FISMA Contract Language
(IT Systems / Applications or Services)
Revised August 2023

INFORMATION SECURITY / FEDERAL INFORMATION SECURITY MODERNIZATION ACT (FISMA)

Pursuant to the Federal Information Security Modernization Act (FISMA), Title III of the E-Government Act of 2014 (Pub. L. 113–283), the contractor shall provide minimum security controls required to protect Federal information and information systems in accordance with NIST Special Publication 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations. The contractor shall provide a risk-based process for selecting the security controls necessary to satisfy the minimum-security requirements in accordance with Federal Information Processing Standard (FIPS) 199. The term *information security* means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentially, integrity and availability. An *information system* is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information resources include information and related resources, such as personnel, equipment, funds, and information technology.

The contractor shall provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by or on behalf of the agency; or information systems used or operated by an agency or by a contractor or subcontractor of an agency. This applies to individuals and organizations having contractual arrangements with the IRS, including employees, contractors, vendors, and outsourcing providers, which use or operate information technology systems containing IRS data.

IRS information or information system with a FIPS 199 security categorization impact level of low, moderate or high, and those systems identified by the As Built Architecture (ABA) and agency FISMA Master Inventory.

The potential impact values for confidentiality, integrity, and availability may not always be the same for a particular information system; the high-water mark concept must be used to determine the overall impact level of the information system. Thus, a *low-impact system* is an information system in which all three of the security objectives are low. A *moderate-impact system* is an information system in which at least one of the security objectives is moderate and no security objective is greater than moderate. And finally, a *high-impact system* is an information system in which at least one security objective is high. The determination of information system impact levels must be accomplished prior to the consideration of minimum-security requirements and the selection of appropriate security controls for those information systems.

Federal Risk and Authorization Management Program (FedRAMP) security requirements shall be applied to all IRS cloud services and products and shall be implemented and complied with as part of a competed FedRAMP authorization.

The enforcement of FedRAMP requirements shall be done through Service Level Agreements(SLA)/Contracts. IRS shall utilize aggregated and individual security categorization information when assessing interagency and Cloud Service Provider (CSP) connections with different FIPS 199Category Impact levels.(e.g., High Impact system connecting to Moderate Impact system etc.)

THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)GUIDANCE FOR INFORMATION SECURITY

The contractor shall follow Information Security guidance established by the National Institute of Standards and Technology (NIST). The contractor shall establish the minimum-security controls identified in NIST Special Publication 800-53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations for FISMA compliance. The contractor shall follow the best practices and guidance established by NIST Special Publication 800 Series and Federal Information Processing Standards (FIPS) for computer security. The IRS may determine such applicable Information Technology (IT) Security standards and policies.

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM) CONTRACT LANGUAGE

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM)

Pursuant to the Federal Information Security Modernization Act (FISMA), Title III of the E-Government Act of 2014 (Pub. L. 113–283), the contractor shall comply with the security controls required to protect Federal information and information systems in accordance with NIST Special Publication 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations and NIST Special Publication 800-161 Rev 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. Additionally, the contractor must comply with guidance provided in Executive Order (EO) 14028, Improving the Nation's Cybersecurity (May 12, 2021), which focuses on the security and integrity of the software supply chain and emphasizes the importance of secure software development environments and NIST Secure Software Development Framework (SSDF), SP 800-218.

The Federal Information Security Modernization Act of 2014 (FISMA) requires all Federal agencies provide security protections for both "information collected or maintained by or on behalf of an agency" and for "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." This contract language is applicable to all Information and Communications technology (ICT) and operational technology (OT) which includes commercial off-the-shelf (COTS) products.

Ensuring software integrity is key to protecting Federal systems from threats and vulnerabilities and reducing overall risk from cyber-attacks. Federal agencies must only use software provided by software producers who can attest to and demonstrate complying with the Government-specified secure software development practices, Security and Privacy controls and Cybersecurity Supply Chain Risk Management Practices, as described in the NIST Guidance.

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM) STRATEGY

An organization-wide supply chain risk management strategy includes an unambiguous expression of the supply chain risk appetite and tolerance for the organization, acceptable supply chain risk mitigation strategies or controls, a process for consistently evaluating and monitoring supply chain risk, approaches for implementing and communicating the supply chain risk management strategy, and the associated roles and responsibilities.

Continuous monitoring at the organization level facilitates ongoing awareness of the security and privacy posture across the organization to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess and monitor their controls and risks at a frequency sufficient to support risk-based decisions. Different types of controls may require different monitoring frequencies. The results of continuous monitoring guide and inform risk response actions by organizations. Continuous monitoring programs allow organizations to maintain the authorizations of systems and common controls in highly dynamic environments of operation with changing mission and business needs, threats, vulnerabilities, and technologies. Having access to security- and privacy-related information on a continuing basis through reports and dashboards gives organizational officials the capability to make effective, timely, and informed risk management decisions, including ongoing authorization decisions.

The contractor shall develop and provide an organization-wide strategy for managing supply chain risks associated with the development, acquisition, maintenance, and disposal of systems, system components, and system services.

CYBERSECURITY SUPPLY CHAIN RISK MANAGEMENT (C-SCRM) PLAN

The dependence on products, systems, and services from external providers, as well as the nature of the relationships with those providers, present an increasing level of risk to an organization. Threat actions that may increase security or privacy risks include unauthorized production, the insertion or use of counterfeits, tampering, theft, insertion of malicious software and hardware, and poor manufacturing and development practices in the supply chain.

The Contractor shall provide evidence of a C-SCRM Plan that identifies supply chain risk with their product or services, components, suppliers, and contractors. The Contractor shall review and update the supply chain risk management plan annually or as required, to address threat, organizational or environmental changes. The Contractor shall follow the standards set forth by the control families of NIST SP 800-53 and by the cybersecurity supplemental guidance provided by NIST SP 800-161 Rev 1. These represent the Security and Privacy Controls for Information Systems and Organizations. Following these standards, the Contractor Shall identify and address weaknesses or deficiencies in the supply chain elements and processes of organization-defined system or system component in this procurement.

CYBERSECURITY SUPPLY CHAIN RISK ASSESSMENT (C-SCRA)

The Contractor shall manage the supply chain risk lifecycle of their products, services and subcontractor tiers using risk assessment methods and procedures identified by NIST SP 800-161 Rev 1. The assessment shall consider documented processes, documented controls, all-source intelligence, public information, foreign ownership, control, or influence (FOCI), Country of Origin (COO), ownership and leadership personnel, comparisons against Federal Government restriction lists, and identification of product vulnerabilities through national known vulnerability databases. The assessment and reviews shall demonstrate the ability of the Contractor to effectively assess subordinate second-tier and third-tier suppliers and contractors. The contractor shall assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide.

During all contract phases, including the Request for Proposal (RFP) and/or Request for Information (RFI), the contractor shall provide responses to the IRS C-SCRA Questionnaire that contains a list of questions based on NIST SP 800-53 Revision 5 Supply Chain Risk Management security controls and NIST SP 800-161 Rev 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations. The questionnaire is tailored for each procurement to assess the maturity of the Contractor's C-SCRM capabilities and any C-SCRM related risks relating to the Contractor and its supplier supply chain components, subsystems, intellectual property, and other services relevant to this procurement. The questionnaire supports the C-SCRA process. The SCRA may include reviewing the subcontractors, suppliers, distributers, manufacturers, or any other sources involved in the awardee's supply chain. This shall be provided at no additional cost to the Federal Government. For any risks identified, the contractor shall create Plan of Action & Milestones (POA&M) to identify and track remediation of the identified risks/vulnerabilities. The contractor shall report POA&M progress to the government as requested and at minimum quarterly. The contractor shall notify the IRS immediately of any supply chain compromises or critical vulnerabilities that could lead to a compromise. Early detection and notification are critical to allow an effective and timely response to a suspected or actual incident.

SELF-ATTESTATION

The contractor shall provide a self-attestation letter that will serve as a "conformance statement" for all third-party software used by the agency, including software renewals and major version changes upon or prior to award. For any practices from the NIST guidance that the software producer cannot attest, the contractor shall provide documented practices in place to mitigate those risks along with a Plan of Action & Milestone (POA&M) to remediate in accordance with Office of Management and Budget (OMB) Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices.

MALICIOUS CODE DETECTION AND PROTECTION

In situations where malicious code cannot be detected by detection methods or technologies, organizations rely on other types of controls, including secure coding practices, configuration management and control, trusted procurement processes, and monitoring practices to ensure that software does not perform functions other than the functions intended.

The Contractor shall monitor code using code protection mechanisms at the entrance and exit points to identify signature and non-signature malicious code in accordance with NIST SP 800-53. The protection is required to ensure software behaves according to its designed functions. The Contractor shall maintain/update the malicious code protection; block, quarantine and/or remove any malicious code; perform real-time and routine periodic malicious code protection scans and address false positives. The contractor shall develop and implement tampering and anti-counterfeit policies and procedures to detect tampering and prevent counterfeit components from entering the system.

VULNERABILITY MONITORING AND SCANNING

Vulnerability monitoring includes scanning for patch levels; scanning for functions, ports, protocols, and services that should not be accessible to users or devices; and scanning for flow control mechanisms that are improperly configured or operating incorrectly.

The Contractor shall, monitor and scan for vulnerabilities in the system and hosted applications using vulnerability monitoring tools and techniques, and when new vulnerabilities potentially affecting the system are identified and reported, perform analysis and remediation activities. For any vulnerabilities identified that cannot be remediated within 30 days, the contractor shall create POA&Ms to identify and track remediation of the identified risks/vulnerabilities. The contractor shall report POA&M progress to the government as requested and at minimum monthly.

SOFTWARE DEVELOPMENT

The Contractor shall comply with NIST Secure Software Development Framework (SSDF) SP 800-218 for its products and services or map to the SSDF to demonstrate a framework for well-secured products.

The Contractor shall apply the SSDF to the entire product lifecycle including design, development, testing and operations. As part of these practices the Contractor shall secure all code in a software versioning library located in a secured environment with access enabled for the government requirements, software review and oversight roles. This tool shall facilitate task management, versioning, check-in/check-out/commits, reporting, testing, automation, deficiencies, and vulnerabilities, debugging, flagging and traceability as examples.

The Contractor shall provide software and systems emphasizing authentication, logging, and monitoring capabilities that detect unusual behavior consistent with NIST 800-53 Security controls.

The Contractor shall use a published secure coding standard or provide their secure coding process for all application development following NIST Secure Software Development Framework (SSDF) SP 800-218.

The Contractor shall ensure the application development team members are trained in secure code development/deployment. The Contractor shall provide a Software Bill of Materials (SBOM) for each product provided. SBOM format and content shall comply with the Department of Commerce and National Telecommunications and Infrastructure Administration's (NTIA) The Minimum Elements for a Software Bill of Materials or guidance published by the Cybersecurity and Infrastructure Security Agency (CISA).

PROVENANCE

The Contractor shall maintain accurate and up to date configuration management on data and controls for third-party products and services regarding chronology of the origin, development, ownership, location, and changes to a system or system component and associated data in accordance with NIST SP 800-53, Rev. 5. It may also include the personnel and processes used to interact with or make modifications to the system, component, or associated data.

The Contractor shall document changes to the baselines of components, component processes, information, systems, organizations, and organizational processes, to be reported to third-party products and services.

The Contractor shall notify the IRS within 7 business days whenever there is a change in subcontractors or suppliers at any point during design, development, fabrication, testing or deployment of software or hardware utilized in this procurement.

ADD TO ADDENDUM H OF CLAUSES SECTION

Office of the President Management and Budget (OMB) Policies for Security of Federal Automated Information Resources

The contractor shall implement protections for personally identifiable information being accessed remotely or transported outside of the agency's secured, physical perimeter, and/or stored offsite. In those instances where personally identifiable information is transported to a remote site of the contractor, the contractor shall implement NIST Special Publication 800-53 Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations security controls and IRS specific security procedures to ensure that information is transported in encrypted form. The contractor shall comply with OMB Circular Policy M-17-12: Preparing for and Responding to a Breach of Personally Identifiable Information.

TREASURY/ IRS POLICIES FOR INFORMATION TECHNOLOGY(IT) SECURITY

The contractor shall comply with FedRAMP Framework, Department of Treasury Directive TD P 85-01, Internal Revenue Manual (IRM) 10.8.1, Information Technology (IT) Security Policy and Guidance and Internal Revenue Manual (IRM) 10.8.24, Information Technology (IT) Security, Cloud Computing Security Policy. The contractor shall comply with IRS IRMs when developing or administering IRS information and information systems.

The contractor shall comply with the Taxpayer Browsing Protection Act of 1997 - Unauthorized Access (UNAX), the Act amends the Internal Revenue Code 6103 of 1986 to prevent the unauthorized inspection of taxpayer returns or tax return information.

The contractor/contractor personnel are bound by the Records Management by Federal Agencies(44 U.S.C. Chapter 31) regarding the care and retention of federal records.

FEDERAL INFORMATION PROCESSING STANDARD (FIPS)-201-2

Homeland Security Presidential Directive-12 [HSPD-12], August 27, 2004, established the requirements for a common identification standard for identity credentials issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to federally controlled facilities and logical access to federally controlled information systems. HSPD-12 directs the Department of Commerce to develop a FIPS publication to define such a common identity credential. In accordance with HSPD-12, this Standard defines the technical requirements for the identity credential that:

(a) is issued based on sound criteria for verifying an individual employee's identity;
(b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
(c) can be rapidly authenticated electronically; and
(d) is issued only by providers whose reliability has been established by an official accreditation process.

The standard for a Personal Identity Verification (PIV) system is based on secure and reliable forms of identity credentials issued by the Federal government to its contractors. These credentials are intended to authenticate individuals who require access to federally controlled facilities, information systems, and applications. A PIV Card must be personalized with identity information for the individual to whom the card is issued, to perform identity verification both by humans and automated systems. Humans can use the physical card for visual comparisons, whereas automated systems can use the electronically stored data on the card to conduct automated identity verification.

IRS will determine the level of security and authentication mechanisms appropriate for their applications and will employ only information technology products on the FIPS 201-approvedproducts list for PIV capability implementation within organization information systems.

CSPs must review SP 800-63-3, use its decision trees to obtain an overview of all digital identity requirements, and read the applicable 800-63 volumes to determine specific requirements that apply to their cloud offerings.

SECURITY AUTHORIZATION / CERTIFICATION AND ACCREDITATION PROCESS

CSP/Contractor systems that collect, maintain, contain or use agency information or an information system on behalf of the agency (a General Support System (GSS), with a FIPS 199 security categorization) must ensure annual reviews and continued security certification and accreditation. Some of the key elements of this IT risk and impact assessment process are project security deliverables such as the System Security Plan (SSP), Information System Contingency Plan (ISCP),Interconnection Security Agreement (ISA), Security Risk Assessment (SRAs), Data Impact Assessments (DIAs), Risk Analyses, Security Threat Analyses, Audit Plan, Source Code Review, Security Control Assessment (SCA), and/or Event-Driven Security Control Assessment (ED-SCA).All systems that complete this process will, at a minimum, meet FedRAMP, Treasury and IRS requirements.

CLOUD SERVICE PROVIDER (CSP) ROLES AND RESPONSIBIILITES - INTERNAL REVENUE MANUAL (IRM) 10.8.24, INFORMATION TECHNOLOGY (IT) SECURITY,

CLOUD COMPUTING SECURITY POLICY

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 shall 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 shall 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 shall also be depicted either in the CSP system authorization boundary diagrams or in separate diagrams.

d. The CSP system data flow diagram(s) shall:

    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 shall be accompanied by a written description of the data flows.

f. If the CSP boundary is not adequately/accurately represented, the 3PAO shall identify boundary deficiencies that could lead to substantial delays in the CSP Readiness Assessment process.

g. If the CSP leverages another CSP that does not have a current FedRAMP JAB or Agency ATO, the CSP shall be fully responsible for the authorization of the entire Cloud Service model stack.

INFORMATION SYSTEMS AND INFORMATION SECURITY CONTROLS FOR CONTRACTING ACTIONS SUBJECT TO IRS PUBLICATION 4812 REVISION 10-201

Note: Publication 4812 is a layperson's guide to NIST SP 800-53, Rev. 5 when access to IRS information or information systems under contracts for services on behalf of the IRS is outside of IRS controlled facilities or the direct control of the Service as opposed to Internal Revenue Manual 10.8.1 - Information Technology (IT) Security, Policy and Guidance, which applies when contractors are accessing IRS information and information systems at Government controlled facilities.

In performance of this contract, the contractor agrees to comply with the following requirements and assumes responsibility for compliance by its employees and subcontractors (and their employees):

(a) *General.* The contractor shall ensure IRS information and information systems (those of the IRS and/or the contractor, as appropriate) are always protected. In order to do so, the contractor shall develop, implement, and maintain effective controls and methodologies in its business processes, physical environments, and human capital or personnel practices that meet or otherwise adhere to the security controls, requirements, and objectives described in applicable security control guidelines, and their respective contracts.

(b) The contractor will be required to input data into a system, to be defined by the IRS, to describe the security controls being used to protect information.

(c) *Publication (PUB) 4812 Applicability.* This contracting action is subject to Publication 4812 – Contractor Security & Privacy Controls. PUB 4812 is available at: https://www.irs.gov/pub/irs-pdf/p4812.pdf

IT SECURITY CONTROLS - (IRM) 10.8.24, INFORMATION TECHNOLOGY (IT) SECURITY, CLOUD COMPUTING SECURITY POLICY

IT Security Controls

(1) The security requirements within this IRM and IRM 10.8.1 must be met to satisfy FISMA compliance. The following FedRAMP security requirements apply to all IRS cloud computing resources, as well as cloud computing resources used or operated by a contractor of the agency or other organization on behalf of the agency; and shall be implemented and complied with as part of FedRAMP.

a. See the Minimum FedRAMP Security Control Baseline Exhibit 10.8.24-5within this IRM for a list of security controls that are to be implemented as part of the minimum FedRAMP security control baseline.

b. For security controls that are a part of the FedRAMP baseline but not explicitly defined within this IRM, IRM 10.8.1 requirements shall be implemented.

(2) Business Units shall use an existing FedRAMP authorized CSO unless there is a compelling justification to use a non-FedRAMP authorized alternative CSO. (IRS-defined)

a. The justification must demonstrate there is no FedRAMP authorized CSO available that provides the same or similar capabilities as the non-FedRAMP authorized CSO being considered.

b. The justification to use a non-FedRAMP solution must be approved by the IRS Senior Agency Information Security Officer (SAISO)/Chief Information Security Officer (CISO) in writing.

(3) If a non-FedRAMP solution is approved, the provisions within this IRM still apply.

Note: This control does not nullify the need for an Analysis of Alternatives (AoA)and market research.

Note: If a CSP has been granted a FedRAMP P-ATO for one or more implementation of a CSO, it does not mean all the CSPs CSO offerings are covered under the FedRAMP P-ATO. P-ATOs on the FedRAMP Marketplace are granted to CSOs, not to the CSPs.

(4) The enforcement of FedRAMP requirements shall be done through Service Level Agreements (SLA)/Contracts. (FedRAMP)

Note: Special contract language to properly address all potential CSP risk includes but it is not limited to security monitoring, auditing, data governance, data protection, data location, data and system availability, data and system confidentiality, data and system integrity, data and system access, data portability, data backup, data encryption, data breach notification, data restoration, contract exit conditions, contract termination conditions, data disposal, data retention, user/device/service authentication, authorization, audit logging and remediation of security concerns.

(5) Business Units shall use the Table in Exhibit 10.8.24-2 within this IRM for the recommended Cloud deployment requirements. (IRS-defined)

a. All CSO with sensitive but unclassified (SBU) data (including Personal Identifiable Information (PII) and Federal Tax Information (FTI)) shall comply with the Privacy requirements codified in PGLD Privacy IRMs 10.5.xand 11.3.x series.

Note: Per NIST SP 800-60 v1r1, the Chief Information Officer (CIO), Senior Agency Information Security Officer (SAISO), Authorizing Officials may adjust the security impact level for each system deploying into Cloud Service Models.

(6) IRS shall utilize aggregated and individual security categorization information when assessing interagency and CSPs connections with different FIPS 199 Category Impact levels. (e.g., High Impact system connecting to Moderate Impact system etc.,)(NIST SP 800-60 v1r1).

Note: For example, if information processed on a high impact information system is flowing to another agency's or CSP moderate impact information system should cause both agencies (US local, state, tribal, or territorial government) or CSPs to evaluate the security categorization information, the implemented or resulting security controls, and the risk associated with interconnecting systems. The results of this evaluation may substantiate the need for additional security controls in the form of an SLA, information systems upgrades, additional mitigating security controls, or alternative means of sharing the required information.

Note: Each use case shall be assessed based on mission, business need and the datatype being exchanged.

CONTRACTOR (AND SUBCONTRACTOR) SITE AND INFORMATION TECHNOLOGY (SOFTWARE, HARDWARE AND DATA) LOCATION

The CSP/Contractor headquarters, infrastructure, servers (including back-up servers) and data must be physically located in the United States (or U.S. territories).

The infrastructure associated with services outsourced by the CSP/Contractor must located in the United States (or U.S. territories).

The current version and all subsequent versions of the software implemented by the CSP/Contractor must be escrowed in the United States (or U.S. territories) at the CSP's expense to protect the code in the event the CSP declares bankruptcy.

Data stored outside the United States cannot be protected under the Privacy Act of 1974 or safe harbor framework and may allow for certain local or foreign law enforcement authorities to search IRS data pursuant to a court order, subpoena, or informal request outside the control of the IRS.

The Clarifying Lawful Overseas Use of Data ("CLOUD") Act enacted into law on March 23, 2018, provides that U.S. law-enforcement orders issued under the Stored Communications Act (SCA) may reach certain data located in other countries.

Recognizing the limits of existing law enforcement tools and privacy laws to govern requests for electronic evidence in the age of cloud computing, the CLOUD Act establishes processes and procedures for law enforcement requests for data in other countries.

Although the Act expands the geographic scope of the SCA, it does not change who is subject to SCA orders or what type of data is subject to U.S. law-enforcement requests under the SCA.

The CLOUD Act lays out the circumstances under which a "provider of electronic communication service or remote computing service" must comply with a U.S. law-enforcement order to disclose data within its "possession, custody, or control," even when that data is "located … outside the United States."

ALTERNATE STORAGE

The CSP/Contractor shall establish an alternate storage site including necessary agreements to permit the storage and retrieval of information system backup information. The alternate storage site shall be geographically separated within the United States (or U.S. territories) from the contractor site to enable recovery of operations. The alternate storage site is separated from the primary storage site so as not to be susceptible to the same hazards and identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. All backup data that contains SBU information shall be encrypted.

The alternate storage site shall provide information security safeguards equivalent to that of the primary site.

BACKUPS

Backups must be provided as part of the CSP service offering.

All backup data that contains SBU information shall be encrypted.

(1) The IRS or CSP/Contractor shall conduct backups for information contained in the information system at the following frequency:

- User-level: daily incremental; weekly full
- System-level: daily incremental; weekly full
- Information system configuration; daily incremental; weekly full

Note: The defined backup frequencies are above IRM 10.8.1 baseline and assigned by FedRAMP.

(2) The CSP/Contractor shall maintain:

- At least three backup copies of user-level information (at least one of which is available online) or provides an equivalent alternative.
- At least three backup copies of system-level information (at least one of which is available online) or provides an equivalent alternative.
- At least three backup copies of information system documentation including security information (at least one of which is available online) or provides an equivalent alternative.

Note: This requirement is defined by FedRAMP.

(3) The IRS or CSP/Contractor shall determine what elements of the cloud environment require the Information

System Backup control.

Note: This requirement is defined by FedRAMP.

1. The CSP/Contractor shall determine how Information System Backup is going to be verified and the appropriate periodicity of the check.

Note: This requirement is defined by FedRAMP.

(4) Backup copies of the operating system (i.e., deployed operating system with agency defined configurations and controls) and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) shall be stored in a separate facility or in a fire-rated container that is not collocated with the operational system.

Note: This requirement is assigned to Moderate and High impact systems by FedRAMP.

DATA LOSS PREVENTION (DLP) SOFTWARE

The CSP/Contractor shall implement data loss prevention (DLP) software to assure existing software will operate effectively in the cloud.

The CSP/Contractor shall be responsible for all patching and vulnerability management (PVM) of software and other systems' components supporting services provided under this agreement so as to prevent proactively the exploitation of IT vulnerabilities that may exist within the CSP/Contractor operating environment. Such patching and vulnerability management shall meet the requirements and recommendations of NIST SP 800-40, as amended, with special emphasis on assuring that the vendor's PVM systems and programs apply standardized configurations with automated continuous monitoring of the same to assess and mitigate risks associated with known and unknown IT vulnerabilities in the CSP/Contractor operating environment.

Furthermore, the CSP/Contractor shall apply standardized and automated acceptable versioning control systems that use a centralized model to capture, store, and authorize all software development control functions on a shared device that is accessible to all developers authorized to revise software supporting the services provided under this agreement. Such versioning control systems shall be configured and maintained to make sure all software products deployed in the CSP/Contractor operating environment and serving the IRS are compatible with existing systems and architecture of the IRS.

CONTINUOUS MONITORING BASELINE CONTRACT DELIVERABLES

Cloud Continuous Monitoring baseline contract deliverables are needed as applicable, such as, but not limited to:

- Weekly Security Status Report
- Monthly Security Status Report
- Continuous Monitoring Plan
- Security Configuration and Change Management Plan
- Security Patch Management Plan
- Security Incident Handling, Monitoring and Response Plan
- Information System Contingency Plan (ISCP)
- Security Concept of Operations (Security CONOPS)
- Access Management Plan (AMP)
- System Security Plan (SSP)
- Authorization Boundary Memorandum
- Interconnection Security Agreements (ISA)
- Security Control Assessment (SCA) Test Plan
- Security Assessment Report (SAR) Mitigation Plan
- Privacy/Civil Liberties Impact Assessment (PCLIA)

- State of Security (SoS) Package
- FISMA Compliance Reports including, but not limited to, inventory, inventory change log, security configuration compliance reports, personal security, and POA&Ms.
- Information Security Status Package
- Alternate Site Processing Environment (ASPE) Plan
- Executive Summary of Analytical Results and Recommendations
- Key Management Practices Statement
- Contractor Security Assessments (CSA) Test Plan
- Configuration Compliance Summary Report
- Security Incident Report
- Mitigation Report
- FSTAR Mitigation Plan
- Incident Response Test Report

USE OF OUTSOURCED / CONTRACTOR FACILITIES TO PROCESS IRS SBU DATA

The infrastructure associated with services outsourced by the CSP/contractor must located in the United States (or U.S. territories).

If IRS products/applications/data/services/solutions are hosted and/or managed by a CSP (outside the IRS network boundaries/facilities (e.g., outsourced)) then all such products/applications/data/services/solutions shall go through (and maintain) the Federal Risk and Authorization Management Program (FedRAMP) certification, and meet all of the IRS unique business/legal requirements (including applicable PUB 4812 requirements, etc.).

Note: FedRAMP is mandatory for all IRS cloud deployments and cloud service models at the Federal Information Processing Standards (FIPS) 199 Low, Moderate and High impact levels. FedRAMP does not apply for internal housed IRS systems that are operated for IRS use only. This service model would be considered an On-Site-Private Cloud.

Special contract language shall be included in all types of Cloud Service Provider (CSP) contracts/non-disclosure agreements/Service Level agreements to address all potential CSP risks(e.g., Data Governance, Data Protection, Data Location, Data Availability, Data Confidentiality, Data Integrity, Data Access, Data Backup, Data Encryption, Data Breach Notification, Contract

Exit Conditions, Contract Termination Conditions, Data Disposal, Data Retention, User/Device/Service AAA services (e.g., Authentication, Authorization, Audit Logging, Background Checks etc.). The Vendor shall pay special attention to the logical and physical separation of IRS data, applications, and communications to maintain security. Vendors are encouraged to manage any cloud environments containing IRS data with only other Federal or State and local Government customers operating at the same security level. The IRS shall control and maintain the centralized/authoritative control (in-house) of ALL the IRS authorized Users/Devices/Services Authentication, Authorization, and Auditing (AAA) functions, even if a particular IRS application/data/service/solution is hosted in a third-party cloud environment.

Outsourced operations shall report monthly for FISMA and Treasury submission. This includes all systems in the following environments: production, disaster recovery, training, development, and testing.

ENCRYPTION

The IRS or CSP shall ensure that the information system implements FIPS-validated or National Security Agency (NSA)-approved cryptography in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Note: This requirement is defined by FedRAMP.

IRS sensitive data (e.g., Sensitive But Unclassified (SBU), Personally Identifiable Information

(PII) that is processed, stored, or transmitted by an information system outside of IRS facilities or IRS IT information system shall be protected with FIPS 140-2 or later validated cryptographic modules with approved modes of operation. The vendor shall provide a system that implements (encryption standard) that provides for origin authentication, data integrity, and signer non- repudiation. Consider AU-11 audit Records retention.

A list of NIST validated modules is available at the following link:
http://csrc.nist.gov/groups/STM/cmvp/validation.html.

The CSP/Contractor shall ensure all SBU information is protected at rest, in transit, and in exchanges(i.e., internal and external communications). Limit access to SBU information to authorized personnel (those favorably adjudicated and trained) with a need to know and ensure internal and external exchanges are conducted only through secure or encrypted channels. The CSP/Contractor shall employ encryption concepts and approved standards to ensure the confidentiality, integrity, and availability of the SBU information, consistent with the security controls under Publication 4812 and any security requirements specified elsewhere in the contract.

Contractual liability to the government only exists with the prime contractor.

The CSP/contractor shall retain operational configuration and control of data repository systems used to process and store government data to include any or remote work. The CSP/contractor shall not subcontract the operational configuration and control of any government data.

IRS retains exclusive ownership over all its data; the CSP/Contractor acquires no rights or licenses through the agreement, including intellectual property rights or licenses, to use the IRS data for its own purposes; and that the CSP/Contractor does not acquire and may not claim any interest in the data due to security. If CSP/Contractor moves data, the IRS will not lose rights and access to conduct audits.

Intellectual property, including original works created using the cloud infrastructure, may be stored. IRS must ensure that the cloud provider contract respects the IRS' right to any intellectual property or original works as far as possible without compromising the quality of service offered (e.g., backups may be a necessary part of offering a good service level).

CONTRACTOR SYSTEM REVIEW / SITE VISIT

In conjunction with the use of outsourced / Contractor facilities, the contractor shall be subject to at the option / discretion of the IRS, to periodically test and inspection (annually) and evaluate the effectiveness of information security controls and techniques. The assessment of information security controls may be performed by an agency independent auditor, security team or Inspector General, and shall include testing of management, operational, and technical controls, as indicated by the security plan, of every information system that maintain, collect, operate or use federal information on behalf of the agency. The agency and contractor shall document and maintain a remedial action plan, also known as a Plan of Action and Milestones (POA&M) to address any deficiencies identified during the test and evaluation. The contractor must cost-effectively reduce information security risks to an acceptable level within the scope, terms and conditions of the contract.

CONTRACTOR SYSTEM OVERSIGHT/COMPLIANCE

(a) The Contractor, service providers, and third-party vendors must complete the IRS Security – Assessments (IT Security Product Questionnaire) and submit the assessments to the Contracting Officer and Cybersecurity for review and evaluation. This is a supplemental requirement and does not replace contract requirements under FISMA. The federal government has the authority to conduct site reviews for compliance validation. Full cooperation by Contractor and third-party providers is required for audits and forensics.

(b) The Contractor must support IRS in its efforts to assess and monitor the Contractor systems and infrastructure. The Contractor must provide logical and physical access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases upon request. The Contractor will be expected to perform automated scans and continuous monitoring activities which may include, but will not be limited to, authenticated and unauthenticated scans of networks, operating systems, applications, and databases and provide the results of the scans to the IRS Cybersecurity, or designate, or allow IRS (or its designate) to run the scans directly.

(c) All Contractor systems must participate in Information Security Continuous Monitoring (ISCM) and

Reporting as defined in the IRS IT Policy.

(d) All Contractor systems must perform vulnerability scanning as defined by IRS IT Security Policy and provide scanning reports to the IRS Cybersecurity, or designate, on a monthly basis.

(e) All Contractor systems must participate in the implementation of automated security controls testing mechanisms and provide automated test results in Security Compliant Automation Protocol

(SCAP) compliant data to the IRS Cybersecurity, or designate, on a monthly basis.

CONTRACTOR SECURITY TRAINING

IR1052.224-9001 Mandatory IRS Security Training for Information Systems, Information Protection and Facilities Physical Access (NOV 2022)

The Federal Information Security Modernization Act of 2014 (FISMA) requires each federal agency to provide periodic information security and privacy awareness training to all contractors/subcontractors involved in the management, use, or operation of Federal information and information systems. In addition, contractor/subcontractor personnel are subject to the Taxpayer Browsing Protection Act of 1997, which prohibits willful unauthorized inspection of returns and return information as defined in IRC 6103(b)(2) and details that any violation of the Act could result in civil and criminal penalties under IRC sections 7213, 7213A and 7431. Contractor/subcontractor personnel are subject to the Privacy Act of 1974 (5 U.S.C. 552a; Pub. L. No. 93-579), December 1974.

Contractor/subcontractor personnel are bound by the Records Management by Federal Agencies (44 U.S.C. Chapter 31) regarding the care and retention of federal records.

1. The contractor must ensure all new contractor/subcontractor personnel complete all assigned briefings which are based on the responses provided on the Risk Assessment Checklist Form 14606. These responses pertaining to access to any IRS system, including basic LAN, email and internet; access to any Sensitive but Unclassified (SBU) data; and access to any IRS facility. Since new contractor/subcontractor personnel will not have access to the IRS training system, the COR shall provide softcopy versions of each briefing.

   i. Exception: Contractor personnel (including subcontractors) performing under IRS contracts with Nonprofit Agencies Employing People Who Are Blind or Severely Disabled (as described in FAR Subpart 8.7) are exempted from the aforementioned briefing requirements, unless the contractor requests access to the training, or there is a compelling justification for requiring the training that is approved by the Contracting Officer (CO). An example of this would be in an instance where visually impaired personnel is assigned to perform systems development and has potential staff-like access to IRS information.

   ii. Contractor/subcontractor personnel working with IRS information at contractor-controlled facilities with no access to the IRS network will be subject to all mandatory briefing excepting the Facilities Management Physical Security briefing as outlined in Publication 4812.

   iii. Service Personnel: Inadvertent Sensitive Information Access Training

   Contractor personnel performing: (i) janitorial and cleaning services (daylight operations), (ii)building maintenance, or (iii) other maintenance and repair and need staff-like access to IRS facilities are required to complete Inadvertent Access to Sensitive Information (SBU) Access training.

   iv. Service Personnel Security Awareness Training: Contractor personnel providing services in the following categories are required to complete FMSS Physical Security Training:

   - Medical;
   - Cafeteria;
   - Landscaping;
   - Janitorial and cleaning (daylight operations);
   - Building maintenance; or

- o Other maintenance and repair

2. In combination these mandatory briefings are known as IRS Security Awareness Training (SAT). The topics covered are Cybersecurity Awareness, Privacy Information Protection and Disclosure, Unauthorized Access to Taxpayer Data, Records Management, Inadvertent Sensitive Information Access, Insider Threat and/or Facilities Physical Security. The completion of the assigned mandatory briefings constitutes the completion of the Security Orientation.

3. The SAT must be completed by contractor/subcontractor personnel within 5 business days of successful resolution of the suitability and eligibility for staff-like access as outlined in IR1052.204-9000 Submission of Security Forms and Related Materials and before being granted access to SBU data. The date listed on the memo provided by IRS Personnel Security shall be used as the commencement date.

i. Note: To be authorized, all personnel must complete required training (IRS annual and role-based privacy, information protection, and disclosure training requirements, Unauthorized Access [UNAX] awareness briefings, records management briefings, and all other specialized privacy training) and background investigations before given access to SBU data (including PII and tax information). [OMB A-130]

4. Training completion process:

The contractor must submit confirmation of completed SAT mandatory briefings for each contractor/subcontractor personnel by either:

i. Using Form 14616 signed and dated by the individual and authorized contractor management entity and returned to the COR. This option is used for new contractor/subcontractor personnel and any that do not have an IRS network account.

ii. Using the IRS training system which is available to all contractors with IRS network accounts.

5. Annual Training. For contracts/orders/agreement exceeding one year in length, either on a multiyear or multiple year basis, the contractor must ensure that personnel complete assigned SAT mandatory briefings annually no later than October 31st of the current calendar year. The contractor must submit confirmation of completed annual SAT on all personnel unable to complete the briefings in the IRS training systems by submitting completed Form 14616 assigned to this contract/order/agreement, via email, to the COR, upon completion.

6. Contractor's failure to comply with IRS privacy and security policy (to include completion and certification of SAT requirements within the timeframe specified) may be subject to suspension, revocation or termination (temporarily or permanently) of staff-like access to IRS IT systems and facilities.

7. Flow down of clauses. The contractor shall include and flow down, in its subcontracts (or arrangements or outsourced service agreements) that entails staff-like access to SBU information by a subcontractor, at any tier, the same Federal Acquisition Regulation (FAR) and local privacy and security or safeguard clauses or provisions for protecting SBU information or information systems that apply to and are incorporated in its prime contract with IRS.

SPECIALIZED IT SECURITY (SITS) TRAINING

This training is also referred to as role-based security training. If a Contractor performs tasks/services such as system administration, network administration, database administration, programmer developer or one of the other specialized IT security roles as defined in IRM 10.8.2.

IR1052.204-9002 IRS Specialized Information Technology (IT) Security Training (Role-Based)Requirements (JUN 2022)

(a) Consistent with the Federal Information Security Modernization Act of 2014 (FISMA), specialized information technology (IT) security training (role-based) shall be completed prior to access to Information Systems and annually thereafter by contractor and subcontractor personnel who have an IT security role or responsibility.

(b) Identifying contractor/subcontractor with a role or responsibility for IT security is completed by the Contractor, and verified by the COR, by completing the Risk Assessment Checklist (RAC). The roles listed in the RAC conform to those roles listed in the Internal Revenue Manual 10.8.1.2 that apply to contractor personnel. This process applies to new contractors/subcontractors, replacement personnel and for existing contractors/subcontractors whose roles change during their work on a contract. This includes, but is not limited to, having an approved elevated privilege to one or more IRS systems through the OL5081 process or Business Entitlement Access Request System (BEARS).

(c) Prior to accessing any IT system, all contractor/subcontractor personnel must be successfully complete all provisions of IR1052.204-9000 Submission of Security Forms and Related Materials.

(d) In keeping with the Security Orientation outlined in IR1052.224-9001, contractors/subcontractors designated on the Risk Assessment Checklist as performing a role shall complete approved training equal to the assigned hours within 5 business days of receiving the Personnel Security's memo approving staff-like access.

(e) Annual Requirements: Thereafter, on an annual basis within a FISMA year cycle beginning July1st of each year, contractor/subcontractor personnel performing under this contract in the role identified herein is required to complete specialized IT security, role-based training by June 1stof the following year.

(f) Training Certificate/Notice: The contractor shall use the Government system identified by Cybersecurity to annually complete specialized IT security training (role-based). The COR will track the courses, hours completed and the adhere to the established due dates for each contractor/subcontractor personnel. Alternatively, courses may be completed outside of the Government system. Any courses taken outside of the Government system must be pre- approved by IRS Cybersecurity's Security System Management team via the COR. Adequate information such as course outline/syllabus must be provided for evaluation. Once a course is approved, certificates of completion provided for each contractor/subcontractor shall be provided to COR in order to receive credit toward the required hours for the contractor/subcontractor personnel. Copies of completion certificates for externally completed course must be shared with the Contracting Officer upon request.

(g) Administrative Remedies: A contractor/subcontractor who fails to complete the specialized IT security training (role-based) requirements, within the timeframe specified, may be subject to suspension, revocation or termination (temporarily or permanently) of staff-like access to IRS IT systems.

(h) Flow down of clauses. The contractor shall include and flow down, in its subcontracts (or arrangements or outsourced service agreements) that entails staff-like access to SBU information by a subcontractor, at any tier, the same Federal Acquisition Regulation (FAR) and local security or safeguard clauses or provisions for protecting SBU information or information systems that apply to and are incorporated in its prime contract with IRS.

SAFEGUARDING / PROTECTING SENSITIVE PERSONALLY IDENTIFIABLE INFORMATION (PII)

Sensitive PII is defined as any information that permits the identity of an individual to be directly or indirectly inferred, including any information that is linked or linkable to that individual, regardless of whether the individual is a U.S. citizen, legal permanent resident, or employee or contractor to the Department. Sensitive PII is Personally Identifiable Information, which if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

Information Systems can be either electronic or manual. IRM 10.8.1 requires IRS sensitive information is to be handled and protected at the contractor's site, including any information stored, processed, or transmitted using the contractor's computer systems. Contractor personnel shall perform a background investigation and/or clearance required; receive security awareness and specialized IT security training required for contractor activities or facilities; and any facility physical security requirements.

IRS sensitive data (e.g., Sensitive But Unclassified (SBU), Personally Identifiable Information (PII)that is processed, stored, or transmitted by an information system outside of IRS facilities or IRS IT information system shall be protected with FIPS 140-2 or later validated cryptographic modules with approved modes of operation.

A list of NIST validated modules is available at the following link: http://csrc.nist.gov/groups/STM/cmvp/validation.html.

(1) The CSP/Contractor shall ensure that individuals accessing an information system processing, storing or transmitting information requiring special protection satisfy the personnel screening criteria.

Note: This requirement is defined by FedRAMP.

(2) The organization shall:

Screen individuals prior to authorizing access to the information system; and

Rescreen individuals according to FedRAMP Assignments: for national security clearances; a reinvestigation is required during the 5th year for top secret security clearance, the 10th year for secret security clearance, and 15th year for confidential security clearance. For moderate risk law enforcement and high impact public trust level, a reinvestigation is required during the 5th year. There is no reinvestigation for other moderate risk positions or any low-risk positions.

The CSP/Contractor shall ensure that data is used, only as identified, in the IRS contract and that the data will be used for nothing else to ensure the privacy of the individual.

The CSP/Contractor is responsible for maintaining an inventory of all PII provided to the contractor, generated by the contractor, or used by the contractor sufficient to enable notification to taxpayers, if disclosed. The inventory of PII must be updated semi-annually with a final inventory notification provided to the COR.

Most IRS information is categorized as Sensitive But Unclassified (SBU). This includes:

(a) Federal Tax Information (FTI)
(b) Personally Identifiable Information(PII)
(c) Protected Health Information(PHI)
(d) Certain procurement information
(e) System vulnerabilities
(f) Case selection methodologies
(g) Systems information
(h) Enforcement procedures
(i) Investigation information
(j) Proprietary processes or algorithms used in investigative work or tax processing

Note: Live data, which is defined as production data in use (production, testing, development),often contains SBU.

IRM 10.8.2, Information Technology (IT) Security, Security Roles and Responsibilities, defines IRS-wide roles and responsibilities related to IRS information and computer security.

a. The IRS shall designate an Authorizing Official for the Cloud Computing Service per IRM10.8.2.
b. Each Business Unit shall assign at least one (1) Information System Security Officer (ISSO)or Security Program Management Officer (SPMO) to the Cloud authorization process.

Various laws and regulations have addressed the need to protect sensitive information held by government agencies including the Federal Information Security Modernization Act (FISMA),the Government Act of 2014, the Privacy Act of 1974, and OMB Circular A-130, Management of Federal Information Resources. FISMA requires agencies to have a security program and controls for systems to protect their sensitive information. Therefore, the contractor shall comply with OMB policies and Treasury / IRS specific policies, procedures or guidance to protect sensitive information.

IRM 10.8.24.2, Internal Revenue Manual (IRM) 10.8.24, Information Technology (IT) Security, Cloud Computing Security Policy, CSP roles and responsibilities related to IRS information and computer security.

Unless specifically identified, the scope of the CSP’s responsibility for the protection of IRS assets depends on the service delivery model being used (SaaS, PaaS, IaaS) and their contractual agreement. The IRS personnel with technical responsibilities for the use, implementation, and acquisition of cloud service shall ensure the CSP is made aware of and adheres to, as part of their contract, all applicable CSP responsibilities according to their Cloud Service Offering (CSO).

CONTRACTOR RIGHTS TO ACCESS DATA

Access Control requirements shall be implemented as defined within Internal Revenue Manual (IRM) 10.8.1, Information Technology (IT) Security, Policy and Guidance and Publication 4812.

1) The CSP/Contractor shall not access, use, or disclose Government data unless specifically authorized by the terms of this contract or a task order issued hereunder. If authorized by the terms of this contract or a task order issued hereunder, any access to, or use or disclosure of, Government data shall only be for purposes specified in this contract or task order. CSP/Contractor shall ensure that each of its employees and representatives, and any others (e.g., subcontractor employees) performing duties hereunder, shall, prior to obtaining access to any Government data, sign a contract or task order specific nondisclosure agreement.

2) The CSP/Contractor shall use Government-related data only to manage the operational environment that supports the government data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer.

CSP/Contractor shall:

a. Be subject to background investigations at the risk level appropriate to the sensitivity of the position and sensitivity/classification of the data.

b. Not access sensitive IT systems until they have at least a favorably adjudicated National Agency Check (a component of the full background investigation).

c. Be responsible for protecting any Personally Identifiable Information (PII) that they have in their possession, whether it is paper-based or in electronic form.

d. Understand the provisions and applicable criminal penalties under Public Law 105-35,Taxpayer Browsing Protection Act, shall also apply to all contractors and contractor employees.

e. Comply with all executives, legislative and Department of Treasury and IRS security policies.

f. Minimize the threat of viruses by write-protecting removable media, routinely scanning files, systems, and media for viruses and never circumventing anti-virus safeguards.

A breach of the obligations or restrictions may subject the CSP/Contractor to criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and any other appropriate remedies by any party adversely affected by the breach.

HANDLING INFORMATION SECURITY INCIDENTS

The IRS Computer Security Incident Response Capability (CSIRC) defines a security incident as: “any adverse event whereby some aspect of computer security could be threatened. Adverse events may include the loss of data confidentiality, disruption of data or system integrity, disruption or denial of availability, loss of accountability, or damage to any part of the system.” User Compromise, Disclosure of Taxpayer/Sensitive Data, Malicious Code (successful or unsuccessful), Denial of Service (DoS) (successful or unsuccessful), Website Defacement, Identity Theft, Misuse of Resources or Policy Violation, Loss or Theft of IT Equipment, IRM/LEM Non- Compliance, Unauthorized Access Attempt, Probe/Scan, and any other security incident that may threaten or damage any IRS or federal agency information or information system(s).

Contractors and their employees must be aware of their responsibilities under the law to safeguard PII and sensitive information, the procedures to follow when data is lost or compromised and the penalties for unauthorized disclosure of PII and sensitive information. Contractors should refer to Data Breach Information for IRS Contractors on irs.gov https://portal.ds.irsnet.gov/sites/vl003/RelatedResources/Doc13347-2020-01-Data%20Breach%20Response%20Playbook.pdf#search=contractors%20data%20breach , Pub 4465-A, Protecting Federal Tax Information for Contractors, and Pub 4812, Contractor Security Controls, for information about a contractor’s responsibilities to protect Federal Tax Information (FTI) and incident/data breach response and reporting procedures.

It is critical to report an incident/data breach as soon as actionable information is available so a response/reaction can be initiated. Incident/data breach updates and any additional notifications to Treasury Inspector General for Tax

Administration (TIGTA) and/or Local Law Enforcement can be completed after the initial report to the Office of Taxpayer Correspondence (OTC), Privacy Governmental Liaison and Disclosure/Incident Management Office (PGLD/IM), or the Computer Security Incident Response Center (CSIRC) is submitted.

All physical security incidents and/or threats should be reported to the SAMC within 30 minutes of incident discovery. SAMC operates 365 days a year, 24 hours a day, seven days a week. Incidents may be reported to the SAMC through any of the following methods:

Primary Method of Reporting: Website incident reporting link, https://tscc.enterprise.irs.gov/irc/

Alternate Reporting Methods:
Telephone: 202-317- 6124 or 1-866-216-4809 (toll free hotline)
Fax: 202-317-6129
Email: samc@irs.gov

The CSP/Contractor shall report security incident information according to U.S. Computer Emergency Response, Department of Treasury, IRS, and the FedRAMP Incident Communications procedures.

All incidents related to IRS processing, information or information systems shall be reported within one (1) hour to the CO, COR, and CSIRC. Contact the CSIRC through any of the following methods:

CSIRC Contacts: Telephone: 240.613.3606E-mail
to csirc@irs.gov

The CSP/Contractor shall be accountable for incident responsiveness, including providing specific time frames for restoration of secure services in the event of an incident.

The CSP/Contractor shall provide and maintain insurance, to include cybersecurity insurance, throughout the performance of this contract, as specified in the Schedule or elsewhere in the contract.

Before commencing performance under this contract, the CSP/Contractor shall provide proof of insurance to the Agency. The CSP/Contractor shall resubmit the proof of insurance within 30 days of notification of any material change that occurs during the performance of the contract.

The CSP/Contractor shall insert the substance of this clause, including this paragraph (c), in subcontracts under this contract that require work with or in support of storage and retrieval of electronic/digital government data and shall require subcontractors to provide and maintain the insurance required in the Schedule or elsewhere in the contract. The CSP shall maintain a copy of all subcontractors' proofs of required insurance and shall make copies available to the Contracting Officer upon request.

CONTRACTOR BOUNDARY PROTECTION

The CSP/Contractor shall ensure IRS data is not comingled with the data from other organizations.

The CSP/Contractor shall implement boundary protection mechanisms at servers, workstations, and mobile devices.

The CSP/Contractor shall isolate the information system from other internal information system components by implementing physically separate subnetworks with managed interfaces to other components of the system.

The CSP/Contractor shall define key information security tools, mechanisms, and support components associated with system and security administration and isolate those tools, mechanisms, and support components from other internal information system components via physically or logically separate subnetworks.

Note: These requirements are above the IRM 10.8.1 baseline and are assigned to Moderate-impact systems by FedRAMP

CLOUD SERVICE PROVIDER'S INFORMATION OUTPUT HANDLING AND RETENTION

The CSP/Contractor shall handle and retain data within the information system, according to record retention standards.

The IRS shall identify the record retention standards to the contractor. In addition, once the contract expires, all data shall be returned to the IRS, unless specifically identified otherwise in the contract. No records shall be maintained, in paper or electronically, unless approved by the IRS COR. Once disposal is complete, a copy of the disposal record and notification must be provided to the IRS CO/COR.

JURISDICTION OVER IRS DATA AND CONTRACT TERMS DATA

The CSP/Contractor shall maintain all data within the United States (or U.S. territories). Jurisdiction over IRS data and contract terms must not be divided. The CSP/Contractor shall provide the IRS with a list of the physical locations which may contain government data. The CSP/Contractor shall provide information about the jurisdictions in which data may be stored and processed and any risks resulting from the location of those jurisdictions must be evaluated. The CSP/Contractor shall identify all data centers that the data at rest or data backup will reside.

The CSP will work with the Information Owner to understand the business rules for information/datastore, collected in the Cloud.

DATA COLLECTED, PROCESSED AND TRANSFERRED

Data provided by the IRS and their customers must be collected, processed, and transferred in accordance with the contract terms established between the IRS and the cloud provider.

Sensitive But Unclassified (SBU) information, data, and/or equipment will only be disclosed to authorized personnel on a Need-To-Know basis. The CSP/Contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to IRS control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST Special Publication 800-88, Guidelines for Media Sanitization.

The disposition of all data will be at the written direction of the COR, this may include documents returned to IRS control; destroyed; or held as specified until otherwise directed. Items returned to the IRS shall be hand carried or sent by certified mail to the COR.

The CSP/Contractor shall have adequate programs in place to protect the information received and information from unauthorized use, access, and disclosure. The CSP/Contractor programs for protecting information received must include documenting notification to employees and subcontractors (at any tier), who will have access to SBU information, the importance of protecting SBU information in general, and returns and return information, and information protected by the Privacy Act; in particular, the disclosure restrictions that apply and the criminal or civil sanctions, penalties, or punishments that may be imposed for unauthorized disclosure or inspection. Disclosure practices and the safeguards used to protect the confidentiality of information entrusted to the Government (and, as provided under the IRC and the Privacy Act) are subject to continual assessment and oversight to ensure their adequacy and efficacy.

DISPOSITION OF DATA

The delivery of data to the CSP/Contractor does not transfer any element of ownership; and as between the customer and data host, the customer retains all right, title and interest in the data.

The CSP/Contractor role with respect to the data is limited to a storage function to fulfill its obligation to provide hosting services, and the CSP/Contractor will not interfere with the customer's access.

The CSP/Contractor is a "bailee for hire" with respect to the data (that is, a person compensated forholding the property as bailee).

The CSP/Contractor will delete or will return the customer's data in an agreed-upon format, at any time at the user's request.

The CSP/Contractor must provide the IRS CO/COR with a copy of the disposal record and notification once disposal is complete.

TERMINATION OF CONTRACT

At the end of the contract period, or if the contract is terminated within the contract period, the CSP/Contractor shall coordinate with the IRS to ensure contractor and contractor employee access privileges to IRS information, IRS systems and facilities are revoked in a timely manner, as necessary.

CSP/Contractor shall confirm to IRS officials that information furnished under the contract has been properly returned, disposed, or destroyed.

Information and IT assets shall be returned to the IRS, destroyed and/or sanitized, as required or

directed by the IRS. This includes assuring the IRS that all IT assets, including laptops, information systems, servers, routers, printers, faxes, switches, voice recordings, and all removable and fixed media have been sanitized of all IRS information prior to returning into production for other use.

CSP/Contractor required to return IRS information and property (as a part of the contract requirements) shall use a process that ensures that the confidentiality of the SBU information is always protected during transport.

A log shall be maintained to ensure that all media destroyed has identified the date of destruction, content of media, serial number, type of media (CD, DVD, Closed Caption Television (CCTV), etc.)destruction performed, personnel performing destruction, and witness.

All VoIP shall be sanitized prior to returning to production, when SBU information is stored on these devices.

All hard drives and removable media shall be inventoried, sanitized, and logged to demonstrate data destruction for all IT assets used to handle SBU data.

All hard copies shall be returned using double-wrapped envelopes and traceable mail.

E-Discovery

In the event of litigation procedures, the CSP shall comply with any and all request to furnish informational data directly to the IRS for electronic discovery (E-discovery) purposes. The IRS shall have the authority to request hardcopy documents or electronically stored information (ESI)from the CSP that is relevant to any legal proceedings.

FOIA Request

The CSP shall not directly disclose any IRS owned data to a third-party requestor who is seeking information through the Freedom of Information Act (FOIA). All FOIA request regarding IRS information and information systems shall be processed directly by the IRS FOIA office. Third- party requestors must contact the respective FOIA public liaison for their state. This information can be found at the following: https://www.irs.gov/privacy-disclosure/freedom-of-information-act-foia- guidelines