EFFECTIVE DATE

(02-02-2024)

PURPOSE

(1) This transmits revised Internal Revenue Manual (IRM) 10.8.24, *Information Technology (IT) Security, Cloud Computing Security Policy.*

MATERIAL CHANGES

(1) The following sections have been updated/clarified/removed with this version of IRM:
10.8.24.1, Program Scope and Objectives - Updated to align with IRM 1.11.2 format.
10.8.24.1.1, Background - Updated to align with IRM 1.11.2 format.
10.8.24.1.2, Authority - Updated to align with IRM 1.11.2 format.
10.8.24.1.3, Roles and Responsibilities - Organized to align with IRM 1.11.2 format and updated the Office of Safeguard requirements.
10.8.24.1.4, Program Management and Review - Added to align with IRM 1.11.2 format.
10.8.24.1.5, Program Controls - Added to align with IRM 1.11.2 format.
10.8.24.1.6, Terms and Acronyms - Added to align with IRM 1.11.2 format.
10.8.24.1.7, Related Resources - Added to align with IRM 1.11.2 format.
10.8.24.2, Risk Acceptance and Risk-based Decisions - Moved from 10.8.24.1.10 to align with IRM 1.11.2 format.
10.8.24.3, IT Security Controls - Updated with language from IG Memo IT-10-0122-0001.
10.8.24.3.1.1, AC-1 - Updated to align with Federal Risk and Authorization Management Program (FedRAMP) Rev 5.
10.8.24.3.1.2, AC-2 - Updated to align with FedRAMP Rev 5.
10.8.24.3.1.4, AC-4 - Updated to align with FedRAMP Rev 5.
10.8.24.3.1.5, AC-5 - Updated to align with FedRAMP Rev 5.
10.8.24.3.1.6, AC-6 - Updated to align with FedRAMP Rev 5.
10.8.24.3.1.7, AC-7 - Updated to align with FedRAMP Rev 5.
10.8.24.3.1.8, AC-8 - Updated to align with FedRAMP Rev 5.
10.8.24.3.1.9, AC-10 - Updated to align with FedRAMP Rev 5.
10.8.24.3.1.10, AC-11 - Updated to align with FedRAMP Rev 5.
10.8.24.3.1.11, AC-12 - Updated to align with FedRAMP Rev 5.
10.8.24.3.1.12, AC-14 - Updated to align with FedRAMP Rev 5.
10.8.24.3.1.13, AC-16 - Removed to align with FedRAMP Rev 5.
10.8.24.3.1.14, AC-17 - Updated to align with FedRAMP Rev 5.
10.8.24.3.1.15, AC-18 - Updated to align with FedRAMP Rev 5.
10.8.24.3.1.16, AC-19 - Updated to align with FedRAMP Rev 5.
10.8.24.3.1.17, AC-20 - Updated to align with FedRAMP Rev 5.
10.8.24.3.1.18, AC-21 - Updated to align with FedRAMP Rev 5.
10.8.24.3.1.19, AC-22 - Updated to align with FedRAMP Rev 5.
10.8.24.3.2.1, AT-1 - Updated to align with FedRAMP Rev 5.
10.8.24.3.2.2, AT-2 - Updated to align with FedRAMP Rev 5.
10.8.24.3.2.3, AT-3 - Updated to align with FedRAMP Rev 5.
10.8.24.3.2.4, AT-4 - Updated to align with FedRAMP Rev 5.
10.8.24.3.3.1, AU-1 - Updated to align with FedRAMP Rev 5.
10.8.24.3.3.2, AU-2 - Updated to align with FedRAMP Rev 5.
10.8.24.3.3.3, AU-3 - Updated to align with FedRAMP Rev 5.
10.8.24.3.3.4, AU-4 - Updated to align with FedRAMP Rev 5.
10.8.24.3.3.5, AU-5 - Updated to align with FedRAMP Rev 5.

10.8.24.3.3.6, AU-6 - Updated to align with FedRAMP Rev 5.
10.8.24.3.3.7, AU-7 - Updated to align with FedRAMP Rev 5.
10.8.24.3.3.8, AU-8 - Updated to align with FedRAMP Rev 5.
10.8.24.3.3.9, AU-9 - Updated to align with FedRAMP Rev 5.
10.8.24.3.3.10, AU-10 - Updated to align with FedRAMP Rev 5.
10.8.24.3.3.11, AU-11 - Updated to align with FedRAMP Rev 5.
10.8.24.3.3.12, AU-12 - Updated to align with FedRAMP Rev 5.
10.8.24.3.4.1, CA-1 - Updated to align with FedRAMP Rev 5.
10.8.24.3.4.2, CA-2 - Updated to align with FedRAMP Rev 5.
10.8.24.3.4.3, CA-3 - Title updated to align with FedRAMP Rev 5.
10.8.24.3.4.4, CA-5 - Updated to align with FedRAMP Rev 5.
10.8.24.3.4.5, CA-6 - Updated to align with FedRAMP Rev 5.
10.8.24.3.4.6, CA-7 - Updated to align with FedRAMP Rev 5.
10.8.24.3.4.7, CA-8 - Updated to align with FedRAMP Rev 5.
10.8.24.3.4.8, CA-9 - Updated to align with FedRAMP Rev 5.
10.8.24.3.5.1, CM-1 - Updated to align with FedRAMP Rev 5.
10.8.24.3.5.2, CM-2 - Updated to align with FedRAMP Rev 5.
10.8.24.3.5.3, CM-3 - Updated to align with FedRAMP Rev 5.
10.8.24.3.5.4, CM-4 - Updated to align with FedRAMP Rev 5.
10.8.24.3.5.5, CM-5 - Updated to align with FedRAMP Rev 5.
10.8.24.3.5.6, CM-6 - Updated to align with FedRAMP Rev 5.
10.8.24.3.5.7, CM-7 - Updated to align with FedRAMP Rev 5.
10.8.24.3.5.8, CM-8 - Updated to align with FedRAMP Rev 5 and IG Memo IT-10-1022-0012.
10.8.24.3.5.9, CM-9 - Updated to align with FedRAMP Rev 5.
10.8.24.3.5.10, CM-10 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.5.11, CM-11 - Updated to align with FedRAMP Rev 5.
10.8.24.3.5.12, CM-12 - Updated to align with FedRAMP Rev 5.
10.8.24.3.5.13, CM-14 - Updated to align with FedRAMP Rev 5.
10.8.24.3.6.1, CP-1 - Updated to align with FedRAMP Rev 5.
10.8.24.3.6.2, CP-2 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.6.3, CP-3 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.6.4, CP-4 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.6.5, CP-6 - Updated to align with FedRAMP Rev 5 and added IRS Responsibility.
10.8.24.3.6.6, CP-7 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.6.7, CP-8 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.6.8, CP-9 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.6.9, CP-10 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.7.1, IA-1 - Updated to align with FedRAMP Rev 5.
10.8.24.3.7.2, IA-2 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.7.3, IA-3 - Updated to align with FedRAMP Rev 5.
10.8.24.3.7.4, IA-4 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.7.5, IA-5 - Updated to align with FedRAMP Rev 5, IG Memo IT-10-1022-0012, and added IRS responsibility.
10.8.24.3.7.6, IA-6 - Updated to align with FedRAMP Rev 5.
10.8.24.3.7.7, IA-7 - Updated to align with FedRAMP Rev 5.
10.8.24.3.7.8, IA-8 - Updated to align with FedRAMP Rev 5.
10.8.24.3.7.11, IA-11 - Updated to align with FedRAMP Rev 5.
10.8.24.3.7.12, IA-12 - Added to align with FedRAMP Rev 5.
10.8.24.3.8.1, IR-1 - Updated to align with FedRAMP Rev 5.
10.8.24.3.8.2, IR-2 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.8.3, IR-3 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.8.4, IR-4 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.8.5, IR-5 - Updated to align with FedRAMP Rev 5.

10.8.24.3.8.6, IR-6 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.8.7, IR-7 - Updated to align with FedRAMP Rev 5.
10.8.24.3.8.8, IR-8 - Updated to align with FedRAMP Rev 5.
10.8.24.3.8.9, IR-9 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.9.1, MA-1 - Updated to align with FedRAMP Rev 5.
10.8.24.3.9.2, MA-2 - Updated to align with FedRAMP Rev 5.
10.8.24.3.9.3, MA-3 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.9.4, MA-4 - Updated to align with FedRAMP Rev 5.
10.8.24.3.9.5, MA-5 - Updated to align with FedRAMP Rev 5.
10.8.24.3.10.1, MP-1 - Updated to align with FedRAMP Rev 5.
10.8.24.3.10.2, MP-2 - Updated to align with FedRAMP Rev 5.
10.8.24.3.10.3, MP-3 - Updated to align with FedRAMP Rev 5.
10.8.24.3.10.4, MP-4 - Updated to align with FedRAMP Rev 5.
10.8.24.3.10.5, MP-5 - Updated to align with FedRAMP Rev 5.
10.8.24.3.10.6, MP-6 - Updated to align with FedRAMP Rev 5.
10.8.24.3.10.7, MP-7 - Updated to align with FedRAMP Rev 5.
10.8.24.3.11.1, PE-1 - Updated to align with FedRAMP Rev 5.
10.8.24.3.11.2, PE-2 - Updated to align with FedRAMP Rev 5.
10.8.24.3.11.3, PE-3 - Updated to align with FedRAMP Rev 5.
10.8.24.3.11.4, PE-4 - Updated to align with FedRAMP Rev 5.
10.8.24.3.11.5, PE-5 - Updated to align with FedRAMP Rev 5.
10.8.24.3.11.6, PE-6 - Updated to align with FedRAMP Rev 5.
10.8.24.3.11.7, PE-8 - Updated to align with FedRAMP Rev 5.
10.8.24.3.11.8, PE-9 - Updated to align with FedRAMP Rev 5.
10.8.24.3.11.9, PE-10 - Updated to align with FedRAMP Rev 5.
10.8.24.3.11.10, PE-11 - Updated to align with FedRAMP Rev 5.
10.8.24.3.11.11, PE-12 - Updated to align with FedRAMP Rev 5.
10.8.24.3.11.12, PE-13 - Updated to align with FedRAMP Rev 5.
10.8.24.3.11.13, PE-14 - Updated to align with FedRAMP Rev 5.
10.8.24.3.11.14, PE-15 - Updated to align with FedRAMP Rev 5.
10.8.24.3.11.15, PE-16 - Updated to align with FedRAMP Rev 5.
10.8.24.3.11.16, PE-17 - Updated to align with FedRAMP Rev 5.
10.8.24.3.11.17, PE-18 - Updated to align with FedRAMP Rev 5.
10.8.24.3.12.1, PL-1 - Updated to align with FedRAMP Rev 5.
10.8.24.3.12.2, PL-2 - Updated to align with FedRAMP Rev 5.
10.8.24.3.12.3, PL-3 - Updated to align with FedRAMP Rev 5.
10.8.24.3.12.5, PL-8 - Updated to align with FedRAMP Rev 5.
10.8.24.3.12.7, PL-10 - Added to align with FedRAMP Rev 5.
10.8.24.3.12.8, PL-11 - Added to align with FedRAMP Rev 5.
10.8.24.3.13.1, PS-1 - Updated to align with FedRAMP Rev 5.
10.8.24.3.13.2, PS-2 - Updated to align with FedRAMP Rev 5.
10.8.24.3.13.3, PS-3 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.13.4, PS-4 - Updated to align with FedRAMP Rev 5.
10.8.24.3.13.5, PS-5 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.13.6, PS-6 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.13.7, PS-7 - Updated to align with FedRAMP Rev 5.
10.8.24.3.13.8, PS-8 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.13.9, PS-9 - Added to align with FedRAMP Rev 5.
10.8.24.3.14.1, RA-1 - Updated to align with FedRAMP Rev 5.
10.8.24.3.14.2, RA-2 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.14.3, RA-3 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.14.4, RA-5 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.14.5, RA-6 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.

10.8.24.3.14.6, RA-7 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.14.7, RA-9 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.15.1, SA-1 - Updated to align with FedRAMP Rev 5.
10.8.24.3.15.2, SA-2 - Updated to align with FedRAMP Rev 5.
10.8.24.3.15.3, SA-3 - Updated to align with FedRAMP Rev 5.
10.8.24.3.15.4, SA-4 - Updated to align with FedRAMP Rev 5.
10.8.24.3.15.5, SA-5 - Updated to align with FedRAMP Rev 5.
10.8.24.3.15.6, SA-8 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.15.7, SA-9 - Updated to align with FedRAMP Rev 5.
10.8.24.3.15.8, SA-10 - Updated to align with FedRAMP Rev 5.
10.8.24.3.15.9, SA-11 - Updated to align with FedRAMP Rev 5.
10.8.24.3.15.13, SA-15 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.15.14, SA-16 - Updated to align with FedRAMP Rev 5.
10.8.24.3.15.15, SA-17 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.15.19, SA-21 - Added to align with FedRAMP Rev 5.
10.8.24.3.15.20, SA-22 - Added to align with FedRAMP Rev 5.
10.8.24.3.15.21, SA-23 - Added to align with Security Policy Boiler Plate.
10.8.24.3.16.1, SC-1 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.2, SC-2 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.3, SC-3 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.4, SC-4 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.5, SC-5 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.6, SC-6 - Removed to align with FedRAMP Rev 5.
10.8.24.3.16.7, SC-7 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.16.8, SC-8 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.9, SC-10 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.11, SC-12 - Updated to align with FedRAMP Rev 5, IG Memo IT-10-0922-0010, and added IRS responsibility.
10.8.24.3.16.12, SC-13 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.13, SC-15 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.14, SC-16 - Title updated to align with FedRAMP Rev 5.
10.8.24.3.16.15, SC-17 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.16, SC-18 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.17, SC-19 - Removed to align with FedRAMP Rev 5.
10.8.24.3.16.18, SC-20 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.19, SC-21 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.20, SC-22 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.21, SC-23 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.22, SC-24 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.26, SC-28 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.30, SC-32 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.36, SC-39 - Updated to align with FedRAMP Rev 5.
10.8.24.3.16.42, SC-45 - Updated to align with FedRAMP Rev 5.
10.8.24.3.17.1, SI-1 - Updated to align with FedRAMP Rev 5.
10.8.24.3.17.2, SI-2 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.17.3, SI-3 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.17.4, SI-4 - Updated to align with FedRAMP Rev 5.
10.8.24.3.17.5, SI-5 - Updated to align with FedRAMP Rev 5.
10.8.24.3.17.6, SI-6 - Updated to align with FedRAMP Rev 5.
10.8.24.3.17.7, SI-7 - Updated to align with FedRAMP Rev 5 and IG Memo IT-10-1022-0012.
10.8.24.3.17.8, SI-8 - Updated to align with FedRAMP Rev 5.
10.8.24.3.17.9, SI-10 - Updated to align with FedRAMP Rev 5.
10.8.24.3.17.10, SI-11 - Updated to align with FedRAMP Rev 5.

10.8.24.3.17.11, SI-12 - Updated to align with FedRAMP Rev 5.
10.8.24.3.17.17-10.8.24.3.17.20 - Updated to align with Security Policy Boiler Plate.
10.8.24.3.18.1, SR-1 - Updated to align with FedRAMP Rev 5.
10.8.24.3.18.2, SR-2 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.18.3, SR-3 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.18.4, SR-5 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.18.5, SR-6 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.18.6, SR-8 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.18.7, SR-9 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.18.8, SR-10 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.18.9, SR-11 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.
10.8.24.3.18.1, SR-12 - Updated to align with FedRAMP Rev 5 and added IRS responsibility.

(2) The following Interim Guidance Memorandums (IG Memos) are incorporated into this IRM:
i. Interim Guidance Memo #IT-10-1122-0026, CA-6 Security Authorization, dated December 6, 2022;
ii. Interim Guidance Memo #IT-10-0922-0010, Information Technology (IT) Security, Cloud Computing Security Policy - SC-12 Cryptographic Key Establishment and Management, dated November 24, 2022; and
iii. Interim Guidance Memo #IT-10-0122-0001 Authorized CSOs - Policy Update Internal Revenue Manual (IRM) 10.8.24, Information Technology (IT) Security, Cloud Computing S, dated February 1, 2022.
iv. 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

(3) Editorial changes made throughout the IRM for clarity. Reviewed and updated plain language, grammar, titles, website addresses, IRM references, terminologies and reorganized content.

EFFECT ON OTHER DOCUMENTS

IRM 10.8.24 dated September 28, 2021, is superseded. This IRM supplements IRM 10.8.1, *Information Technology (IT) Security , Policy and Guidance*; and IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*.
This IRM incorporates Interim Guidance Memo # IT-10-1122-0026, CA-6 Security Authorization, dated December 6, 2022, Interim Guidance Memo #IT-10-0922-0010, Information Technology (IT) Security, Cloud Computing Security Policy - SC-12 Cryptographic Key Establishment and Management, dated November 24, 2022, IT-10-0122-0001 Authorized CSOs - Policy Update Internal Revenue Manual (IRM) 10.8.24, Information Technology (IT) Security, Cloud Computing S, dated February 1, 2022 and 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.

AUDIENCE

IRM 10.8.24 applies to all IRS personnel and must be distributed to all personnel responsible for ensuring that adequate security is provided to Cloud Computing systems and Internal Revenue Service (IRS) information residing on these systems.

Kaschit Pandya
Acting, Chief Information Officer

10.8.24
Cloud Computing Security Policy

Table of Contents

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

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

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

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

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

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

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

#
#
#
#
#
#

Exhibits

10.8.24.1
(02-02-2024)
Program Scope and Objectives

(1) **Overview:** This Internal Revenue Manual (IRM) lays the foundation to implement and manage security guidance for the use of cloud computing systems within the Internal Revenue Service (IRS).

a. This policy is subordinate to IRM 10.8.1, Information Technology (IT) Security, Policy and Guidance and augments the existing requirements identified within IRM 10.8.1, as they relate to Cloud computing systems.

(2) **Purpose of the Program**:Develop and publish security policies to protect the IRS against potential IT threats and vulnerabilities and ensure compliance with federal mandates and legislation.

(3) **Audience:** The provisions within this 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 systems.

10.8.24.1.1
(02-02-2024)
Background

(1) The Federal Government launched the Federal Risk and Authorization Management Program (FedRAMP) in June 2012 to account for the unique security requirements surrounding cloud computing. FedRAMP consists of a subset of NIST Special Publication (SP) 800-53 security controls targeted towards cloud provider and customer security requirements. The security requirements within this IRM are based on the FedRAMP Security Assessment Framework and are designed to enhance the requirements defined within IRM 10.8.1.

(2) IRM 10.8.24 is part of the Security, Privacy and Assurance policy family, IRM Part 10 series for IRS Information Technology Cybersecurity.

10.8.24.1.2
(02-02-2024)
Authority

(1) Consistent with the President's International Strategy for Cyberspace and Cloud First policy, the Office of Management and Budget (OMB) Chief Information Officer (CIO) Memo, Security Authorization of Systems in Cloud Computing Environments establishes the FedRAMP as a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

(2) The FedRAMP Authority Act 2023 codifies the FedRAMP program as the authoritative standardized approach to security assessment and authorization for cloud computing products and services that process unclassified federal information.

(3) Treasury Directive Publication (TD P) 85-01, Treasury Information Technology (IT) Security Program establishes that cloud systems must comply with FedRAMP guidelines. Bureaus may develop supplemental guidance on cloud systems and services tailored to meet their specific mission needs and risk tolerance.

10.8.24.1.3 (02-02-2024) **Roles and Responsibilities**

(1) IRM 10.8.2, *Information Technology (IT) Security, IT Security Roles and Responsibilities*, defines IRS-wide roles and responsibilities related to IRS information and information systems security and is the authoritative source for such information, including for cloud service providers (CSP)s in IRS. FedRAMP PMO is the source of the roles and responsibilities of the FedRAMP PMO, cloud service providers, Third Party Assessment Organization (3PAO), agency, and the FedRAMP Collaboration Group.

10.8.24.1.3.1 (02-02-2024) **The FedRAMP Program Management Office (PMO)**

(1) The FedRAMP Program Management Office (PMO) was established by General Services Administration (GSA) and is responsible for the following:

a. Create a process for executive departments and agencies and CSPs to adhere to the FedRAMP security authorization requirements created by the Joint Authorization Board (JAB) to include, but not limited to:
i. A methodology for harmonizing agency-specific security and privacy controls with the FedRAMP security authorization requirements;
ii. A mechanism for executive departments and agencies and CSPs to request security authorization initiation through the FedRAMP PMO and JAB;
iii. Guidance for executive departments and agencies to satisfy FedRAMP security authorization requirements when a proposed cloud service is not prioritized for review by the FedRAMP PMO and JAB.
iv. A framework for executive departments and agencies to leverage security authorization packages processed by FedRAMP;
v. In coordination with Department of Homeland Security, a framework for continuous monitoring, incident response and remediation, and FISMA reporting.

b. Prioritize requests for authorization and authorization package review by the JAB in accordance with the JAB-approved priority queue requirements and publish and update on a continuous basis the FedRAMP priority queue;

c. Establish a centralized, secure repository detailing requests for authorization, agency-provided authorization packages, CSP-provided authorization packages, and JAB provisional authorization packages of cloud services that executive departments and agencies can leverage to grant security authorizations;

d. Coordinate and collaborate with the NIST to develop and implement a formal conformity assessment program to accredit 3PAOs to provide independent assessments of how CSPs implement the FedRAMP requirements;

e. Develop and make available to executive departments and agencies templates that can satisfy FedRAMP security authorization requirements through standard contract language and service level agreements (SLAs) for use in the acquisition of cloud services; and

f. Develop and make available to executive departments and agencies template memorandum of understanding (MOU) and/or memorandum of agreement (MOA) that will govern the exchange of information between executive departments, agencies and the FedRAMP PMO.

(2) The FedRAMP PMO provides the authoritative source roles and responsibilities for cloud computing requirements.

(3) As a member of the JAB Charter, the FedRAMP PMO is responsible for the following:

a. Provide project management support to the JAB and JAB technical representatives and their teams.
b. Work with the JAB to create a process and framework for Federal agencies to meet FedRAMP requirements.
c. Maintain the 3PAO accreditation program and provide oversight of the performance and qualifications of accredited 3PAOs.
d. Conduct outreach and education on FedRAMP with stakeholder, including Federal agencies, industry, and oversight organizations.
e. Work with Federal departments and agencies to promote the issuance of FedRAMP agency authority to operate (ATO)s and the re-use of JAB provisional authority tooperate (P-ATO)s and agency ATOs.

Note: The JAB is a part of FedRAMP. The JAB performs risk authorizations and grants or revokes the FedRAMP provisional ATO. The JAB is the primary governance and decision-making body for the FedRAMP program.

10.8.24.1.3.2 (02-02-2024) **Cloud Service Provider (CSP)**

(1) Before a CSP launches into the FedRAMP process, and before getting a 3PAO consultant or assessor involved in the process, a CSP drafts an accurate illustration of the system authorization boundary and all associated data flow diagrams.

a. The CSP system authorization boundary illustration must include network and architecture diagram(s) and provide a written description of the authorization boundary. Ensure each diagram:
i. Includes a clearly defined authorization boundary.
ii. Clearly defines services wholly within the boundary.
iii. Depicts all major components or groups within the boundary.
iv. Identifies all interconnected systems.
v. Depicts all major software/virtual components (or groups of) within the boundary.
vi. Is validated against the inventory.
b. The CSP system boundary description must clearly define the following:
i. All shared corporate services, with explicit rationale of any that are not within the boundary, such as a corporate security operations center (SOC) or corporate security awareness training.
ii. All other external services with explicit rationale of any that are not within the boundary that includes all leveraged services.
iii. All systems related to, but excluded from the boundary.
c. In addition to describing these, all of the services must also be depicted either in the CSP system authorization boundary diagrams or in separate diagrams.
d. The CSP system data flow diagram(s) must:
i. Clearly identify anywhere Federal data is to be processed, stored, or transmitted.
ii. Clearly delineate how data comes into and out of the system boundary.
iii. Clearly identify data flows for privileged, non-privileged and customers access.
iv. Depict how all ports, protocols, and services of all inbound and outbound traffic are represented and managed.
e. The data flow diagrams must be accompanied by a written description of the data flows.

f. If the CSP boundary is not adequately/accurately represented, the 3PAO must identify boundary deficiencies that could lead to substantial delays in the CSP readiness assessment process.
g. If the CSP leverages another CSP or cloud service offering (CSO) that does not have a current FedRAMP JAB or agency ATO, the CSP must be fully responsible for the authorization of the entire cloud service model stack.

10.8.24.1.3.3 (02-02-2024)
Third-Party Assessment Organization (3PAO)

(1) A 3PAO must adhere strictly and continuously to the FedRAMP accreditation requirements.

(2) A 3PAO must be independent from any CSP they assess.

(3) A 3PAO must demonstrate technical competence through:

a. Review of system security plans (SSP);
b. Creation of a security assessment plan (SAP); and
c. Documenting the results in security assessment test cases as well as a security assessment report (SAR).

Note: This is demonstrated in their American Association for Laboratory Accreditation (A2LA) assessment.

Note: A FedRAMP approved 3PAO is optional for FedRAMP agency authorization packages.

(4) During a FedRAMP assessment, a 3PAO must produce the following documents as a part of the overall security authorization package submitted for authorization to a government authorizing official:

a. Security Assessment Plan (SAP):
i. Inventories.
ii. Rules of Engagement.
b. Security Assessment Report (SAR):
i. Security Assessment Test Case Workbook.
ii. Risk Exposure Table.
iii. Penetration Test Report.
iv. Vulnerability Scan Data Files.
v. Test Artifacts.

(5) A 3PAO performs the following:

a. During the readiness assessment phase:
i. Conducts readiness assessment.
ii. Develops readiness assessment report (RAR).
iii. Submits RAR to the FedRAMP PMO upon notification.
iv. Supports FedRAMP PMO during RAR review (as necessary).
b. During the full security assessment phase:
i. Performs in-depth review of the SSP for compliance.
ii. Develop SAP, and schedule and perform assessment activities.
iii. Develop SAR.
iv. Completes full security assessment, including SAP and SAR with matching POA&M and test cases.
v. Ensures documentation within SSP matches security control implemen-

tations (this is a portion of the test cases).
vi. Supports FedRAMP PMO completeness check and kick-off coordination activities.

c. During the JAB authorization process kick-off phase:
i. Supports JAB reviewers in gaining an in-depth understanding of any risks associated with CSP system, typically through a combination of briefings and informal question and answer.
ii. Ensures representatives who can answer in-depth questions about the full assessment are present.

d. During the JAB authorization process review phase:
i. Supports JAB reviewers by addressing questions about full security assessment.
ii. Participates in regular meetings among CSP, 3PAO, PMO, and JAB reviews.

e. During the JAB authorization process remediation phase:
i. Performs any retesting required by JAB reviewers.
ii. Updates and resubmits full security documentation based on retesting.
iii. Ensures all comments from JAB reviewers are appropriately addressed.

10.8.24.1.3.4
(02-02-2024)
Agency

(1) Office of Management and Budget (OMB) Circular A-130 (revised 7/28/2016) now explicitly outlines agency responsibilities for their information and information systems, and links their information security program to OMB Circular A-123, Management's Responsibility for Enterprise Risk Management and Internal Controls. OMB Circular A-130 Appendix I incorporates requirements of the Federal Information Security Modernization Act (FISMA) (44 U.S.C. Chapter 35), the E-Government Act of 2002 (44 U.S.C. Chapters 35 and 36), the Paperwork Reduction Act (44 U.S.C. Chapter 35), and the Privacy Act of 1974, and responsibilities assigned in executive orders and presidential directives.

(2) Agencies are responsible for:
i. Ensuring all new CSP CSO projects minimally use the FedRAMP baseline controls and templates for Low, Moderate, and High baseline systems.
ii. Ensuring existing cloud projects (implemented or in the acquisition process) meet FedRAMP requirements.
iii. Adding or modifying contractual provisions that require CSPs and the associated CSO projects meet FedRAMP requirements.
iv. OMB PortfolioStat data quarterly to identify use of CSPs and agency plans to meet FedRAMP requirements, and provide agency-specific rationale to support lack of compliance.
v. Issuing the initial agency authorization.
vi. Reviewing CSP documentation and test results prior to leveraging a JAB provisional authority to aperate (P-ATO) or leveraging the agency-issued authorization to operate (agency ATO).
vii. Reviewing Plans of Action and Milestones (POA&M) for leveraged CSP CSOs.
viii. Adding any agency-specific controls that may exist above the FedRAMP baseline or above the baseline required by a partnering agency.
ix. Ensuring the submittal of agency ATO security packages.
x. Reviewing all CSP and 3PAO provided documentation for the ATO and continuous monitoring (ConMon), as appropriate.
xi. Ensuring the submittal of Agency ATO memo for each agency authorization packages.

xii. Revoking the ATO of non-compliant CSPs and CSOs.
xiii. Ensuring the agency business unit use of a CSP supplied or agency security package is assessed by a FedRAMP approved 3PAO.

10.8.24.1.3.5
(02-02-2024)
FedRAMP Collaboration Group

(1) FedRAMP recommends agencies create a FedRAMP Collaboration Group to manage the continuous monitoring (ConMon) of a common cloud system. This Collaboration Group should include members from all the agencies currently using and/or committed to using the cloud service.

(2) The Collaboration Group allows the member agencies to share the responsibility of ConMon; reduce the dependency of leveraging agencies on the initial authorizing agency; and collaborate with the CSP and other member agencies to ensure the cloud service continues to meet the member agencies' needs. The Collaboration Group members should establish a charter for sharing this responsibility and for collaborating amongst themselves.

(3) A Collaboration Group can be established whenever there are two or more agencies currently using or committed to using the same cloud system. Agencies may find it easier to establish a Collaboration Group amongst current cloud service users because the agencies are already committed to the service and all have contractual relationships with the CSP.

(4) The Collaboration Group membership will change over time as new agencies leverage the cloud service and other agencies discontinue using the cloud service. CSPs with multiple FedRAMP agency ATO system offerings should maintain Collaboration Groups for each of their service offerings to ensure the correct agencies are engaged.

(5) Refer to the FedRAMP Collaborative ConMon Quick Guide for Collaboration Group guidance.

10.8.24.1.3.6
(02-02-2024)
Office of Safeguards

(1) The IRS Office of Safeguards has developed a Safeguard Computer Security Evaluation Matrix (SCSEM), which is used to evaluate compliance with IRM 11.3 series, and the disclosure of official information for government agencies that have implemented a cloud computing environment that receives, stores, processes or transmits federal tax information (FTI).

10.8.24.1.4
(02-02-2024)
Program Management and Review

(1) The IRS Security Policy Program establishes a framework of security controls to ensure the inclusion of security in the daily operations and management of IRS IT resources. This framework of security controls is provided through the issuance of security policies via the IRM 10.8 series and the development of technology specific security requirement checklists. Stakeholders are notified when revisions to the security policies and security requirement checklists are made.

(2) It is the policy of the IRS:

a. To establish and manage an information security program within all its offices. This policy provides uniform policies and guidance to be used by each office.
b. To protect all IT resources belonging to, or used by, the IRS at a level commensurate with the risk and magnitude of harm that could result from loss, misuse, or unauthorized access to that IT resource.

c. To protect its information resources and allow the use, access, disposition, and disclosure of information in accordance with applicable laws, policies, federal regulations, OMB guidance, Treasury Directives (TDs), NIST Publications, 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), Software Development Life Cycle (SDLC), Information Technology Infrastructure Library (ITIL), and Lean Six Sigma (LSS)) to document and improve IRS IT process and service efficiency and effectiveness.

10.8.24.1.5
(02-02-2024)
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, DISA) for potential revisions to security policies and security requirement checklists. Revisions to security policies and checklists are reviewed by the security policy team, in collaboration with applicable stakeholders, for potential impact to the IRS operational environment.

(2) Security Policy provides a report identifying security policies and security requirement checklists that have recently been revised or are in the process of being revised.

(3) This IRM applies to all IRS information and systems, which include IRS production, development, test, and contractor systems. For systems that store, process, or transmit classified national security information, refer to IRM 10.9.1, Classified National Security Information (NSI), for additional guidance for protecting classified information.

(4) This IRM establishes the minimum baseline security policy and requirements for all IRS Cloud computing systems, in order to:

a. Protect the critical infrastructure and assets of the IRS against attacks that exploit IRS assets.
b. Prevent unauthorized access to IRS assets.
c. Enable IRS IT computing environments to meet the security requirements of this policy and support the business needs of the organization.

(5) Systems designated as High Value Assets (HVA) must implement security controls identified in the CISA High Value Assets (HVA) Overlay 2.0.

a. HVA overlay controls within this IRM are designated with HVA at the end of the requirement.
b. The PM and PT family of controls in the CISA government-wide baseline are excluded from the IRM 10.8.24 baseline.

(6) In the event, there is a discrepancy between this policy and IRM 10.8.1, this IRM has precedence, unless the security controls/requirements in IRM 10.8.1 are more restrictive.

10.8.24.1.6
(02-02-2024)
Terms and Acronyms

(1) Refer to Exhibit 10.8.24-7 for a list of terms, acronyms, and definitions.

10.8.24.1.7
(02-02-2024)
Related Resources

(1) Refer to Exhibit 10.8.24-8 for a list of related resources.

10.8.24.2
(02-02-2024)
Risk Acceptance and Risk-Based Decisions

(1) Any exception to this IRM requires that the authorizing official (AO) make a risk-based decision (RBD).

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

Note: Users can access the RBD application on the Enterprise FISMA Compliance SharePoint site via the Risk Acceptance Requests link at: *https://irsgov.sharepoint.com/sites/CyberSRM/SitePages/RiskBasedDecision.aspx*

#
#
#
#
#

#
#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#
#
#

#
#

#
#
#
#

#
#

#
#
#

#
#
#

#
#
#
#
#

#
#

#
#

#

#
#

#

#
#

#
#

#
#

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

#
#
#

#
#

#
#
#

#
#

#
#

#

#
#
#
#
#
#
#

#
#
#

#
#

#
#
#

#
#

#

#
#
#
#

#
#
#

#
#
#

#
#

#
#

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

#
#

#
#
#
#
#
#
#
#

#
#
#
#
#
#
#

#
#
#
#

#

#
#
#
#

#
#
#
#
#
#
#

#
#

#
#
#
#
#
#
#

#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#

#

#
#
#

#
#

#
#

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

#
#
#

#
#

#
#

#
#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#

#
#
#
#
#
#
#

#
#
#

#
#

#
#
#

#
#
#

#
#
#

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

#
#

#
#

#
#

#
#

#
#
#
#
#

#
#

#
#
#
#

#
#

#
#

#
#
#
#
#
#
#

#
#
#

#
#

#
#

#
#
#
#
#

#
#

#
#

#
#

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

#
#
#

#
#

#
#
#
#

#
#
#
#

#
#

#
#
#

#
#

#
#

#
#
#
#

#
#

#
#

#
#
#

#
#
#

#
#
#

#
#

#
#
#

#

#
#
#
#
#
#
#
#
#

#
#

#
#

#
#

#
#
#

#
#
#
#

#
#
#
#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#

#
#

#

#
#
#

#
#

#
#

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

#
#

#
#

#
#

#
#

#
#

#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#

#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#

#
#

#
#
#
#

#
#
#

#
#

#
#
#

#
#

#
#

#
#
#
#

#
#
#
#

#
#
#
#
#
#
#

#
#

#

#
#
#
#
#

#
#
#
#
#

#
#
#

#
#
#
#
#
#
#

#
#

#
#
#
#
#
#
#

#
#

#
#

#
#
#

#
#
#

#
#
#

#
#

#
#
#

#
#
#
#
#

#
#
#
#

#
#

#

#
#
#

#
#

#
#

#
#
#
#
#
#
#

#

#
#

#
#

#
#

#
#

#
#
#
#
#
#
#

#
#
#
#

#
#

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

#

#
#
#
#
#
#
#
#
#

#

#
#
#
#
#
#

#
#

#
#

#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#

#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#

#

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

#
#

#
#
#
#
#
#
#
#

#

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

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

#
#
#
#
#
#
#
#
#
#
#

#

#
#
#

#
#
#
#
#
#

#

#
#
#
#
#
#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#
#
#
#
#
#
#

#
#

#

#
#
#

#
#

#
#

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

#
#

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

#
#

#
#
#

#
#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#
#

#
#

#
#

#
#
#
#
#
#

#
#
#

#
#
#
#

#
#
#
#
#
#

#
#
#
#

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

#
#
#

#

#
#
#

#
#

#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#

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

#
#
#
#

#
#
#

#
#
#

#
#

#
#

#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#

#
#
#
#
#
#
#
#
#
#

#
#
#
#
#
#
#
#
#

#
#
#

#
#
#
#

#
#

#
#
#
#
#

#
#
#

#
#

#
#
#

#
#
#

#

#
#

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

#

#

#
#
#
#
#

#
#
#
#
#

#
#
#

#
#
#

#
#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#

#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#

#
#
#
#

#

#
#
#
#

#
#
#
#
#
#
#

#
#

#
#
#

#
#
#
#
#
#

#
#
#

#
#
#
#

#

#
#
#
#
#
#
#
#

#
#
#

#
#

#
#
#

#
#

#
#

#
#
#

#
#
#

#

#
#
#
#
#

#
#
#
#

#
#
#
#
#

#
#
#

#
#

#
#

#
#
#
#

#
#
#

#
#
#
#

#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#
#

#
#
#
#
#
#
#
#
#
#
#

#
#

#

#
#
#
#

#
#
#

#
#
#
#
#

#
#

#
#

This Page Intentionally Left Blank

Exhibit 10.8.24-1 (02-02-2024)
Appendix A: FedRAMP Documents and Templates

(1) FedRAMP developed Documents and Templates must be used.

a. The following FedRAMP Key Agency Documents are available at *https://www.fedramp.gov/documents-templates/* and must be utilized:
   i. FedRAMP Agency ATO Review Template
   ii. Package Request Form
   iii. FedRAMP Collaborative ConMon Quick Guide
   iv. Agency ATO Quick Guide
   v. Standard Contract Clauses
   vi. Control Specific Contract Clauses
   vii. FedRAMP Package Validation Process
   viii. FedRAMP Initial Authorization Package Checklist
b. FedRAMP Templates can be located at: *https://www.fedramp.gov/documents-templates/*

The Three (3) Types of FedRAMP Cloud Security Packages:

a. FedRAMP JAB P-ATO: Either a CSP or an Agency can make a request to have a system processed for a JAB P-ATO by submitting an Initiate Request form on www.fedramp.gov. For JAB P-ATOs, the JAB will provide the risk review of all documentation provided by the CSP in the security authorization package. CSPs will work with the FedRAMP PMO through the FedRAMP SAF and present all documentation to the JAB for risk review. When the JAB grants the P-ATO, the JAB will provide a recommendation to all Federal Agencies about whether a cloud service has a recommended acceptable risk posture for Federal Government use at the designated data impact levels. For FedRAMP JAB P-ATOs, CSPs must contract with an accredited 3PAO to independently verify and validate the security implementations and the security assessment package. (FedRAMP)
b. FedRAMP AGENCY ATO: CSPs may work directly with an Agency to obtain a FedRAMP Agency ATO. In this case, the Federal Agency will provide the risk review of all documentation provided by the CSP in its security authorization package. CSPs will work directly with the Federal Agency security office and present all documentation to the Authorizing Official (AO) or equivalent for an authorization. If a non-accredited assessor is used, the Agency must provide evidence of the assessor's independence and provide a letter of attestation of the assessor's independence with the security authorization package. The FedRAMP PMO highly recommends Agencies select an assessor from the FedRAMP 3PAO accreditation program. Once an Agency authorizes a package, the Agency must inform the FedRAMP PMO. (FedRAMP)
c. CSP SUPPLIED PACKAGE: CSPs may supply a security package to the FedRAMP Secure Repository for prospective Agency use. For CSP-supplied packages, CSPs must contract with an accredited 3PAO to independently verify and validate the security implementations and the security assessment package. If an Agency decides to issue an ATO to a CSP-supplied package, the status of the package will be changed in the Secure Repository to indicate that it has evolved to a FedRAMP Agency ATO package. (FedRAMP)

Exhibit 10.8.24-2 (02-02-2024)
Appendix B: Cloud Deployment Requirements for IRS Systems

IRS System Data Type	FedRAMP Cloud FIPS 199 Level	Cloud Deployment Model
• Public • Public Releasable Information Types	• Low • Low-Tailored	• Public • Private • Government Community (Local, State, Federal, Tribal and their Contractors tenants) • Hybrid (Any combination of Public, Private, and Government Community including Local, State, Federal, Tribal and their Contractors tenants)
• Sensitive but Unclassified (SBU) • Personal Identifiable Information (PII) • Federal Tax Information (FTI) (Systems containing FTI with a **Low or Moderate** reputational risk*)	• Moderate	• Private • Government Community (Local, State, Federal, Tribal and their Contractors tenants) • Hybrid (Any combination of Private, and Government Community including Local, State, Federal, Tribal and their Contractors tenants)
• Moderate Information Types (FIPS 199 Moderate and/High Systems (Systems with High Reputational Risk*) • Federal Tax Information (FTI) - FIPS 199 Moderate • High Value Assets (HVA) • If the current IRS system is categorized as High	• High	• Private • Government Community (Local, State, Federal, Tribal and their contractors tenants) • Hybrid (Any combination of On-Prem, Private, and Government Community (including Local, State, Tribal and their Contractor tenants)

* Placement in Moderate or High Cloud deployment for FTI at Moderate FIPS 199 levels will be determined based on the Reputational Risk factors risk. The Reputational Risk Assessment Tool (RRAT) must be used to identify additional factors (tailoring) beyond impact. The RRAT can be found on the IRS Cloud Front Door website.

Exhibit 10.8.24-3 (02-02-2024)

Appendix C: FedRAMP Continuous Monitoring Strategy Guide

(1) The following minimum FedRAMP Continuous Monitoring Strategy Guide must be adhered to and can be located at: *https://www.fedramp.gov/documents-templates/*

Exhibit 10.8.24-4 (03-20-2019)

Appendix D: FedRAMP Contract Clauses and Language

1. FedRAMP has developed a security contract clause template to assist federal agencies in procuring cloud-based services.

a. This template should be reviewed by the IRS Chief Counsel to ensure it meets all agency requirements, and then incorporated into the security assessment section of a solicitation.
b. The clauses cover FedRAMP requirements for areas like the security assessment process and related ongoing assessment and authorization. The template also provides basic security requirements identifying Cloud Service Provider responsibilities for privacy and security, protection of government data, personnel background screening and security deliverables with associated frequencies.
c. The clauses can be located in the Key Agency Documents area of the FedRAMP Documents web page at: *https://www.fedramp.gov/documents-templates/*

2. FedRAMP has developed a FedRAMP Control Specific Contract Clauses document, which identifies areas and security controls needing additional specific acquisition/contractual language.

a. The following areas and security controls have been identified as needing additional contractual language:
   i. Data Jurisdiction
   ii. FIPS 140-2 Validated Cryptography for Secure Communications
   iii. AU-10(5): Non-Repudiation - Digital Signature
   iv. AU-11: Audit Record Retention
   v. IA-2(1): Identification and Authentication (Organizational Users) – Network Access to Privileged Accounts
   vi. IA-2(3): Identification and Authentication (Organizational Users) – Local Access to Privileged Accounts
   vii. IA-2(8): Identification and Authentication (Organizational Users) – Network Access to Privileged Accounts - Replay Resistant
   viii. IA-8: Identification and Authentication (Non-Organizational Users)
   ix. IR-6: Incident Reporting
   x. MP-5(2): Media Transport – Documentation of Activities
   xi. MP-5 (4): Media Transport – Cryptographic Protection
   xii. PS-3: Personnel Screening
   xiii. SC-7: Boundary Protection (TIC)
   xiv. SC-28: Protection of Information At Rest
   xv. SI-5: Security Alerts, Advisories, and Directives
b. This document is directed at acquisition and contracting personnel who might need to negotiate specific contractual language for contracts involving cloud computing, and is located in the Key Agency Documents area of the FedRAMP Documents web page at : *https://www.fedramp.gov/documents-templates/*

Exhibit 10.8.24-5 (02-02-2024)

Appendix E: Minimum FedRAMP Security Control Baseline and High Value Asset Overlay

(1) Systems must meet minimum security control baseline requirements. Upon categorizing a system as Low, Moderate, or High sensitivity in accordance with FIPS 199, the corresponding security control baseline standards summarized in the following table apply:

ID	Control Description	Sensitivity Level			High Value Asset Overlay 2.0	
		Low	Moderate	High	HVA Controls	Enterprise Controls
AC - Access Control						
AC-1	Policy and Procedures	AC-1	AC-1	AC-1		
AC-2	Account Management	AC-2	AC-2 (1) (2) (3) (4) (5) (7) (9) (12) (13)	AC-2 (1) (2) (3) (4) (5) (7) (9) (11) (12) (13)	AC-2 (2)	
AC-3	Access Enforcement	AC-3	AC-3	AC-3	AC-3 (9)	
AC-4	Information Flow Enforcement	Not selected	AC-4 (21)	AC-4 (4) (21)	AC-4	
AC-5	Separation of Duties	Not selected	AC-5	AC-5	AC-5	
AC-6	Least Privilege	Not selected	AC-6 (1) (2) (5) (7) (9) (10)	AC-6 (1) (2) (3) (5) (7) (8) (9) (10)	AC-6 (5) (7)	
AC-7	Unsuccessful Logon Attempts	AC-7	AC-7	AC-7		
AC-8	System Use Notification	AC-8	AC-8	AC-8		
AC-10	Concurrent Session Control	Not selected	Not selected	AC-10		
AC-11	Session Lock	Not selected	AC-11(1)	AC-11(1)		
AC-12	Session Termination	Not selected	AC-12	AC-12		
AC-14	Permitted Actions without Identification or Authentication	AC-14	AC-14	AC-14		
AC-17	Remote Access	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)	AC-17 (2)	
AC-18	Wireless Access	AC-18	AC-18 (1) (3)	AC-18 (1) (3) (4) (5)		

Exhibit 10.8.24-5 (Cont. 1) (02-02-2024)
Appendix E: Minimum FedRAMP Security Control Baseline and High Value Asset Overlay

AC-19	Access Control For Mobile Devices	AC-19	AC-19 (5)	AC-19 (5)		
AC-20	Use of External Systems	AC-20	AC-20 (1) (2)	AC-20 (1) (2)	AC-20	
AC-21	Information Sharing	Not selected	AC-21	AC-21		
AC-22	Publicly Accessible Content	AC-22	AC-22	AC-22		
*Control included in baseline by either TD P 85-01 or IRM 10.8.1						
AT-Awareness and Training						
AT-1	Policy and Procedures	AT-1	AT-1	AT-1		
AT-2	Literacy Training and Awareness	AT-2(2)	AT-2 (2) (3)	AT-2 (2) (3)	AT-2 (1)	
AT-3	Role-Based Training	AT-3	AT-3	AT-3		
AT-4	Training Records	AT-4	AT-4	AT-4		
AU - Audit and Accountability						
AU-1	Policy and Procedures	AU-1	AU-1	AU-1		
AU-2	Events Logging	AU-2	AU-2	AU-2	AU-2	
AU-3	Content of Audit Records	AU-3	AU-3 (1)	AU-3 (1)		
AU-4	Audit Log Storage Capacity	AU-4	AU-4	AU-4		
AU-5	Response to Audit Logging Process Failures	AU-5	AU-5	AU-5 (1) (2)		
AU-6	Audit Record Review, Analysis and Reporting	AU-6	AU-6 (1) (3)	AU-6 (1) (3) (4) (5) (6) (7)	AU-6	AU-6 (3) (4) (5)
AU-7	Audit Record Reduction and Report Generation	Not selected	AU-7 (1)	AU-7 (1)		
AU-8	Time Stamps	AU-8	AU-8	AU-8		

Exhibit 10.8.24-5 (Cont. 2) (02-02-2024)
Appendix E: Minimum FedRAMP Security Control Baseline and High Value Asset Overlay

AU-9	Protection of Audit Information	AU-9	AU-9 (4)	AU-9 (2) (3) (4)	AU-9 (2) (3) (5) (6)	
AU-10	Non-repudiation	Not selected	Not selected	AU-10	AU-10	
AU-11	Audit Record Retention	AU-11	AU-11	AU-11		
AU-12	Audit Record Generation	AU-12	AU-12	AU-12 (1) (3)		
AU-16	Cross-Organizational Audit Logging	Not selected	Not selected	Not selected	AU-16	
CA – Security Assessment and Authorization)						
CA-1	Policies and Procedures	CA-1	CA-1	CA-1		
CA-2	Control Assessments	CA-2 (1)	CA-2 (1) (3)	CA-2 (1) (2) (3)		
CA-3	Information Exchange	CA-3	CA-3	CA-3 (6)	CA-3	
CA-5	Plan of Action and Milestones	CA-5	CA-5	CA-5	CA-5	
CA-6	Authorization	CA-6	CA-6	CA-6	CA-6 (1)	
CA-7	Continuous Monitoring	CA-7(4)	CA-7 (1) (4)	CA-7 (1) (4)	CA-7 (3)	
CA-8	Penetration Testing	Not selected	CA-8 (1) (2)	CA-8 (1) (2)		
CA-9	Internal System Connections	CA-9	CA-9	CA-9	CA-9	
CM – Configuration Management						
CM-1	Policy and Procedures	CM-1	CM-1	CM-1		
CM-2	Baseline Configuration	CM-2	CM-2 (2) (3) (7)	CM-2 (2) (3) (7)	CM-2	
CM-3	Configuration Change Control	Not selected	CM-3 (2) (4)	CM-3 (1) (2) (4) (6)	CM-3 (2) (7)	
CM-4	Impact Analyses	CM-4	CM-4 (2)	CM-4 (1) (2)	CM-4(1)	
CM-5	Access Restrictions For Change	CM-5	CM-5 (1) (5)	CM-5 (1) (5)		

Exhibit 10.8.24-5 (Cont. 3) (02-02-2024)
Appendix E: Minimum FedRAMP Security Control Baseline and High Value Asset Overlay

CM-6	Configuration Settings	CM-6	CM-6 (1)	CM-6 (1) (2)	CM-6 (2)	
CM-7	Least Functionality	CM-7	CM-7 (1) (2) (5)	CM-7 (1) (2) (5)	CM-7(1)	
CM-8	System Component Inventory	CM-8	CM-8 (1) (3)	CM-8 (1) (2) (3) (4)	CM-8	
CM-9	Configuration Management Plan	Not selected	CM-9	CM-9		
CM-10	Software Usage Restrictions	CM-10	CM-10	CM-10		
CM-11	User-Installed Software	CM-11	CM-11	CM-11		
CM-12	Information Location	Not selected	CM-12 (1)	CM-12 (1)		
CM-14	Signed Components	Not selected	Not selected	CM-14		
CP – Contingency Planning						
CP-1	Policy and Procedures	CP-1	CP-1	CP-1		
CP-2	Contingency Plan	CP-2	CP-2 (1) (3) (8)	CP-2 (1) (2) (3) (5) (8)		CP-2
CP-3	Contingency Training	CP-3	CP-3	CP-3 (1)		
CP-4	Contingency Plan Testing	CP-4	CP-4 (1)	CP-4 (1) (2)	CP-4	
CP-6	Alternate Storage Site	Not selected	CP-6 (1) (3)	CP-6 (1) (2) (3)		
CP-7	Alternate Processing Site	Not selected	CP-7 (1)(2)(3)	CP-7 (1) (2) (3) (4)	CP-7 (3)	
CP-8	Telecommunications Services	Not selected	CP-8 (1) (2)	CP-8 (1) (2) (3) (4)		CP-8 (5)
CP-9	System Backup	CP-9	CP-9 (1) (8)	CP-9 (1) (2) (3) (5) (8)	CP-9 (1)	
CP-10	System Recovery and Reconstitution	CP-10	CP-10 (2)	CP-10 (2) (4)	CP-10 (4)	
IA - Identification and Authentication						

Exhibit 10.8.24-5 (Cont. 4) (02-02-2024)
Appendix E: Minimum FedRAMP Security Control Baseline and High Value Asset Overlay

IA-1	Policy and Procedures	IA-1	IA-1	IA-1		
IA-2	Identification and Authentication (Organizational Users)	IA-2 (1) (8) (12)	IA-2 (1) (2) (5) (6) (8) (12)	IA-2 (1) (2) (5) (6) (8) (12)	IA-2 (1) (2) (12)	
IA-3	Device Identification and Authentication	Not selected	IA-3	IA-3	IA-3	
IA-4	Identifier Management	IA-4	IA-4 (4)	IA-4 (4)		
IA-5	Authenticator Management	IA-5 (1)	IA-5 (1) (2) (6) (7)	IA-5 (1) (2) (6) (7) (8) (13)	IA-5 (1)	
IA-6	Authenticator Feedback	IA-6	IA-6	IA-6		
IA-7	Cryptographic Module Authentication	IA-7	IA-7	IA-7		
IA-8	Identification and Authentication (Non-Organizational Users)	IA-8 (1) (2) (4)	IA-8 (1) (2) (4)	IA-8 (1) (2) (4)		
IA-11	Re-authentication	IA-11	IA-11	IA-11		
IA-12	Identity Proofing	Not selected	IA-12 (2) (3) (5)	IA-12 (2) (3) (4) (5)		
IR – Incident Response						
IR-1	Policy and Procedures	IR-1	IR-1	IR-1		
IR-2	Incident Response Training	IR-2	IR-2	IR-2 (1) (2)		
IR-3	Incident Response Testing	Not selected	IR-3 (2)	IR-3 (2)		
IR-4	Incident Handling	IR-4	IR-4 (1)	IR-4 (1) (2) (4) (6) (11)	IR-4 (2) (8) (10)	IR-4 (4)
IR-5	Incident Monitoring	IR-5	IR-5	IR-5 (1)	IR-5	
IR-6	Incident Reporting	IR-6 (2)*	IR-6 (1)	IR-6 (1) (3)		

Exhibit 10.8.24-5 (Cont. 5) (02-02-2024)
Appendix E: Minimum FedRAMP Security Control Baseline and High Value Asset Overlay

IR-7	Incident Response Assistance	IR-7	IR-7 (1)	IR-7 (1)		
IR-8	Incident Response Plan	IR-8	IR-8	IR-8		
IR-9	Information Spillage Response	Not selected	IR-9 (2) (3) (4)	IR-9 (2) (3) (4)		
MA - Maintenance						
MA-1	Policy and Procedures	MA-1	MA-1	MA-1		
MA-2	Controlled Maintenance	MA-2	MA-2	MA-2 (2)		
MA-3	Maintenance Tools	Not selected	MA-3 (1) (2) (3)	MA-3 (1) (2) (3)		
MA-4	Nonlocal Maintenance	MA-4	MA-4	MA-4 (3)		
MA-5	Maintenance Personnel	MA-5	MA-5 (1)	MA-5 (1)		
MA-6	Timely Maintenance	Not selected	MA-6	MA-6		
MP – Media Protection						
MP-1	Policy and Procedures	MP-1	MP-1	MP-1		
MP-2	Media Access	MP-2	MP-2	MP-2		
MP-3	Media Marking	Not selected	MP-3	MP-3		
MP-4	Media Storage	Not selected	MP-4	MP-4		
MP-5	Media Transport	Not selected	MP-5	MP-5		
MP-6	Media Sanitization	MP-6	MP-6	MP-6 (1) (2) (3)	MP-6 (8)	
MP-7	Media Use	MP-7	MP-7	MP-7		
PE – Physical and Environmental Protection						
PE-1	Policy and Procedures	PE-1	PE-1	PE-1		
PE-2	Physical Access Authorizations	PE-2	PE-2	PE-2		

Exhibit 10.8.24-5 (Cont. 6) (02-02-2024)
Appendix E: Minimum FedRAMP Security Control Baseline and High Value Asset Overlay

PE-3	Physical Access Control	PE-3	PE-3	PE-3 (1)	PE-3 (1)	
PE-4	Access Control For Transmission	Not selected	PE-4	PE-4		
PE-5	Access Control For Output Devices	Not selected	PE-5	PE-5		
PE-6	Monitoring Physical Access	PE-6	PE-6 (1)	PE-6 (1) (4)		
PE-8	Visitor Access Records	PE-8	PE-8	PE-8 (1)		
PE-9	Power Equipment and Cabling	Not selected	PE-9	PE-9		
PE-10	Emergency Shutoff	Not selected	PE-10	PE-10		
PE-11	Emergency Power	Not selected	PE-11	PE-11(1)		
PE-12	Emergency Lighting	PE-12	PE-12	PE-12		
PE-13	Fire Protection	PE-13	PE-13 (1) (2)	PE-13 (1) (2)		
PE-14	Environmental Controls	PE-14	PE-14	PE-14 (2)		
PE-15	Water Damage Protection	PE-15	PE-15	PE-15 (1)		
PE-16	Delivery and Removal	PE-16	PE-16	PE-16		
PE-17	Alternate Work Site	Not selected	PE-17	PE-17		
PE-18	Location of System Components	Not selected	Not selected	PE-18		
PL – Planning						
PL-1	Policy and Procedures	PL-1	PL-1	PL-1		
PL-2	System Security and Privacy Plans	PL-2	PL-2	PL-2	PL-2	
PL-4	Rules of Behavior	PL-4 (1)	PL-4 (1)	PL-4 (1)		

Exhibit 10.8.24-5 (Cont. 7) (02-02-2024)
Appendix E: Minimum FedRAMP Security Control Baseline and High Value Asset Overlay

PL-8	Security and Privacy Architectures	PL-8	PL-8	PL-8	PL-8 (1)	
PL-10	Baseline Selection	PL-10	PL-10	PL-10	PL-10	
PL-11	Baseline Tailoring	PL-11	PL-11	PL-11		
PS – Personnel Security						
PS-1	Policy and Procedures	PS-1	PS-1	PS-1		
PS-2	Position Risk Designation	PS-2	PS-2	PS-2		
PS-3	Personnel Screening	PS-3	PS-3 (3)	PS-3 (3)		
PS-4	Personnel Termination	PS-4	PS-4	PS-4 (2)		
PS-5	Personnel Transfer	PS-5	PS-5	PS-5		
PS-6	Access Agreements	PS-6	PS-6	PS-6		
PS-7	External Personnel Security	PS-7	PS-7	PS-7		
PS-8	Personnel Sanctions	PS-8	PS-8	PS-8		
PS-9	Position Descriptions	PS-9	PS-9	PS-9		
RA – Risk Assessment						
RA-1	Policy and Procedures	RA-1	RA-1	RA-1		
RA-2	Security Categorization	RA-2	RA-2	RA-2	RA-2	
RA-3	Risk Assessment	RA-3 (1)	RA-3 (1)	RA-3 (1)	RA-3 (1)	RA-3
RA-5	Vulnerability Monitoring and Scanning	RA-5 (2) (11)	RA-5 (2) (3) (5) (11)	RA-5 (2) (3) (4) (5) (11)	RA-5 (6) (10)	
SA – System and Services Acquisition						
SA-1	Policy and Procedures	SA-1	SA-1	SA-1		

Exhibit 10.8.24-5 (Cont. 8) (02-02-2024)
Appendix E: Minimum FedRAMP Security Control Baseline and High Value Asset Overlay

SA-2	Allocation of Resources	SA-2	SA-2	SA-2		
SA-3	System Development Life Cycle	SA-3	SA-3	SA-3		
SA-4	Acquisition Process	SA-4 (10)	SA-4 (1) (2) (9) (10)	SA-4 (1) (2) (5) (9) (10)	SA-4	
SA-5	System Documentation	SA-5	SA-5	SA-5		
SA-8	Security and Privacy Engineering Principles	SA-8	SA-8	SA-8		
SA-9	External System Services	SA-9	SA-9 (1) (2) (5)	SA-9 (1) (2) (5)	SA-9	
SA-10	Developer Configuration Management	Not selected	SA-10 (1)	SA-10 (1)		
SA-11	Developer Testing and Evaluation	Not selected	SA-11 (1) (2)	SA-11 (1) (2)	SA-11 (1) (2) (4) (5) (8)	
SA-15	Development Process, Standards and Tools	Not selected	SA-15 (3)	SA-15 (3)		
SA-16	Developer-Provided Training	Not selected	Not selected	SA-16		
SA-17	Developer Security and Privacy Architecture and Design	Not selected	Not selected	SA-17		
SA-21	Developer Screening	Not selected	Not selected	SA-21		
SA-22	Unsupported System Components	SA-22	SA-22	SA-22		
SC – System and Communications Protection						
SC-1	Policy and Procedures	SC-1	SC-1	SC-1		
SC-2	Separation of System and User Functionality	Not selected	SC-2	SC-2		

Exhibit 10.8.24-5 (Cont. 9) (02-02-2024)
Appendix E: Minimum FedRAMP Security Control Baseline and High Value Asset Overlay

SC-3	Security Function Isolation	Not selected	Not selected	SC-3	SC-3 (2)	
SC-4	Information In Shared System Resources	Not selected	SC-4	SC-4		
SC-5	Denial- of-Service Protection	SC-5	SC-5	SC-5	SC-5 (1) (2) (3)	
SC-7	Boundary Protection	SC-7	SC-7 (3) (4) (5) (7) (8) (12) (18)	SC-7 (3) (4) (5) (7) (8) (10) (12) (18) (20) (21)	SC-7 (3) (5) (10) (11) (12) (14) (17) (21) (22)	
SC-8	Transmission Confidentiality and Integrity	SC-8 (1)	SC-8 (1)	SC-8 (1)	SC-8	
SC-10	Network Disconnect	Not selected	SC-10	SC-10		
SC-12	Cryptographic Key Establishment and Management	SC-12	SC-12	SC-12 (1)		
SC-13	Cryptographic Protection	SC-13	SC-13	SC-13		
SC-15	Collaborative Computing Devices and Applications	SC-15	SC-15	SC-15		
SC-17	Public Key Infrastructure Certificates	Not selected	SC-17	SC-17		
SC-18	Mobile Code	Not selected	SC-18	SC-18	SC-18 (4)	
SC-20	Secure Name/ Address Resolution Service (Authoritative Source)	SC-20	SC-20	SC-20		

Exhibit 10.8.24-5 (Cont. 10) (02-02-2024)
Appendix E: Minimum FedRAMP Security Control Baseline and High Value Asset Overlay

SC-21	Secure Name/ Address Resolution Service (Recursive or Caching Resolver)	SC-21	SC-21	SC-21		
SC-22	Architecture and Provisioning for Name/Address Resolution Service	SC-22	SC-22	SC-22		
SC-23	Session Authenticity	Not selected	SC-23	SC-23		
SC-24	Fail in Known State	Not selected	Not selected	SC-24		
SC-28	Protection of Information At Rest	SC-28 (1)	SC-28 (1)	SC-28 (1)	SC-28 (1)	
SC-39	Process Isolation	SC-39	SC-39	SC-39		
SC-45	System Time Synchronization	Not selected	SC-45 (1)	SC-45 (1)		
SI – System and Information Integrity						
SI-1	Policy and Procedures	SI-1	SI-1	SI-1		
SI-2	Flaw Remediation	SI-2	SI-2 (2) (3)	SI-2 (2) (3)	SI-2	
SI-3	Malicious Code Protection	SI-3	SI-3	SI-3	SI-3	
SI-4	System Monitoring	SI-4	SI-4 (1) (2) (4) (5) (16) (18) (23)	SI-4 (1) (2) (4) (5) (10) (11) (12) (14) (16) (18) (19) (20) (22) (23)	SI-4 (1) (10) (11) (13) (18) (20) (22) (23)	SI-4 (16)
SI-5	Security Alerts, Advisories and Directives	SI-5	SI-5	SI-5 (1)	SI-5	
SI-6	Security and Privacy Function Verification	Not selected	SI-6	SI-6		

Exhibit 10.8.24-5 (Cont. 11) (02-02-2024)
Appendix E: Minimum FedRAMP Security Control Baseline and High Value Asset Overlay

SI-7	Software, Firmware and Information Integrity	Not selected	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (15)		
SI-8	Spam Protection	Not selected	SI-8 (2)	SI-8 (2)		
SI-10	Information Input Validation	Not selected	SI-10	SI-10		
SI-11	Error Handling	Not selected	SI-11	SI-11		
SI-12	Information Handling and Retention	SI-12	SI-12	SI-12		
SI-16	Memory Protection	Not selected	SI-16	SI-16		
SR- Supply Chain Risk Management						
SR-1	Policy and Procedures	SR-1	SR-1	SR-1		
SR-2	Supply Chain Risk Management Plan	SR-2 (1)	SR-2 (1)	SR-2 (1)		
SR-3	Supply Chain Controls and Processes	SR-3	SR-3	SR-3		
SR-4	Provenance	Not selected	Not selected	Not selected	SR-4 (2) (3)	
SR-5	Acquisition Strategies, Tools, and Methods	SR-5	SR-5	SR-5	SR-5 (2)	
SR-6	Supplier Assessments and Reviews	Not selected	SR-6	SR-6		SR-6
SR-8	Notification Agreements	SR-8	SR-8	SR-8		
SR-9	Tamper Resistance and Detection	Not selected	Not selected	SR-9 (1)	SR-9	
SR-10	Inspection of Systems or Components	SR-10	SR-10	SR-10	SR-10	
SR-11	Component Authenticity	SR-11(1) (2)	SR-11(1) (2)	SR-11 (1) (2)		

Exhibit 10.8.24-5 (Cont. 12) (02-02-2024)
Appendix E: Minimum FedRAMP Security Control Baseline and High Value Asset Overlay

SR-12	Component Disposal	SR-12	SR-12	SR-12		

Note: The high value asset overlay controls in this IRM are intended to be implemented at the HVA system/component level, while the enterprise controls must be implemented at the enterprise level to secure the enterprise systems, architectures, and networks that support HVA operations.

Exhibit 10.8.24-6 (02-02-2024)
Appendix G: Terms and Acronyms

0-9

3PAO – Third Party Assessment Organization: Within FedRAMP, 3PAOs perform initial and ongoing independent verification and validation of the security controls deployed within the Cloud Service Provider's system

A

A2LA – American Association for Laboratory Accreditation

Authentication Assurance Levels (AAL) – The robustness of the authentication process itself, and the binding between an authenticator and a specific individual's identifier. AAL is selected to mitigate potential authentication failures.

Authorizing official (AO) – A senior (federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

AoA – Analysis of Alternatives

ASHRAE – American Society of Heating, Refrigerating and Air-conditioning Engineers

Authority to operate (ATO) – The official management decision given by a senior Federal official or officials to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security and privacy controls. Authorization also applies to common controls inherited by agency information systems.

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.

Authorized individuals (services, and other IoT product components) - An entity (i.e., a person, device, service, network, domain, developer, or other party who might interact with an IoT device) that has implicitly or explicitly been granted approval to interact with a particular IoT device.

Authorized User - Any appropriately cleared individual with a requirement to access an information system (IS) for performing or assisting in a lawful and authorized governmental function.

B

Baseline – Benchmark used as a reference point:

1. Configuration Management Baseline can enable the IT Infrastructure to be restored to a known configuration if a change or release fails.
2. Performance Baseline can measure change in performance over the lifetime of an IT Service.
3. Security Baseline can document the security of a system as security requirements and expectations.

CAC – Common Access Card

Certificate - Refer to Digital Certificate

CIO - Chief Information Officer

Exhibit 10.8.24-6 (Cont. 1) (02-02-2024)
Appendix G: Terms and Acronyms

CIS - Center for Internet Security

CISA - Cybersecurity & Infrastructure Security Agency

CISO – Chief Information Security Officer

Client – A machine or software application that accesses a cloud over a network connection. This can be on behalf of a consumer.

Cloud Computing – A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud Service Model – Three service models:

1. Infrastructure as a Service (IaaS): Infrastructure includes virtual machines, servers, storage, load, balancers, network, etc.
2. Platform as a Service (PaaS): Platform includes execution runtime, database, web server, development tools, etc.
3. Software as a Service (SaaS): Software includes Email, virtual desktop, communication, applications, etc.

CSO - Cloud Service Offering (See Cloud Service Model)

Cloud Service Provider (CSP) – Also referred to as service provider or provider. Any organization that provides cloud services (Commercial vendor or Federal organization).

Compliance – Conformity in fulfilling official requirements

ConMon - Continuous Monitoring

CSIRC - Computer Security Incident Response Center

D

Data Portability - Defines the ability to physically move application or data from one system to another. Also the ability to move data among different application programs, computing environments or cloud services.

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

DoD – Department of Defense

E

EA – Enterprise Architecture

F

Exhibit 10.8.24-6 (Cont. 2) (02-02-2024)
Appendix G: Terms and Acronyms

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 information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

Federal Assurance Level (FAL) – The robustness of the federation process used to communicate authentication and attribute information (if applicable) to an rely party from an identity provider. FAL is optional as not all digital systems will leverage federated identity architectures. FAL is selected to mitigate potential federation failures.

FedRAMP – Federal Risk and Authorization Management Program

FICAM – The government-wide effort to provide policy and programmatic support for identity, credential, and access management business functions within the Federal Government. It is governed by the ICAMSC within the Federal CIO Council and managed operationally by the GSA Office of Government wide Policy. It addresses the convergence of HSPD-12 and the Federal PIV infrastructure, Federal PKI Management and Policy Authorities and FICAM governance/guidance

FIPS – Federal Information Processing Standards

FTI – Federal Tax Information

G

GSA – General Services Administration

H

HTML – Hypertext Markup Language

HTTP – Hypertext Transfer Protocol

HTTPS - Hypertext Transfer Protocol Secure

High Value Asset (HVA) - Federal information systems, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the United States's national security interests, foreign relations, economy, or the public confidence, civil liberties, or public health and safety of the American people. HVA can fall into one of three categories:
• Informational value - The information or information system that processes, stores, or transmits the information is of high value to the Government or its adversaries.
• Mission Essential – The agency that owns the information or information system cannot accomplish its Primary Mission Essential Functions (PMEF), as approved in accordance with Presidential Policy Directive 40 (PPD-40) National Continuity Policy, within expected timelines without the information or information system.
• Federal Civilian Enterprise Essential (FCEE) – The information or information system serves a critical function in maintaining the security and resilience of the federal civilian enterprise.

I

IaaS – Infrastructure as a Service

Identity Assurance Level (IAL) – The robustness of the identity proofing process to confidently determine the identity of an individual. IAL is selected to mitigate potential identity proofing failures.

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

Exhibit 10.8.24-6 (Cont. 3) (02-02-2024)
Appendix G: Terms and Acronyms

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

Information Technology (IT) - Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by an executive agency. For purposes of the preceding definition, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which:

1) requires the use of such equipment or;.

2) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term information technology includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services) and related resources.

IRC – Internal Revenue Code

J

JAB – Joint Authorization Board: Part of FedRAMP, the JAB performs risk authorizations and grants the FedRAMP provisional ATO. The JAB is the primary governance and decision-making body for the FedRAMP program.

N

NARA - National Archives and Records Administration

NIST - National Institute of Standards and Technology

NSA - National Security Agency

O

OMB - Office of Management and Budget

On-Premise - Cloud computing that resides on the premises of the Cloud user (i.e., Treasury or IRS facility)

P

PA - Provisional Authorization

P-ATO – Provisional Authorization to Operate

PaaS – Platform as a Service

PDS – Protective Distribution System

PKI – Public Key Infrastructure

PII – Personally Identifiable Information

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.

Exhibit 10.8.24-6 (Cont. 4) (02-02-2024)
Appendix G: Terms and Acronyms

PMO – Program Management Office

Plan of Action and Milestones (POA&M) – A Plan of Action and Milestones (POA&M) is a requirement for managing the security weaknesses pertaining to a specific application or system. In addition to noting weaknesses, each POA&M details steps that need to be taken to correct or mitigate any weaknesses, as well as resources required to accomplish task milestones and a correction/mitigation timeline. POA&M are intended to help identify, assess and prioritize security weaknesses, and monitor progress on appropriate corrective actions. In order to meet FISMA requirements, agencies like the IRS must maintain POA&M, in Treasury FISMA Inventory Management System (TFIMS), for each system in their inventory.

R

RAR - Readiness Assessment Report

Reputational Risk Assessment Tool (RRAT) - The RRAT is used in conjunction with the FIPS-199 categorization of the system to identify the Cloud Service level (Moderate, High) required to Host IRS Systems according to their information type.

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.

S

SA – System Administrator

SaaS – Software as a Service

SAISO – Senior Agency Information Security Officer

SAP - Security Assessment Plan

SAR - Security Assessment Report

Sensitive But Unclassified (SBU) - Any information which if lost, stolen, misused, or accessed or altered without proper authorization, may adversely affect the national interest or the conduct of federal programs (including IRS operations), or the privacy to which individuals are entitled under FOIA (5 U.S.C. 552).

SCSEM – Safeguard Computer Security Evaluation Matrix

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.

SOP – Standard Operating Procedure

SP – NIST Special Publication

SRG – Security Requirements Guide

Exhibit 10.8.24-6 (Cont. 5) (02-02-2024)
Appendix G: Terms and Acronyms

STIG – Security Technical Implementation Guide

T

TD P - Treasury Directive Publication

TIC - Trusted Internet Connection

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

U

United States Government Configuration Baseline (USGCB) – The USGCB replaces the Federal Desktop Core Configuration (FDCC) and provides the baseline settings that Federal agencies are required to implement for security and environmental reasons. The USGCB initiative is to create security configuration baselines for Information Technology products widely deployed across the federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate. The USGCB is a Federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain an effective configuration settings focusing primarily on security. Refer to *http://usgcb.nist.gov/* for more information.

Unrestricted Data: Public facing, publicly available data

US-CERT - United States Computer Emergency Readiness Team

Exhibit 10.8.24-7 (02-02-2024)
Appendix H: Related Resources

IRS Publications

1. IRM 10.8.1 – *Information Technology (IT) Security, Security Policy and Guidance*
2. IRM 10.8.2 – *Information Technology (IT) Security, Security Roles and Responsibilities*
3. IRM 10.8.62 – *Information Technology (IT) Security, Information Systems Contingency Plan (ISCP)*
4. IRM 10.8.50 – *Information Technology (IT) Security, Service-wide Security Patch Management*
5. IRM 10.9.1 - *Classified National Security Information*
6. IRM 10.5.1 - *Privacy and Information Protection, Privacy Policy*
7. IRM 1.15 series - *Records and Information Management*
8. IRM 11.3 series - *Disclosure of Official Information*

Treasury Publications

1. TD P 85–01 Volume I (Non-National Security Systems), Version 3.1, *Department of Treasury Information Technology Security Program*, October 03, 2020

NIST Publications

1. NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, May 2010 (amended November 11, 2010)
2. NIST SP 800-37 Rev 2, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, December 20, 2018
3. NIST SP 800-53 Rev 5, *Security and Privacy Controls for Information Systems and Organizations*, December 10, 2020
4. NIST SP 800-57 Rev 5, *Recommendation for Key Management, Part 1: General* June 4, 2020
5. NIST SP 800-60 Volume 1, Rev 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 1, 2008
6. NIST SP 800-61 Rev 2, *Computer Security Incident Handling Guide*, August 6, 2012
7. NIST SP 800-63 Rev 3, *Digital Identity Requirements*, March, 2, 2020
8. NIST SP 800-144, *Guidelines on Security and Privacy in Public Cloud Computing*, December 9, 2011
9. NIST SP 800-145, *The NIST Definition of Cloud Computing*, September 28, 2011
10. NIST SP 800-146, *Cloud Computing Synopsis and Recommendations*, May 29, 2012
11. NIST SP 800-171 Rev 2, *Protecting Unclassified Information in Nonfederal Information Systems and Organizations*, January 28, 2021
12. FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
13. FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*

Federal Publications

1. Federal Risk and Authorization Management Program (FedRAMP) Home Page *https://www.fedramp.gov*
2. Federal Cloud Computing Strategy, June 24, 2019
3. FedRAMP Collaborative ConMon Quick Guide, August 30, 2023
4. OMB Memo, Security Authorization of Information Systems in Cloud Computing Environments, December 8, 2011
5. OMB Memo M-13-08, Improving Financial System Through Shared Services, March 23, 2013
6. OMB Memo M-13-09, Fiscal Year 2013 Portfolio Guidance: Strengthening Federal IT Portfolio Management, March 27, 2013
7. OMB Memo M-21-31, Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incident, August 27, 2021
8. OMB M-22-09, Moving the U.S. Government Toward Zero Trust Cybersecurity Principles, January 26, 2022

Exhibit 10.8.24-7 (Cont. 1) (02-02-2024)
Appendix H: Related Resources

9. OMB Memos and Circulars *https://www.whitehouse.gov/omb/information-for-agencies/circulars*

Other Publications

ASHRAE - Thermal Guidelines for Data Processing Environments