#
#

#
#
#
#

#
#
#

#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

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

#
#
#

#
#
#
#
#
#
#
#

#
#

#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#

#
#
#
#
#
#
#

#
#

#
#
#
#
#

#
#
#

#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#

#
#
#
#

#
#
#

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

#
#
#
#

#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#

#

#
#
#
#

#
#
#
#
#
#
#

#
#
#
#
#
#

#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#

#
#

#
#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#

#
#

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

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#

#
#
#

#
#

#
#
#
#

#

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

#
#
#
#

#
#
#
#
#
#
#
#
#

#
#

#
#

#
#
#
#
#

#
#
#

#
#

#
#
#

#
#
#
#
#
#

#
#

#
#
#
#

#

#
#
#

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

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

#
#
#
#
#

#
#

#

#
#
#
#
#
#

#
#
#
#

#
#
#
#
#
#
#
#

#
#
#
#

#
#

#
#

#
#

#
#

#

#
#
#

#
#
#

#
#
#
#

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

#
#
#

#
#
#
#
#
#
#
#
#
#
#

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

#

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

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

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

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

#
#
#
#
#
#

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

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

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

#
#
#

#
#
#
#
#
#
#
#
#
#
#

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

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

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

#
#
#
#

#
#
#

#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#

#
#

#
#

#

#
#
#

#
#
#

#
#
#

#
#
#
#
#
#
#
#
#

#
#
#

#
#
#

#
#
#
#

#
#
#
#

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

#
#
#

#
#
#
#
#

#
#

#
#
#
#
#
#
#

#

#
#
#
#
#
#
#
#
#

#
#
#

#
#

#

#
#
#
#

#
#
#
#
#
#
#
#

#
#
#
#
#
#
#

#
#

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

#
#
#

#
#

#
#
#
#

#

#
#
#
#
#
#
#
#
#

#
#

#
#
#
#

#
#

#
#

#
#

#

#
#
#
#
#
#
#

#
#
#
#

#
#
#
#
#
#
#

#
#
#

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

#
#
#

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

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

#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#

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

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

#

#
#
#
#
#
#

#
#
#
#
#

#
#
#
#
#

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

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

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#

#
#
#
#

#
#
#
#

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

#

#
#
#
#
#

#
#
#
#
#

#
#
#

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

#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#

#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#

#
#
#
#
#

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

#
#
#
#
#
#
#
#
#

#

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

#
#
#
#
#
#
#
#
#
#
#

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

#

#
#
#
#

#
#
#
#
#
#
#

#

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

#
#
#
#
#
#
#

#
#

#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#

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

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

#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#

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

#

#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#

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

#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#

#

#
#
#
#
#
#
#
#

#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#

#
#
#
#
#
#
#
#
#

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

#

#
#
#
#
#
#
#
#

#
#
#
#
#
#

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

#

#
#
#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#

#
#
#
#
#
#
#

#
#
#
#
#
#

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

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

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

#

#
#
#

#
#
#
#
#
#
#
#
#
#

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

#
#
#

#
#
#

#
#
#
#
#
#
#
#
#

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

#
#

#
#
#
#
#

#
#
#

#
#
#
#
#
#

#
#

#
#

#
#
#
#
#
#

#
#
#
#

#

#
#
#
#
#
#

#
#
#
#
#
#
#
#

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

#
#

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

#
#
#
#
#

#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#

#
#
#
#
#
#

#
#

#
#
#

#
#
#
#
#

#
#

#
#
#
#
#

#
#
#
#
#
#
#

#
#
#
#

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

#
#
#
#
#
#
#
#

#

#
#

#
#
#
#

#
#
#
#
#
#
#

#

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

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

#
#
#
#
#

#
#

#
#
#
#

#
#
#
#
#
#

#
#
#

#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#

#
#
#
#

#
#

#
#
#
#

#
#

#
#
#

#
#
#

#
#

#
#
#
#
#
#
#

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

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

#
#
#

#
#
#

#

#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#

#
#
#
#
#

#
#
#
#
#

#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#

#
#
#
#
#
#
#
#

#

#
#
#
#
#
#
#
#

#
#

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

#
#

#
#
#

#
#

#
#

#
#

#
#
#

#
#
#
#

#
#
#
#
#
#
#

#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#

#
#
#
#
#
#

Any line marked with a #
is for **Official Use Only**

#
#
#
#
#
#
#
#
#
#

#
#
#

#

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

#
#
#

#
#
#

#
#
#
#

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

#
#
#
#
#
#
#
#

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

#
#
#
#
#
#

#
#
#

#

#
#
#
#
#
#

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

#
#

#
#
#
#
#
#
#
#
#
#
#

#
#

#

#
#
#

#

#
#
#

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

#
#

#
#
#
#

#
#
#
#

#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#

#
#
#
#
#

#
#
#

#
#
#

#
#
#

#
#

#
#
#
#
#
#
#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#
#
#

#
#

#
#

#
#
#
#
#
#
#
#
#
#
#

#
#

#
#
#
#
#
#

#
#
#
#
#
#

#

#
#
#
#

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

#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#
#
#
#
#

#

#
#
#
#
#

#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#

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

#
#
#
#

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

#
#
#

#
#
#

#
#
#
#
#

#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#

#

#
#
#
#
#
#
#

#
#

#
#

#
#
#
#
#
#

#
#
#

#

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

#
#
#
#

#
#
#
#
#
#
#
#
#

#
#

#
#

#
#

#
#
#
#
#
#
#
#

#
#
#
#
#

#
#
#

#

#
#
#
#
#

#
#
#

#
#

#
#
#
#
#

#
#
#

#
#
#
#

#
#

#
#
#
#

#
#

#
#
#

#
#
#
#

#
#
#
#
#
#

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

#
#

#
#
#
#

#
#
#
#

#
#
#

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

#
#
#

#
#
#

#
#
#

#
#

#
#
#

#

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

#
#
#
#
#
#
#
#

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

#
#
#

#
#
#
#
#

#
#
#

#
#
#

#
#
#

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

#
#
#

#

#
#
#
#
#
#
#
#
#

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

#
#
#
#
#
#
#
#

#
#
#

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

#
#
#
#
#
#

#
#
#

#
#
#
#

#
#
#
#
#

#
#
#
#
#
#

#
#
#

#
#

#
#
#
#
#
#
#
#

#
#

#
#
#
#
#

#
#

#
#

#
#
#

#
#
#
#
#

#
#

#

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

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

#
#
#

#
#

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

#
#
#

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

#
#
#

#

#
#
#
#
#

#

#
#
#

#
#
#

#
#
#

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

#
#
#
#
#
#
#
#

#
#

#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#

#
#

#
#
#
#
#
#
#

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

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

#
#
#

#
#
#

#
#
#
#
#

#
#
#
#

#
#
#

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

#
#
#

#
#
#

#
#

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

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

#
#

#
#
#
#
#
#
#

#
#

#
#
#
#
#

#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

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

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

#

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

#
#

#
#
#
#

#
#
#
#
#

#
#
#
#
#
#
#
#

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

#
#
#
#
#
#
#

#
#
#

#
#

#
#

#
#

#
#
#

#
#
#
#

#
#
#

#
#
#
#
#
#
#

#
#

#
#

#
#
#
#
#

#
#

#
#

#
#

#
#
#
#
#

#
#
#

#
#

#
#
#
#
#
#

#
#
#

#
#
#
#

#
#
#
#
#

#
#
#
#

#
#
#
#
#
#
#

#
#
#
#

#
#
#

#
#
#
#
#
#

#
#
#
#

#
#
#

#
#
#

#
#

#
#
#
#

#
#

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

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

#
#

#
#
#
#
#
#
#
#
#

#

#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#

#
#
#

#
#
#
#
#
#

#
#
#

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

#
#

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

#
#

#
#
#
#
#
#
#

#
#

#
#
#
#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#

#
#
#

#
#

#

#
#
#
#
#
#

#
#

#
#

#

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

#
#

#
#
#
#
#
#
#
#

#
#

#
#
#
#
#

#
#
#
#
#
#
#
#

#
#
#

#
#
#

#
#
#
#
#

#
#
#
#
#
#
#

#
#
#

#
#

#
#
#

#
#
#
#

#
#
#

#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#

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

#
#
#

#
#

#
#
#

#
#

#
#
#

#
#
#
#
#
#
#

#
#

#
#
#
#
#
#

#
#

#
#
#

#
#

#
#

#
#
#

#
#

#
#
#

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

#
#

#
#
#
#
#
#

#
#
#
#

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

#
#

#
#
#
#
#
#

#
#
#

#
#

#
#
#
#
#

#
#

#
#
#

#
#
#
#

#

#
#
#
#
#
#
#
#
#
#

#
#
#

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

#
#
#
#
#
#
#
#
#

#
#

#
#

#
#
#
#

#
#

#
#

#
#
#
#
#

#
#
#
#

#
#

#
#
#

#
#
#
#
#

#
#

#

#

#
#
#
#
#
#
#

#
#

#

#

#
#
#
#
#

#
#
#

#

#
#
#
#

#
#
#
#
#
#
#
#
#

#
#

#
#
#
#
#
#

#

#
#
#

#
#
#
#

#

#
#

#
#

#
#

#
#

#
#
#

#
#
#

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

#
#
#

#
#
#
#
#
#

#
#
#
#

#
#
#
#
#

#
#

#
#
#

#
#
#
#
#
#

#
#
#

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

#
#
#

#
#
#
#
#
#

#
#

#
#
#
#
#
#

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

#
#
#

#
#

#
#
#

#
#

#
#

#
#
#
#

#
#

#
#

#
#

#
#
#

#
#
#
#
#
#
#
#
#

#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#

#
#
#

#
#

#
#

#
#

#
#

#

#
#
#
#
#

#
#
#

#
#
#
#
#
#
#

#
#

#
#

#
#
#

#
#

#
#
#

#
#

#
#
#
#
#
#
#
#

#
#
#

#
#

#
#
#

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

#
#
#

#
#
#

#
#
#

#
#

#
#
#
#
#

#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#

#
#
#

#
#
#
#

#
#
#
#
#

#
#

#
#

#
#
#
#
#

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

#
#
#
#
#
#

#
#
#

#
#
#

#
#
#

#
#

#
#
#

#
#
#
#
#
#
#
#
#
#
#

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

#
#
#
#

#
#

#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#

#
#
#
#
#

#
#
#

#
#
#
#
#

#
#
#
#
#

#
#

#
#
#

#
#

#
#

#
#
#
#

#
#

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

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

#
#
#
#
#
#
#
#

#
#
#
#

#
#
#
#
#
#

#
#

#
#
#

#
#
#

#
#
#
#
#

#
#
#
#
#
#

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

#
#
#

#
#
#
#
#
#

#
#
#
#
#
#
#

#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#
#
#
#

#
#
#

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

#
#
#
#
#
#

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

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#
#
#

#
#
#
#
#

#
#
#
#

#
#
#
#
#
#
#

#
#
#
#
#
#
#
#

#
#
#

#
#
#

#
#

#

#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#

#
#

#
#
#

#
#
#

#
#

#
#
#
#

#
#

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

#
#
#
#

#
#
#
#
#

#
#
#
#
#
#
#
#
#

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

#
#
#
#
#
#

#
#

#
#

#
#
#
#
#
#
#
#
#
#

#
#

#
#
#
#
#
#
#

#
#
#
#
#

#
#
#

#
#
#

#
#
#

#
#
#
#
#

#
#

#
#
#
#
#
#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#

#
#
#
#
#
#

#
#
#
#
#

#
#
#
#
#

#
#
#
#
#

#
#
#

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

#
#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#

#
#
#
#
#

#
#

#
#
#

#
#
#
#
#
#

#
#

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

#
#
#
#
#
#

#
#
#

#
#

#
#
#
#
#
#

#
#
#

#
#
#
#
#

#
#
#
#
#
#

#
#
#

#
#
#
#

#
#
#

#
#

#
#

#
#

#
#
#

#
#
#
#

#
#

#
#
#
#
#

#
#
#
#

#
#

#
#
#
#

#
#
#

#
#
#

#
#
#
#
#
#
#
#
#
#

#
#

#
#

#
#

#
#

#
#
#

#
#
#

#
#

#

#

#
#
#
#
#

#
#

#
#

#
#

#
#
#
#
#

#
#
#
#
#
#
#

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

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

#
#
#

#
#

#
#
#
#
#
#
#
#
#
#

#
#

#

#
#

#
#
#
#

#
#
#
#
#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#
#
#
#
#
#

#
#
#
#

#
#
#

#
#
#
#
#

#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#

#
#
#
#
#
#

#

#
#
#
#
#
#
#

#
#

#
#

#
#
#

#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#

#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#

#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#

#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#

#
#

#
#

#
#

#
#
#
#
#
#
#

#
#

#
#

#
#
#
#
#

#
#

#
#
#
#
#

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

#
#
#

#
#
#
#

#
#
#
#

#
#

#
#

#
#
#

#
#
#

#
#

#
#
#

#
#
#

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

#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#

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

#
#
#
#

#
#
#
#

#
#
#

#

#
#
#
#

#
#
#

#
#
#
#

#
#
#
#
#
#
#
#
#

#
#
#
#

#
#
#
#
#
#
#
#

#
#
#
#

#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

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

#
#
#

#
#
#

#
#
#

#
#
#
#
#
#
#
#
#

#
#

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

#
#

#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#

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

#

#
#
#

#
#
#
#
#
#

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

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

#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#

#
#
#

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

#
#
#
#

#
#

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

#
#
#
#

#
#
#

#
#
#

#
#
#
#

#
#

#
#
#
#

#
#
#
#

#
#
#
#
#
#

#
#

#
#

#
#
#

#
#

#
#
#
#

#
#

#
#

#
#
#
#
#
#
#
#

#
#
#
#
#
#

#
#
#
#
#
#

#
#
#
#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

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

Exhibit 10.8.1-1 (12-12-2023)
Terms and Acronyms

0-9

3PAO - Third Party Assessor Organization

A

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

1) Obtain and use information and related information processing services, and

2) Enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).

Account Manager - User account management involves the process of requesting, establishing, issuing, modifying, and closing user accounts; tracking users and their access authorization and privileges.

Accountability - The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports non-repudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action. Principle that an individual is entrusted to safeguard and control equipment, keying material, and information and is answerable to proper authority for the loss or misuse of that equipment or information.

ACIO - Associate Chief Information Officer

Adequate Security - Security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.

Note: This includes assuring that systems operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

Administrative Furlough - A planned event by an agency which is designed to absorb reductions necessitated by downsizing, reduced funding, lack of work, or any budget situation other than a lapse in appropriations. Furloughs that would potentially result from sequestration would generally be considered administrative furloughs. (OPM.gov)

Advanced Persistent Threat (APT) - An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat:
(i) Pursues its objectives repeatedly over an extended period of time,
(ii) Adapts to defenders' efforts to resist it, and
(iii) Is determined to maintain the level of interaction needed to execute its objectives.

AIFIS - Automated Integrated Fingerprint Identification System

AIS - Automated Information System

AP - Authority and Purpose

APNSA - Assistant to the President and National Security Advisor

Exhibit 10.8.1-1 (Cont. 1) (12-12-2023)
Terms and Acronyms

Application Developers - Refer to Developers

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 operational procedures.

Audit Trail - A chronological record that reconstructs and examines the sequence of activities surrounding or leading to a specific operation, procedure, or event in a security relevant transaction from inception to final result.

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 or token).

Authorization - Access privileges granted to a user, program, or process or the act of granting those privileges.

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

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

Authorized Personnel - Applies to all IRS personnel cleared with a requirement to access information systems (IS) for performing or assisting in a lawful and authorized government function.

Authorizing Official (AO) - Official with the authority to formally assume responsibility for operating an 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 system operations. Previously known as the Designated Approving Authority.

Availability - Ensuring timely and reliable access to and use of information.

Awareness (Information Security) - Activities which seek to focus an individual’s attention on an (information security) issue or set of issues.

B

BIA - Business Impact Analysis

BEARS - Business Entitlement Access Request System - Use BEARS to request access to and perform recertifications on subapps (entitlements) which have been migrated from OL5081.

Binding - The process of associating two related elements of information.

Binding Operational Directive (BOD) - A compulsory direction issued by CISA to federal, executive branch, departments and agencies for the purposes of safeguarding federal information and systems.

Exhibit 10.8.1-1 (Cont. 2) (12-12-2023)
Terms and Acronyms

BGP - Border Gateway Protocol

BIOS - Basic Input/Output System

Blacklist - A list of discrete entities, such as hosts or applications, that have been previously determined to be associated with malicious activity.

Bureau(s) and IRS Head - Refer to Department

Bot - A bot also known as software robot (web robot or chat robot) is a software program or an application that runs repetitive tasks at a higher rate than would be possible for human alone.

Breach - The loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where (1) a person other than an authorized user accesses or potentially accesses personally identifiable information or (2) a person accesses or potentially accesses personally identifiable information for an unauthorized purpose (i.e., a purpose unrelated to their official duties/functions). (OMB M-17-12, Treasury IR Plan)

Note: A breach is a type of incident.

Business Partner - A term used to denote an entity with which another entity has some form of alliance. This relationship may be a highly contractual, exclusive bond in which both entities commit not to ally with third parties.

BYOD - Bring Your Own Device

C

CASB - Cloud Access Security Broker

CAVP - Cryptographic Algorithm Validation Program

CD - Compact Disk

CDM - Continuous Diagnostics and Mitigation

CD-ROM - Compact Disc - Read Only Memory

Certificate - Refer to Digital Certificate

Certification Authority (CA) - A trusted entity in a public key infrastructure (PKI) that issues and revokes certificates exacting compliance to a PKI policy.

CGI - Common Gateway Interface

CIA - Confidentiality, Integrity, and Availability

CIO - Chief Information Officer

CIP - Critical Infrastructure Protection

CIS - Center for Internet Security

CISO - Chief Information Security Officer

Exhibit 10.8.1-1 (Cont. 3) (12-12-2023)
Terms and Acronyms

Classified Information - Information that has been determined pursuant to EO 13556 or any predecessor order to require protection against unauthorized disclosure and is marked to indicate its classified status when in documentary form.

Cloud Computing - A model for enabling on-demand network access to a shared pool of configurable IT capabilities/ resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three cloud service delivery models (Software as a Service [SaaS], Platform as a Service [PaaS], and Infrastructure as a Service [IaaS]); and four models for enterprise access (Private, Community, Public, and Hybrid).

CMMI - Capability Maturity Model Integration

CMVP - Cryptographic Module Validation Program

Common Control - A Security control that is inherited by one or more organizational systems. Refer to Security Control Inheritance.

Common Vulnerabilities and Exposures (CVE) - A dictionary of common names (i.e., CVE Identifiers) for publicly known cybersecurity vulnerabilities. CVE's common identifiers make it easier to share data across separate network security databases and tools, and provide a baseline for evaluating the coverage of an organization's security tools. If a report from a security tool incorporates CVE Identifiers, an individual then quickly and accurately access fix information in one or more separate CVE-compatible database to remediate the problem. *https://www.cve.org/About/Overview*.

Common Vulnerability Scoring System (CVSS) - Organizations can reference CVSS in order to work on the action(s) that have the highest priority or present the greatest amount of risk. CVSS can measure how serious a given vulnerability is compared to other vulnerabilities so remediation efforts can be prioritized. The Base metrics produce a score ranging from 0 to 10. *https://www.first.org/cvss/*

Concurrent - Operating or occurring at the same time; running parallel; and/or acting in conjunction.

Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Configuration Control - Process of controlling modifications to hardware, firmware, software, and documentation to protect the system against improper modifications prior to, during, and after system implementation.

Configuration Control Board (CCB) - A group of qualified people with responsibility for the process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an system.

CONOPS - Concept of Operations

Contingency Plan - Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the Continuity of Operations Plan (COOP) or Disaster Recovery Plan for major disruptions.

Continuity of Operations Plan (COOP) - A predetermined set of instructions or procedures that describe how an organization's essential functions will be sustained within 12 hours for up to 30 days as a result of a disaster event before returning to normal operations.

Exhibit 10.8.1-1 (Cont. 4) (12-12-2023)
Terms and Acronyms

Continuous Monitoring - Maintaining an ongoing awareness to support organizational risk decisions.

Controlled Area - A security area which requires one single authentication mechanism to ensure only authorized personnel have unescorted access. (per IRM 10.2.14)

Controlled Unclassified Information (CUI) - A categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under EO 12958, as amended, but requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces “Sensitive But Unclassified” (SBU).

Controlled Unclassified Information (CUI) Program - The CUI Program is the program to standardize CUI handling by all Federal agencies. The Program includes the rules, organization, and procedures for CUI. (NARA, 2002.4)

COR - Contracting Officer’s Representative (previously known as COTR – Contracting Officer’s Technical Representative)

Core hours - The time periods during the workday, workweek, or pay period that are within the tour of duty during which an employee covered by a flexible work schedule is required by the agency to be present for work. (Refer to 5 U.S.C. 6122(a)(1).)

COTS - Commercial Off The Shelf

Countermeasures - Actions, devices, procedures, techniques, or other measures that reduce the vulnerability of a system. Synonymous with security controls and safeguards.

CPIC (Capital Planning Investment Control) - The CPIC Program is a structured, integrated approach to managing Information Technology (IT) investments. It ensures that all IT investments align with the EPA mission and support business needs while minimizing risks and maximizing returns throughout the investment’s lifecycle. The CPIC relies on a systematic approach to IT investment management in three (3) distinct phases: select, control, and ongoing evaluation, to ensure each investment’s objectives support the business and mission needs of the agency.

CPU - Central Processing Unit

Critical Infrastructure Protection (CIP) - System and assets, whether physical or virtual, so vital to the U.S. that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. (CNSSI No. 4009)

Critical Software - Any software that has, or has direct software dependencies upon, one or more components with at least one of these attributes: (As defined by NIST for EO 14028)

- Has direct or privileged access to networking or computing resources;
- Is designed to run with elevated privilege or manage privileges;
- Is designed to control access to data or operational technology;
- Performs a function critical to trust; or
- Operates outside of normal trust boundaries with privileged access.

Cryptographic System - An active software or hardware implementation of one or more cryptographic algorithms that provide one or more of the following services: creation and exchange of encryption keys, encrypted connections, or creation and validation of digital signatures. (OMB M-23-02)

Exhibit 10.8.1-1 (Cont. 5) (12-12-2023)
Terms and Acronyms

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

CSIRC - Computer Security Incident Response Center

CSP - Cloud Service Provider

CUI - Controlled Unclassified Information

Cyber Event - Any observable occurrence in a network or system that may indicate a cyber incident has occurred. (Treasury IR Plan)

Cyber Hygiene Report - A weekly report by CISA, which operates under DHS. Cyber Hygiene leverages the Common Vulnerability Scoring System (CVSS), which is a vulnerability scoring system designed to provide a universally open and standardized method for rating IT vulnerabilities. CVSS helps organizations prioritize vulnerability management strategies by providing a score representative of the base, temporal, and environmental properties of vulnerabilities. (CISA BOD 19-02)

Cybersecurity and Infrastructure Security Agency (CISA) - An operational component under Department of Homeland Security (DHS). Responsible for protecting the Nation’s critical infrastructure from physical and cyber threats. Develops and oversees the implementation of “binding operational directives” and “emergency directives,” which require action on the part of certain federal agencies in the civilian executive branch.

D

Data at Rest - All data in computer storage (e.g., on hard disk drives, CDs/DVDs, floppy disks, thumb drives, PDAs, cellphones, other removable storage media) 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).

DBA - Database Administrator

De-identification - The process by which a collection of data is stripped of information which would allow the identification of the source of the data.

Demilitarized Zone (DMZ) - 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.

Denial of Service (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.)

Department - Within the context of this IRM, the terms department, departments, departmental, etc. refer solely to the IRS unless there is a specific reference to Treasury. The terms “department employee(s)” and “Treasury employee(s)” also refer to the IRS.

Desktop Sharing - A common name for technologies and products that allow remote access and remote collaboration on a person’s computer desktop through a graphical Terminal emulator.

Developer - A general term that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; (iv) and product resellers. Development of systems, components, or services can occur internally within organizations (i.e., in-house development) or through external entities. (CNSSI No. 4009) Refer to IRM 10.8.2 for definitions for program developer/programmer and web developer.

Exhibit 10.8.1-1 (Cont. 6) (12-12-2023)
Terms and Acronyms

DHCP - Dynamic Host Configuration Protocol

DHS - Department of Homeland Security

Digital Certificate - A digital representation of information used in conjunction with a public key encryption system, which at a minimum:

1. Identifies the certification authority issuing it;
2. Names or identifies its subscriber;
3. Contains the subscriber's public key;
4. Identifies its operational period.
5. Is digitally signed by the certification authority issuing it.

DISA - Defense Information Systems Agency

Discretionary Access Control (DAC) - 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).

DLP - Data Loss Prevention

DNS - Domain Name System

Download - To copy or transfer (software, data, character sets, etc.) from a distant to a nearby computer, from a larger to a smaller computer, or from a computer to a peripheral device.

DPI - Deep Packet Inspection

DR - Disaster Recovery

DVD - Digital Video Disc

DVI - Digital Video Interface

E

EAP - Extensible Authentication Protocol

ECC-MTB - Enterprise Computing Center - Martinsburg

eCM - Enterprise Continuous Monitoring

EDR - Endpoint Detection and Response

Education (Information Security) - Education integrates all security skills and competencies of the various functional specialties into a common body of knowledge and strives to produce IT security specialists and professionals capable of forward vision and proactive thinking.

EEPROM - Electrically Erasable Read Only Memory

ELC - Enterprise Life Cycle

Elevated Privileges - Any user right assignment that is above the baseline indicated within this IRM.

Email - Electronic Mail

Exhibit 10.8.1-1 (Cont. 7) (12-12-2023)
Terms and Acronyms

Encryption - Conversion of plaintext to ciphertext through the use of a cryptographic algorithm.

Endpoints - Includes the following: (FY 2017 CIO FISMA Metrics)

- Servers (including mainframe/minicomputers/midrange computers)
- Workstations (desktops laptops, Tablet PCs, and net-books)
- Virtual machines

Enterprise Architecture (EA) - The description of an enterprise's entire set of systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture.

EOps - Enterprise Operations

ESAT - Enterprise Security Audit Trails

EVIDACT - Foundations for Evidence-Based Policymaking Act of 2018 (P.L. 115-435), January 2019

F

FAM - U.S. Department of State Foreign Affairs Manual

Federal Information Security Modernization Act of 2014 (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 systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

FedRAMP - Federal Risk and Authorization Management Program

FICAM - Federal, Identity, Credential and Access Management

FIPS - Federal Information Processing Standards

FIPS-Validated Cryptography - A cryptographic module validated by the Cryptographic Module Validation Program (CMVP) to meet requirements specified in FIPS Publication 140-3 (as amended). As a prerequisite to CMVP validation, the cryptographic module is required to employ a cryptographic algorithm implementation that has successfully passed validation testing by the Cryptographic Algorithm Validation Program (CAVP). (NIST SP 800-53 Rev 5)

Fire Call - Used to represent an emergency, time-critical situation.

FW - Firewall

FMSS - Facilities Management and Security Services

FOIA - Freedom of Information Act

Foreign Intelligence Information - This type of information relates to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but does not include counterintelligence (with the exception of information on international terrorist activities). Contact the Special Assistant to the Secretary (National Security) regarding security policies and procedures relating to IT that processes, stores, or transmits foreign intelligence information.

FTI - Federal Taxpayer Information

Exhibit 10.8.1-1 (Cont. 8) (12-12-2023)
Terms and Acronyms

FTP - File Transfer Protocol

G

GAO - Government Accountability Office

Generic account, generic access, generic identification, generic logon - Terms refer to definition and implementation of user authentication information (such as user IDs and passwords) and procedures which are designed so that they do NOT require specific information associated with a unique individual but accept some nonspecific identification information to enable access.

GFE - Government Furnished Equipment

GIS - Geographic Information System

GMT - Greenwich Mean Time

GPS - Global Positioning System

GRS - General Records Schedules

GSA - General Services Administration

GSS - General Support System

H

HIDS - Host Intrusion Detection System

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

High Value Asset (HVA) - Are those assets, Federal systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States' national security interests, foreign relations, economy, or to the public confidence, civil liberties, or public health and safety of the American people. HVAs may contain sensitive controls, instructions, data used in critical Federal operations, or unique collections of data (by size or content), or support an agency's mission essential functions, making them of specific value to criminal, politically motivated, or states-sponsored actors for either direct exploitation or to cause a loss of confidence in the U.S. Government.

HSPD - Homeland Security Presidential Directive

HTTP - Hypertext Transfer Protocol

HTTPS - Hypertext Transfer Protocol Secure

HVAC - Heating, Ventilation, and Air Conditioning

I

I&A - Identification & Authentication

IAM - Identity and Access Management

IANA - Internet Assigned Numbers Authority

ICMP - Internet Control Message Protocol

Exhibit 10.8.1-1 (Cont. 9) (12-12-2023)
Terms and Acronyms

Identification - The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.

IDRS - Integrated Data Retrieval System

IF - Intermediate Frequency

IG - Interim Guidance

IMAP - Internet Message Access Protocol

Impact - The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or system availability.

Incident - An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or a system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies. (Treasury IR Plan)

Incident Handling - The mitigation of violations of security policies and recommended practices.

Incident Response Plan - The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of malicious cyber-attacks against an organization's system(s).

Independent Assessor/Independent Assessment Team - Individuals or groups conducting impartial assessments of systems. Impartiality means that assessors are free from any perceived or actual conflicts of interest regarding development, operation, sustainment, or management of the systems under assessment or the determination of control effectiveness. To achieve impartiality, assessors do not create a mutual or conflicting interest with the organizations where the assessments are being conducted; assess their own work; act as management or employees of the organizations they are serving; or place themselves in positions of advocacy for the organizations acquiring their services. Independent assessments can be obtained from elements within an organization or can be contracted to public or private sector entities outside of organizations.

Information Assurance (IA) - Measures that protect and defend information and systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of systems by incorporating protection, detection, and reaction capabilities.

Information Owner - Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal.

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

Information Sharing Environment (ISE) - 1. An approach that facilitates the sharing of terrorism and homeland security information; or 2. ISE in its broader application enables those in a trusted partnership to share, discover, and access controlled information.

Information System - A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information.

Information System Contingency Plan (ISCP) (previously known as ITCP – IT Contingency Plan) - Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures, or disasters.

Exhibit 10.8.1-1 (Cont. 10) (12-12-2023)
Terms and Acronyms

Information System Owner - Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of a system.

Information System Security Manager (ISSM) - Individual responsible for the information assurance of a program, organization, system, or enclave.

Information System Security Officer (ISSO) - Individual assigned responsibility by the senior agency information security officer, authorizing official, management official, or system owner for maintaining the appropriate operational security posture for a system or program.

Information Technology (IT) - 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.

3) The term “information technology” does not include any equipment that:

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.

InTC - Insider Threat Capability

Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. The property whereby an entity has not been modified in an unauthorized manner.

Interconnected Systems - The direct connection of two or more systems for the purpose of sharing data and other information resources. Refer to NIST SP 800-47 for additional information.

Interconnection Security Agreement (ISA) - An agreement established between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. The ISA also supports a Memorandum of Understanding or Agreement (MOU/MOA) between the organizations.

Internet-Accessible System - Any system that is globally accessible over the public internet. It has a publicly routed IP address or a hostname that resolve publicly in DNS to such an address. It doesn’t pertain to infra-

Exhibit 10.8.1-1 (Cont. 11) (12-12-2023)
Terms and Acronyms

structure that is internal to a bureau network that enables endpoints to be accessible over the internet, systems reachable from the internet but that require special configuration or access controls (e.g., via a Virtual Private Network), or shared services.

I/O - Input/Output

IoT - Internet of Things

IPP - Internet Printing Protocol

IRC - Internal Revenue Code

IRM - Internal Revenue Manual

IRS - Internal Revenue Service

IRS Personnel - Includes employees, consultants, detailees, seasonal/temporary employees, interns, IRS contractors, volunteers, rehired annuitants and non-person entity (NPE) also referred to as robotic process automation(RPA) bots, artificial intelligence workers, digital assistants etc.

ISP - Internet Service Provider

ITL - Information Technology Laboratory

ITIL - Information Technology Infrastructure Library

ITM - Integrated Talent Management

ITSCM - Information Technology Service Continuity Management

IWAM - Internet Web Application Manager

K

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

Key Pair - Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and 2) even knowing one key, it is computationally infeasible to discover the other key.

Keystroke Monitoring - The process used to view or record both the keystrokes entered by a computer user and the computer’s response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails.

L

LBI - Limited Background Investigation

LDAP - Lightweight Directory Access Protocol

Least Privilege - The security objective of granting users only those accesses they need to perform their official duties.

Exhibit 10.8.1-1 (Cont. 12) (12-12-2023)
Terms and Acronyms

Limited Area - A security area to which access is limited to authorized personnel by a two-factor authentication mechanism. All limited areas must either meet secured area criteria (as outlined in IRM 10.2.14) or provisions must be made to store protect able items in appropriate containers during non-duty hours. “Open office” refers to any area which is not designated as a limited area.

Live Data - Production data in use (e.g., electronic, hardcopy); might include SBU information (i.e., PII, PHI, taxpayer data, system-sensitive information).

LOW Impact System - A system in which all three (3) security objectives (i.e., confidentiality, integrity, and availability) are assigned a FIPS 199 potential impact of LOW.

LPD - Line Printer daemon

LSS - Lean Six Sigma

LWOP - Leave Without Pay

M

MAC - Media Access Control

Major Application - An application that requires special attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application.

Note: All federal applications require some level of protection. Certain applications, because of the information in them, however, require special management oversight and should be treated as major. Adequate security for other applications should be provided by security of the systems in which they operate.

Major Incident - Any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. (OMB M-17-05) Refer to also Breach.

Major Information System - A system that requires special management attention because of its importance to an agency mission; its high development, operating, or maintenance costs; or its significant role in the administration of agency programs, finances, property, or other resources.

Management Controls - The security controls (e.g., safeguards or countermeasures) for an system that focus on the management of risk and the management of system security.

Mass Storage Device - A storage drive: hard disk, solid state disk, or USB drive that makes it possible to store and port large amounts of data across computers, servers and within an IT environment.

Maximum Tolerable Downtime (MTD) - The amount of time mission/business processes can be disrupted without causing significant harm to the organization’s mission.

MBI - MODERATE Risk Background Investigation

MEF - Mission Essential Functions

Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA) - A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this guide, an MOU/MOA defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.

Exhibit 10.8.1-1 (Cont. 13) (12-12-2023)
Terms and Acronyms

Mission Critical - Any telecommunications or system that is defined as a national security system (Federal Information Security Modernization Act of 2014 - FISMA) or processes any information the loss, misuse, disclosure, or unauthorized access to or modification of, would have a debilitating impact on the mission of the agency.

MSL - Multiple Security Level

Mobile Code - Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient.

Mobile Computing Device (MCD) - Portable computing and communications device with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices).

MODERATE Impact System - A system in which at least one security objective (e.g., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of MODERATE and no security objective is assigned a FIPS 199 potential impact value of HIGH.

MTIPS - Managed Trusted Internet Protocol Service

Multifactor Authentication - Requires using two or more factors to achieve authentication. Factors include: (i) something you know (e.g., password, personal identification number [PIN]); (ii) something you have (i.e., cryptographic identification device, token); or (iii) something you are (e.g., biometric). Refer to Authenticator.

Multi-Functional Device (MFD) - Also known as MFP (Multi-Function Product/ Printer/ Peripheral), or all-in-one (AIO), is an office machine which incorporates the functionality of multiple devices in one, so as to have a smaller footprint in the business environment, or to provide centralized document management, distribution, and production in a large-office setting. A typical MFP may act as a combination of some or all of the following devices: Printer, Scanner, Photocopier, Fax, Email.

N

NARA - National Archives and Records Administration

National Critical Assets - Assets essential to the minimum operations of the economy and the Government. A project is considered a national critical asset if its failure or inability to function will result in an adverse national impact.

National Information Assurance Partnership (NIAP) - A U.S. government initiative established to promote the use of evaluated systems products and champion the development and use of national and international standards for information technology security. NIAP was originally established as collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) in fulfilling their respective responsibilities under P.L. 100-235 (Computer Security Act of 1987). NIST officially withdrew from the partnership in 2007 but NSA continues to manage and operate the program. The key operational component of NIAP is the Common Criteria Evaluation and Validation Scheme (CCEVS) which is the only U.S. government-sponsored and endorsed program for conducting internationally recognized security evaluations of COTS Information Assurance (IA) and IA-enabled information technology products. NIAP employs the CCEVS to provide government oversight or “validation” to U.S. CC evaluations to ensure correct conformance to the International Common Criteria for IT Security Evaluation (ISO/IEC 15408).

National Security Information - Any agency information (processed by telecommunications and/or systems) that must be protected at all times by procedures established for information that have been specifically authorized under criteria established by an EO or an act of Congress to be kept secret in the interest of national defense or foreign policy. The national security function, operation, or use of which involves: intelligence activi-

Exhibit 10.8.1-1 (Cont. 14) (12-12-2023)
Terms and Acronyms

ties; cryptologic activities related to national security; command and control of military force; equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military/intelligence missions provided that this definition does not apply to a system that is used for routine administrative and business applications (including payroll, finance, logistics and personnel management applications).

NCP - National Checklist Program

NCPR - National Checklist Program Repository

NEF - National Essential Functions

Network Access - Access to an organizational 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).

NFS - Network File System

NIACAP - National Information Assurance Certification and Accreditation Process

NIST - National Institute of Standards and Technology

NSA - National Security Agency

NSTISSI - National Security Telecommunications and Information Systems Security Instruction

Non-government furnished/owned devices - Includes devices owned by contractors and personally-owned.

Non-organizational User - An employee or an individual considered by the organization to have the equivalent status of an employee. Organizational users include contractors, guest researchers, or individuals detailed from other organizations. A non-organizational user is a user who is not an organizational user. (NIST)

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.

Notable Cyber Event - Any deviation from the norm or observable occurrence in a network or system that could have led to a cyber incident but was otherwise mitigated and the source or threat vector poses an ongoing risk to the IRS. (Treasury IR Plan)

NPE - Non- Person Entity is an entity with a digital identity that acts in cyberspace but is not a human actor. This can include organizations, hardware devices, software applications, and information artifacts.

O

OFCIO - Office of the Federal Chief Information Officer (OMB)

OMB - Office of Management and Budget

ONCD - Office of the National Cyber Director

OSS - Open Source Software

OPM - Office of Personnel Management

Operational Controls - The security controls (e.g., safeguards or countermeasures) for a system that primarily are implemented and executed by people (as opposed to systems).

Exhibit 10.8.1-1 (Cont. 15) (12-12-2023)
Terms and Acronyms

Organizational User - An employee or an individual considered by the organization to have the equivalent status of an employee. Organizational users include contractors, guest researchers, or individuals detailed from other organizations. (NIST)

OS - Operating System

P

PACS - Physical Access Control Systems

PBX - Private Branch Exchange

PAM - Privileged Account Management

PCLIA - Privacy and Civil Liberties Impact Assessment

PDF - Portable Document Format

PEAP - Protected Extensible Authentication Protocol

Personally Identifiable Information (PII) - Refer to IRM 10.8.1.4.16.1.3 # Personally Identifiable Information (PII) within this IRM for a definition.

Personal Identification Number (PIN) - An alphanumeric code or password used to authenticate an identity.

Personal Identity Verification (PIV) - The process of creating and using a government wide secure and reliable form of identification for federal employees and contractors, in support of HSPD 12, Policy for a Common Identification Standard for Federal Employees and Contractors.

Personal Identity Verification Card (PIV Card) - Physical artifact (e.g., identity card, “smart” card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) such that a claimed identity of the cardholder may be verified against the stored credentials by another person (human-readable and verifiable) or an automated process (computer-readable and verifiable).

PGLD - Privacy, Governmental Liaison and Disclosure

Physical Separation - Primarily deals with the use of separate devices (firewalls, proxy servers, etc.) with the intent of achieving system segmentation. This can further be augmented by implementing protected distribution system (e.g., steel pipes and guards) and separate sites such as data centers.

Plan of Action and Milestones (POA&M) - A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

POC - Point of Contact

POP - Post Office Protocol

Portable Electronic Device (PED) - Any nonstationary electronic apparatus with singular or multiple capabilities of recording, storing, and/or transmitting data, voice, video, or photo images. This includes, but is not limited to: laptops, cellular telephones, thumb drives, video cameras, and pagers.

PRIVACT - Privacy Act of 1974 (P. L. 93-579)

Private Key - The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.

Privileged Account - An account with elevated privileges. Refer to Elevated Privileges.

Exhibit 10.8.1-1 (Cont. 16) (12-12-2023)
Terms and Acronyms

Program - A program is the process of translating broadly stated mission needs into a set of operational requirements from which specific performance specifications are derived. A program consists of a functional area that supports a Treasury or IRS mission and has associated systems and budgetary resources. A program is an organized set of activities directed towards a common purpose, objective, goal, or understanding proposed by IRS to carry out responsibilities assigned to the organization. Examples of programs include: Compliance, Accounts Management, Submission Processing, production of U.S. currency, asset forfeiture, and bank supervision.

Program Management Controls - Complement the security controls of a system by focusing on the organization-wide information security requirements that are independent of any particular system and are essential for managing information security programs. Organizations are required to implement security program management controls to provide a foundation for the organization's information security program. May also be deemed as common controls by the organization since the controls are employed at the organization level and typically serve multiple systems.

PSO - Personnel Security Office

Public Information - This type of information may be disclosed to the public without restriction, but requires protection against erroneous manipulation or alteration. Example: public Web site.

Public Key - The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.

Public Key Cryptography - Encryption system that uses a public-private key pair for encryption and/or digital signature.

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.

R

RAFT - Risk Acceptance Form and Tool

RAM - Random Access Memory

Recovery Time Objective (RTO) - The overall length of time a system's components can be in the recovery phase before negatively impacting the organization's mission or mission/business functions.

Remediation - The act of correcting a vulnerability or eliminating a threat. Three possible types of remediation are installing a patch, adjusting configuration settings, or uninstalling a software application.

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

Remote Maintenance - Maintenance activities conducted by individuals communicating external to a system security perimeter.

Removable Media - Any type of storage device that can be removed from a computer while the system is still running. Examples include CDs, DVDs, diskettes, and USB drives.

Review - Based on the Government Auditing Standards (2003), the IRS cannot perform self-audits, however, it can perform many of the audit activities in the context of reviews. The IRS reviews are primarily internal control reviews, based on definitions contained within this subsection, and comprised of assessments. This is a significant concept as it should reduce the amount of redundant work possible to conduct a review.

Exhibit 10.8.1-1 (Cont. 17) (12-12-2023)
Terms and Acronyms

RF - Radio Frequency

Risk - A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (1) the adverse impacts that would arise if the circumstance or event occurs, and (2) the likelihood of occurrence.

Note: System-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Risk Assessment - The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of risk assessment is a list of estimated potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF).

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.

Risk Management Framework (RMF) - A structured approach used to oversee and manage risk for an enterprise.

Role-Based Access Control (RBAC) - Access control based on user roles (i.e., a collection of access authorizations a user receives based on an explicit or implicit assumption of a given role). Role permissions may be inherited through a role hierarchy and typically reflect the permissions needed to perform defined functions within an organization. A given role may apply to a single individual or to several individuals.

ROM - Read Only Memory

RPA - Robotic Process Automation is a business process automation technology that automates manual tasks that are largely rules based, structured and repetitive using software robots, also known as bots. RPA tools map a process for a robot to follow which allows the bot to operate in place of a human. A RPA may be attended or unattended.

RPO - Recovery Point Objective

RSSO - Reduced SmartID Sign-On

S

SA&A - Security Assessment & Authorization

Safeguards - Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for a system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Exhibit 10.8.1-1 (Cont. 18) (12-12-2023)
Terms and Acronyms

Sanitization - Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.

SAOP - Senior Agency Official for Privacy

SAR - Security Assessment Report

SAS – Security Assessment Services

SASE - Secure Access Service Edge

SCADA - Supervisory Control and Data Acquisition

SCRM – Supply Chain Risk Management

Scanning - Refer to Vulnerability Scanning

SDWAN - Software-Defined Wide Area Network

SecCM - Security Configuration Management

Security Area - Consists of either controlled or limited areas, which require individual access authentication to gain entry (per IRM 10.2.14)

Security Attribute - An abstraction representing the basic properties or characteristics of an entity with respect to safeguarding information; typically associated with internal data structures (e.g., records, buffers, files) within the system and are used to enable the implementation of access control and flow control policies, reflect special dissemination, handling or distribution instructions, or support other aspects of the information security policy.

Security Authorization - Refer to Authorization.

Security Authorization Boundary - Refer to Authorization Boundary.

Security Authorization Package (formerly Certification & Accreditation) - The evidence provided to the authorizing official to be used in the security authorization decision process. Evidence includes, but is not limited to:

1. The system security plan;
2. The assessment results from the security certification.
3. The plan of action and milestones.

Security Category - The characterization of information or a system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or system would have on organizational operations, organizational assets, individuals, other organizations, and the Nation.

Security Content Automation Protocol (SCAP) - A method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation against a standardized set of security requirements.

Security Control Enhancements - Statements of security capability to 1) build in additional, but related, functionality to a basic control; and/or 2) increase the strength of a basic control.

Security Control Inheritance - A situation in which a system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. Refer to Common Control.

Exhibit 10.8.1-1 (Cont. 19) (12-12-2023)
Terms and Acronyms

Security Controls - The management, operational, and technical control (i.e., safeguards or countermeasures) prescribed for a system to protect the confidentiality, integrity, and availability of the system and its information.

Security Domain - A collection of entities to which applies a single security policy executed by a single authority.

Security Information and Event Management (SIEM) Tool - Application that provides the ability to gather security data from system components and present that data as actionable information via a single interface.

Security Requirements - Requirements levied on a system that are derived from applicable laws, executive orders, directives, policies, standards, instructions, regulations, or procedures, or organizational mission/business case needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Security Role - An individual performing computer security responsibilities in some form or fashion. Refer to IRM 10.8.2 for additional roles and responsibilities guidance.

Security Test & Evaluation (ST&E) - Examination and analysis of the safeguards required to protect a system, as they have been applied in an operational environment, to determine the security posture of that system.

SEID - Standard Employee Identifier

Self-Assessment - A method for agency officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. For a self-assessment to be effective, a risk assessment must be conducted in conjunction with, or prior to the self-assessment. A self-assessment does not eliminate the need for a risk assessment.

SEMS - Secure Enterprise Messaging System

Senior Agency Information Security Officer (SAISO) - Official responsible for carrying out the Chief Information Officer responsibilities under the Federal Information Security Modernization Act of 2014 (FISMA) and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, system owners, and system security officers.

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.

Sensitive Information (NIST SP 800-53) - Information where the loss, misuse, or unauthorized access or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. 552a (the Privacy Act); that has not been specifically authorized under criteria established by an EO or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

Sensitivity Levels - A graduated system of marking (e.g., LOW, MODERATE, HIGH) information and information processing systems based on threats and risks that result if a threat is successfully conducted.

Service Account - Security accounts that are used by an OS or application to run a service or process. The purpose of the service accounts is to let the associated program login as a service and perform some high-level task even when no one is logged directly into the server.

Service-Level Agreement (SLA) - Defines the specific responsibilities of the service provider and sets the customer expectations.

Exhibit 10.8.1-1 (Cont. 20) (12-12-2023)
Terms and Acronyms

Session - A semi-permanent interactive information interchange, also known as a dialogue, a conversation or a meeting, between two or more communicating devices, or between a computer and user. A session is set up or established at a certain point in time, and torn down at a later point in time. An established communication session may involve more than one message in each direction. A session is typically, but not always, stateful, meaning that at least one of the communicating parties needs to save information about the session history in order to be able to communicate, as opposed to stateless communication, where the communication consists of independent requests with responses.

Significant Change - Also referred to as major change – A change that is likely to affect the security state of a system. Significant changes to a system may include for example: (i) installation of a new or upgraded operating system, middleware component, or application; (ii) modifications to system ports, protocols, or services; (iii) installation of a new or upgraded hardware platform; (iv) modifications to cryptographic modules or services; or (v) modifications to security controls. Examples of significant changes to the environment of operation may include for example: (i) moving to a new facility; (ii) adding new core missions or business functions; (iii) acquiring specific and credible threat information that the organization is being targeted by a threat source; or (iv) establishing new/modified laws, directives, policies, or regulations. If a formal reauthorization action is initiated, the organization targets only the specific security controls affected by the changes and reuses previous assessment results wherever possible. (NIST SP 800-37, F-7)

Note: The examples of changes listed above are only significant when they meet the threshold established in the definition of significant change (i.e., a change that is likely to affect the security state of the system).

SNMP - Simple Network Management Protocol

SOAR - Security, Orchestration, Automation, and Response

SOP - Standard Operating Procedure

SOW - Statement of Work

SP - Special Publication

Sponsor - An individual, separate from the process owner or developer and typically from within the business unit (selected by the business unit), receives authorization to run specific automation and have privileges to access to the production environment using authorized agency identity and access management services.

SQL - Structured Query Language

SRA - Security Risk Assessment

SSN - Social Security Number

Standalone - A desktop or laptop computer that is used on its own without requiring a connection to a network. A system that does not require a connection to any other computer for it to use an application (e.g., word processor or spreadsheet program); instead, the application programs stored on its hard drive are used. A standalone computer may be equipped with a printer, scanner, or external zip or hard drive.

STIG - Security Technical Implementation Guide

SWG - Software Web Gateway

System - Refer to Information System

Exhibit 10.8.1-1 (Cont. 21) (12-12-2023)
Terms and Acronyms

System Administrator (SA) - Individual responsible for the installation and maintenance of a system, providing effective system utilization, adequate security parameters, and sound implementation of established Information Assurance policy and procedures.

System Development Life Cycle (SDLC) - The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

System Security Plan (SSP) - Formal document that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements.

T

Tailoring - The process by which a security control baseline is modified based on the following:

1. The application of scoping guidance;
2. The specification of compensating security controls, if needed; and
3. The specification of IRS-defined parameters in the security controls via explicit assignment and selection statements.

TAS - Taxpayer Advocate Services

TCP/IP - Transmission Control Protocol/Internet Protocol

TCSIRC - Treasury Computer Security Incident Response Center

TD - Treasury Directive

TD P - Treasury Directive Publication

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

TFTP - trivial FTP

Threat - Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

TIC - Trusted Internet Connection

TIGTA - Treasury Inspector General Tax Administration

TIN - Taxpayer Identification Number

TFIMS - Treasury FISMA Inventory Management System

Tour of Duty - A tour of duty consists of the hours during the day (a daily tour of duty) and the days of an administrative workweek (a weekly tour of duty) that constitutes an employee's regularly scheduled administrative workweek. (Refer to IRM 6.610.1.2.1, Establishing and Recording the Tour of Duty)

Training - Training is more formal than "awareness," having the goal of building knowledge and skills to facilitate security in one's job performance. The training level strives to produce relevant and needed security skills

Exhibit 10.8.1-1 (Cont. 22) (12-12-2023)
Terms and Acronyms

and competency by practitioners whose functional specialties are other than IT security (e.g., management, systems design, development, acquisition, auditing). Current training guidance encourages Role-Based Training.

Transport Layer Security (TLS) - An authentication and security protocol widely implemented in browsers and Web servers.

Treasury System - A system that is:

a. Owned, leased, or operated by the IRS, departmental offices (DO), Office of the Inspector General (OIG) and TIGTA, or a component thereof.
b. Operated by a contractor on behalf of an IRS, DO, OIG, or a component thereof.

Trust Boundary - A border between two connected zones with different trust levels.

Trusted Network - The networks inside an organization’s security perimeter.

TSSSOC - Treasury Shared Services Security Operations Center

TT&E - Testing, Training, and Exercise

U

U.S.C. - United States Code

UDP - User Datagram Protocol

UEBA - User and Entity Behavior Analytics

UHF - Ultra High Frequency

Unauthorized Personnel - Applies to all IRS personnel not cleared with a requirement to access information systems (IS) for performing or assisting in a lawful and authorized government function.

UNAX - Unauthorized Access

Uninterruptible Power Supply (UPS) - An electrical system or mechanism that provides emergency power when there is a failure of the main power source.

Unix - An operating system well known for its relative hardware independence and portable application interfaces. The different versions of Unix fall into the following three (3) branches: System V, BSD Unix, and Open systems. Some of the popular Unix derivatives are: Linux, Solaris, HP-UX, and AIX.

Unprivileged Network Account - Any account that is not classified as a privileged network account.

UNS - User and Network Services

URL - Uniform Resource Locator

USB - Universal Serial Bus

User - Refer to IRS Personnel

USGv6 - Developed by NIST, it is the technical basis (standards and testing) to facilitate broad US Government (USG) initiatives in IPv6 adoption. The USGv6 Program provides a standards profile and product test program to facilitate the trustworthy acquisition of IPv6 enabled networked information technology products and

Exhibit 10.8.1-1 (Cont. 23) (12-12-2023)
Terms and Acronyms

services. The USGv6 Profile and USGv6 Test Program were designed to leverage and align to the maximum extent possible existing industry-led efforts on product test and certification and other profiling and testing efforts at the time.

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 a system and its resources.

UTC - Coordinated Universal Time

UVPROM - Ultraviolet Programmable Read Only Memory

V

VHF - Very High Frequency

Verification - Confirmation, through the provision of objective evidence, that specified requirements have been fulfilled (e.g., an entity's requirements have been correctly defined, or an entity's attributes have been correctly presented; or a procedure or function performs as intended and leads to the expected outcome). (CNSSI No. 4009)

Virtual Private Network (VPN) - A virtual network, built on top of existing physical networks that provide a secure communications tunnel for data and other information transmitted between networks.

Vulnerability - Weakness in a 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 a system.

Vulnerability & Patch Management - Patch management supports Vulnerability Management as a means to automate patching of software in response to vendor-discovered vulnerabilities. Effective patch management is a key (but not the only) requirement for effective vulnerability management. Vulnerability Management uses automated tools to find CVEs that are included in a report to be fixed, but does not itself focus on their remediation. Patch management tools often report what patches are present and assist with the automated patching of systems, but these tools do not necessarily correlate what they detect on systems to a set of known vulnerabilities.

Vulnerability Scanning - The process of proactively identifying vulnerabilities of a 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 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.

Web Conferencing - The utilization of technologies to conduct live meetings or presentations via the Internet whereby each participant's computer is connected to other participants via the Internet. Such a connection can be achieved either by downloading and installing an application onto each participant's computer or by accessing a web-based application via an Internet browser.

White List - A list of discrete entities, such as hosts or applications that are known to be benign and are approved for use within an organization and/or system.

Exhibit 10.8.1-1 (Cont. 24) (12-12-2023)
Terms and Acronyms

WLAN - Wireless Local Area Network

WORM - Write-Once-Read-Many

WWW - World Wide Web

X

XDR - Extended Detection and Response

Z

Zero Trust (ZT) - Provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. (NIST SP 800-207)

Zero Trust Architecture (ZTA) - An enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan. (NIST SP 800-207)

Exhibit 10.8.1-2 (12-13-2022)
Related Resources

Public Law

- Public Law 113-283, *Federal Information Security Modernization Act of 2014*, December 18, 2014
- Public Law 81-754, *Federal Records Act of 1950*, (P.L. 113-187, 2014 Amendments)
- Public Law 93–579, *Privacy Act of 1974*, as Amended (PRIVACT)
- Public Law 97–255, *Federal Managers' Financial Integrity Act (FMFIA) of 1982*
- Public Law 99–474, *The Computer Fraud and Abuse Act of 1986*
- Public Law 100–235, *Computer Security Act of 1987*
- Public Law 104–13, *Paperwork Reduction Act of 1995*
- Public Law 104–106, *National Defense Authorization Act for Fiscal Year*
- Public Law 105-35, *Taxpayer Browsing Protection Act of 1997*
- Public Law 106–398, *Floyd D. Spence National Defense Authorization Act for Fiscal Year 2001*
- Public Law 107-347, *E-Government Act of 2002*, December 17, 2002
- Public Law 115-435, *Foundations for Evidence-Based Policymaking Act of 2018*, January 2019 (EVIDACT)

Executive Order

- Executive Order 10450: *Security Requirements for Government Employment*, April 27, 1953
- Executive Order 13010: *Critical Infrastructure Protection*, July 15, 1996
- Executive Order 13025: *Further Amendment to Executive Order 13010, as Amended, Critical Infrastructure Protection*, November 13, 1996
- Executive Order 13041: *Further Amendment to Executive Order 13010, as Amended, Critical Infrastructure Protection*, April 8, 1997
- Executive Order 13064: *Further Amendment to Executive Order 13010, as Amended, Critical Infrastructure Protection*, October 11, 1997
- Executive Order 13077: *Further Amendment to Executive Order 13010, as Amended, Critical Infrastructure Protection*, March 10, 1998
- Executive Order 13138: *Continuance of Certain Federal Advisory Committee*, September 30, 1999
- Executive Order 13526: *Classified National Security Information*, December 29, 2009
- Executive Order 13556: *Controlled Unclassified Information (CUI)*, November 4, 2010
- Executive Order 13587: *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, October 7, 2011
- Executive Order 13800: *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, May 11, 2017
- Executive Order 13960: *Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government*, December 3, 2020
- Executive Order 14028, *Improving the Nation's Cybersecurity*, May 12, 2021

Presidential Decision Directive (PDD)

- PDD 63, *Critical Infrastructure Protection*, May 22, 1998

Office of Management and Budget (OMB) Circular

- OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, August 6, 2022
- OMB Circular No. A-123, *Management's Responsibility for Internal Control*, December 21, 2004
- OMB Circular No. A-127, *Financial Management Systems*, January 9, 2009
- OMB Circular No. A-130, *Management Information as a Strategic Resource*, July 27, 2016

Exhibit 10.8.1-2 (Cont. 1) (12-13-2022)
Related Resources

Office of Management and Budget (OMB) Memoranda

- M-99-18, *Privacy Polices on Federal Web Sites*, June 2, 1999
- M-01-05, *Guidance on Inter-Agency Sharing of Personal Data - Protecting Personal Privacy*, December 20, 2000
- M-10-22, *Guidance for Online Use of Web Measurement and Customization Technologies*, June 25, 2010
- M-14-03, *Enhancing the Security of Federal Information and Information Systems*, November 18, 2013
- M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for Federal Civilian Government*, October 30, 2015
- M-16-24, *Role and Designation of Senior Agency Officials for Privacy*, September 15, 2016
- M-17-06, *Policies for Federal Agency Public Websites and Digital Services*, November 8, 2016
- M-17-09, *Management of Federal High Assets*, December 9, 2016
- M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, January 3, 2017
- M-17-15, *Rescission of Memoranda Related to Identity Management*, January 19, 2017
- M-19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, December 10, 2018
- M-19-13, *Category Management: Making Smarter Use of Common Contract Solutions and Practices*, March 20, 2019
- M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, May 21, 2019
- M-19-23, *Phase 1 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Learning Agendas, Personnel, and Planning Guidance*, July 10, 2019
- M-19-26, *Update to the Trusted Internet Connections (TIC) Initiative*, September 12, 2019
- M-21-04, *Modernizing Access to and Consent for Disclosure of Records Subject to the Privacy Act*, November 12, 2020
- M-21-07, *Completing the Transition to Internet Protocol Version 6 (IPv6)*, November 19, 2020
- M-21-30, *Protecting Critical Software Through Enhanced Security Measures*, August 10, 2021
- M-21-31, *Improving the Federal Governments Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, August 27, 2021
- M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*, October 8, 2021
- M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, January 26, 2022
- M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, September 14, 2022
- M-23-02, *Migrating to Post-Quantum Cryptography*, November 18, 2022
- M-23-03, *FY23 FISMA Guidance*, December 2, 2022
- M-23-10, *The Registration and Use of .gov Domains in the Federal Government,* February 8, 2023
- M-23-16, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, June 9, 2023
- OMB Federal CIO Memo, *Transition to IPv6*, September 28, 2010

The listed OMB Circulars and Memos are available on the White House web site at: www.whitehouse.gov/omb/information-for-agencies.

Federal Regulations

- Federal Telecommunications System 2000 (FTS 2000)

Exhibit 10.8.1-2 (Cont. 2) (12-13-2022)
Related Resources

- Federal Acquisition Regulation (FAR)
- Federal Management Regulation (FMR)

Department of the Treasury Publications

- Department of the Treasury OCIO - Cybersecurity, Version 4.0, *Departmental Incident Response Plan*, May 23, 2023
- TD P 15-71, *Department of the Treasury Security Manual*, June 17, 2011
- TD P 85-01, Version 3.1.3, *Department of the Treasury Information Technology Security Program*, February 28, 2022
- Treasury Order (TO) 105-20, *Insider Threat Program*, January 6, 2020
- TD 80-05, *Records and Information Management Program*, June 26, 2002

Federal Risk and Authorization Management Program (FedRAMP)

- FedRAMP, U.S. Chief Information Officer, Office of Management & Budget *https://cloud.cio.gov*
- FedRAMP web site: *https://www.fedramp.gov*
- FedRAMP Knowledgebase: *https://www.fedramp.gov/faqs/*

Internal Revenue Service (IRS) Policy Publications

- IRM 1.15, **Records and Information Management** series
- IRM 2.5, **Systems Development** series
- IRM 2.7.1, **Information Technology (IT) Operations, Inter-Center**
- IRM 2.16.1, **Enterprise Life Cycle (ELC), ELC Guidance**
- IRM 2.25, **Management Service for IRS** series
- IRM 2.149, **IT Asset Management** series
- IRM 2.150.2, **Configuration Management, Configuration Management (CM) Process**
- IRM 3.10, **Campus Mail and Work Control** series
- RM 6.610.1, **Hours of Duty, IRS Hours of Duty**
- IRM 6.751.1, **Disciplinary Suspensions and Adverse Actions, Policies, Responsibilities Authorities, and Guidance**
- IRM 6.752, **Disciplinary Suspensions and Adverse Actions** series
- IRM 10.2, **Physical Security Program** series
- IRM 10.5, **Privacy and Information Protection** series
- IRM 10.6, *Continuity Operations* series
- IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*
- IRM 10.8.5, *Information Technology (IT) Security, Domain Name System (DNS) Security Policy*
- IRM 10.8.15, *Information Technology (IT) Security, General Platform Operating System Security Policy*
- IRM 10.8.22, *Information Technology (IT) Security, Web Server Security Policy*
- IRM 10.8.24, **Information Technology (IT) Security, Cloud Computing Security Policy**
- IRM 10.8.26, *Information Technology (IT) Security, Wireless and Mobile Device Security Policy*
- IRM 10.8.50, *Information Technology (IT) Security, Servicewide Security Patch Management*
- IRM 10.8.52, *Information Technology (IT) Security, IRS Public Key Infrastructure (PKI) X.509 Certificate Policy*
- IRM 10.8.54, *Information Technology (IT) Security, Minimum Firewall Administration Requirements*
- IRM 10.8.60, *Information Technology (IT) Security, IT Service Continuity Management (ITSCM) Policy and Guidance*
- IRM 10.8.62, *Information Technology (IT) Security, Information Systems Contingency Plan (ISCP) and Disaster Recovery (DR) Testing, Training, and Exercise (TT&E) Program*

Exhibit 10.8.1-2 (Cont. 3) (12-13-2022)
Related Resources

- IRM 10.8.63, *Information Technology (IT) Security, Central Log Server Security Policy*
- IRM 10.9.1, *National Security Information, Classified National Security Information (NSI)*
- IRM 10.23.1, **Personnel Security, National Security Positions and Access to Classified Information**
- IRM 10.23.2, **Personnel Security, Contractor Investigations**
- IRM 10.23.3, **Personnel Security, Personnel Security/Suitability for Employment and Personnel Security Operations**
- IRM 11.3.1, **Disclosure of Official Information, Introduction to Disclosures**
- IRM 11.3.24, *Disclosure of Official Information, Disclosures to Contractors*
- IRM 13.1, *Taxpayer Advocate Case Procedures* series
- IRM 21.1, *Accounts Management and Compliance Services Operations* series
- IRS Ethics Handbook, Document 12011
- IRS Managers Guide to Penalty Determinations, Document 11500
- IRS Publication 4812, **Contractor Security & Privacy Controls - Handling and Protecting Information or Information Systems**
- Policy Statement 2-90 (formerly P-1-144), Designing safeguards for computer systems (located at IRM 1.2.1.3.2)

#
#
#
#

General Accounting Office (GAO)

- *Executive Guide on Information Security Management*, May 1998
- *Information Security Risk Assessment, Practices of Leading Organizations*, November 1999
- *Federal Information System Control Audit Manual (FISCAM)*, January 2000

The listed GAO Publications are available on GAO web site: https://www.gao.gov.

National Institute of Standards and Technology (NIST) Publications

- NIST SP 800-207, *Zero Trust Architecture*, August 2020
- NIST SP 800-189, *Resilient Interdomain Traffic Exchange: BGP Security and DDoS Mitigation,* December 2019
- NIST SP 800-166, *Derived PIV Application and Data Model Test Guidelines*, June 6, 2016
- NIST SP 800-161, Revision 1 *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, May 2022
- NIST SP 800-160 Volume 1, *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems*, March 2018
- NIST SP 800-153, *Guidelines for Securing Wireless Local Area Networks (WLANs)*, February 2012
- NIST SP 800-152, *A Profile for U. S. Federal Cryptographic Key Management Systems*, October 2015
- NIST SP 800-147, *BIOS Protection Guidelines*, April 2011
- NIST SP 800-146, *Cloud Computing Synopsis and Recommendations*, May 2012
- NIST SP 800-145, *The NIST Definition of Cloud Computing*, September 2011
- NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, December 2011
- NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, September 2011
- NIST SP 800-126, Revision 3 *The Technical Specifications for the Security Content Automation Protocol (SCAP): SCAP Version 1.3*, February 2018

Exhibit 10.8.1-2 (Cont. 4) (12-13-2022)
Related Resources

- NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, April 2010
- NIST SP 800-119, *Guidelines for the Secure Deployment of IPv6*, December 2010
- NIST SP 800-116, Revision 1, *Guidelines for the Use of PIV Credentials in Facility Access,*, June 2018
- NIST SP 800-115, *Technical Guide to Information Security Testing and Assessment*, September 2008
- NIST SP 800-88, Revision 1, *Guidelines for Media Sanitization*, December 2014
- NIST SP 800-84, *Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities*, September 2006
- NIST SP 800-81-2, *Secure Domain Name System (DNS) Deployment Guide*, September 2013
- NIST SP 800-79-2, *Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)*, July 2015
- NIST SP 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, May 2015
- NIST SP 800-76-2, Revision 1, *Biometric Specifications for Personal Identity Verification*, July 2013
- NIST SP 800-73-4, *Interfaces for Personal Identity Verification*, May 2015 (Updated 2/8/2016)
- NIST SP 800-70, Revision 4, *National Checklist Program for IT Products-Guidelines for Checklist Users and Developers*, May 2018
- NIST SP 800-63-3, *Digital Identity Guidelines*, June 2017
- NIST SP 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*, March 2, 2020
- NIST SP 800-63A, *Digital Identity Guidelines: Enrollment and Identity Proofing*, March 2, 2020
- NIST SP 800-61, Revision 2, *Computer Security Incident Handling Guide*, August 2012
- NIST SP 800-57, Part 3, Revision 1, *Recommendation for Key Management, Part 3 Application-Specific Key Management Guidance*, January 2015
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, September 2020 (Updated 12/10/2020)
- NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*, January 2022
- NIST SP 800-53B, *Control Baselines for Information Systems and Organizations*, October 2020 (Updated 12/10/2020)
- NIST SP 800-52 Revision 2, *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*, August 29, 2019
- NIST SP 800-47 Revision 1, *Managing the Security of Information Exchanges*, July 2021
- NIST SP 800-45, Version 2, *Guidelines on Electronic Mail Security*, February 2007
- NIST SP 800-41, Revision 1, *Guidelines on Firewalls and Firewall Policy*, September 2009
- NIST SP 800-40, Revision 4, *Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technologies*, April 2022
- NIST SP 800-37, Revision 2, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach for Security and Privacy*, December 20, 2018
- NIST SP 800-34 Revision 1, *Contingency Planning Guide for Federal Information Systems*, November 11, 2010
- NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments*, September 2012
- NIST SP 800-28, Version 2, *Guidelines on Active Content and Mobile Code*, March 2008
- NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006
- NIST SP 800-12, Revision 1, *An Introduction to Computer Security: The NIST Handbook*, June 2022
- NIST publications can be found at: *https://csrc.nist.gov/publications*.

Exhibit 10.8.1-2 (Cont. 5) (12-13-2022)
Related Resources

FIPS Publications

- FIPS 140-2, *Security Requirements for Cryptographic Modules*, December 3, 2002
- FIPS 140-3, *Security Requirements for Cryptographic Modules*, March 22, 2019
- FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 1, 2004
- FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, March 1, 2006

Other Publications

- National Security Agency, Information Systems Security Organization, *Controlled Access Protection Profile*, October 1999
- National Information Assurance Certification and Accreditation Process (NIACAP), NSTISSI No. 1000, April 2000
- National Information Assurance Partnership (NIAP), *Security Requirements Profiling*, August 2000
- Security, Privacy, and Critical Infrastructure Committee, Federal Information Technology Security Assessment Framework, November 2000
- Security, Privacy, and Critical Infrastructure Committee, Securing Electronic Government, January 2001
- NARA, *Controlled Unclassified Information (CUI) Office Notice 2011-01: Initial Implementation Guidance for Executive Order 13556*, June 2011
- NARA, *General Records Schedules (GRS)* (*https://www.archives.gov/records-mgmt/grs.html*)
- CISA, *Cloud Security Technical Reference Architecture*, Version 2.9, June 2022
- CISA, BOD 19-02, *Vulnerability Remediation Requirements for Internet-Accessible System*, April 2019
- CISA BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, November 2021
- CISA BOD 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks*, October 2022
- CISA BOD 23-02, *Mitigating the Risk from Internet-Exposed Management Interfaces*, June 2023
- Code of Federal Regulations, Title 32, *Controlled Unclassified Information* (32 C.F.R. 2002)
- DHS TIC – Department of Homeland Security, *Trusted Internet Connections* (TIC). *https://www.cisa.gov/resources-tools/programs/trusted-internet-connections-tic*