52.245.1.

8. Government Furnished Information

GFI *(to include manuals, notes, memos, instruction materials, and other information)* will be provided in the performance of the task orders. The Contractor shall comply with Government- wide and Bureau-specific policies, including but not limited to the following:

	INFORMATION ITEMS
	Information regarding IRS data sources and data sets
	IRS users' business requirements and workflows
	A link to the IRM & Security Standards

Upon request, these documents will be made available. The Contractor shall comply with all new versions, amendments, and modifications made to the above-mentioned documents/standards, if and when they become applicable in the future.

At the end of this task order, disposition of GFI shall be in accordance with FAR 52.245.1.

Section III – Clauses

GSA terms and conditions, as well as BPA terms and clauses, flow down to this Order. In the event of a conflict between the terms and conditions of these documents, the IRS and the contractor will adhere to the following order of precedence, GSA contract, BPA, Task Order.

52.217-8 Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 60 days.

(End of Clause)

1052.201-70 Contracting Officer's Representative (COR) Appointment and Authority (APR 2015)
(a) The COR is (b)(6)

(b) Performance of work under this contract is subject to the technical direction of the COR identified above, or a representative designated in writing. The term “technical direction” includes, without limitation, direction to the contractor that directs or redirects the labor effort, shifts the work between work areas or locations, and/or fills in details and otherwise serves to ensure that tasks outlined in the work statement are accomplished satisfactorily.

(c) Technical direction must be within the scope of the contract specification(s)/work statement. The COR does not have authority to issue technical direction that:

(1) Constitutes a change of assignment or additional work outside the contract specification(s)/work statement;

(2) Constitutes a change as defined in the clause entitled “Changes”;

(3) In any manner causes an increase or decrease in the contract price, or the time required for contract performance;

(4) Changes any of the terms, conditions, or specification(s)/work statement of the contract;

(5) Interferes with the contractor's right to perform under the terms and conditions of the contract; or

(6) Directs, supervises or otherwise controls the actions of the Contractor's employees.

(d) Technical direction may be oral or in writing. The COR must confirm oral direction in writing within five workdays, with a copy to the Contracting Officer.

(e) The Contractor shall proceed promptly with performance resulting from the technical direction issued by the COR. If, in the opinion of the Contractor, any direction of the COR or the designated

representative falls within the limitations of (c) above, the Contractor shall immediately notify the Contracting Officer no later than the beginning of the next Government workday.

(f) Failure of the Contractor and the Contracting Officer to agree that technical direction is within the scope of the contract shall be subject to the terms of the clause entitled ``Disputes."

(End of clause)

1052.204-70 Insider Threat Awareness Training (Jul 2016)

(a) Definition. “Classified information,” as used in this clause, is defined in FAR 2.101(b).

(b) The Government has determined that access to classified information is necessary in performance of this contract.

(c) Contractor personnel, including subcontractor personnel, determined to require access to classified information in performance of this contract shall successfully complete Insider Threat Awareness training initially and annually thereafter.

(1) Failure of a contractor employee to successfully complete the training in paragraph (c) of this clause will result in their access to classified information being revoked until such time the training is successfully completed. The Government reserves the right to take additional action deemed necessary to protect its interests.

(d) The Government may provide Contractor personnel access to a system for purposes of completing this training electronically.

(e) The Contractor shall ensure all Contractor personnel, including subcontractor personnel comply with the requirements of this clause.

(f) The Contractor shall include the substance of this clause in all subcontracts at any tier where subcontractor personnel will have access to classified information.

(End of Clause)

1052.204-71 Cybersecurity and Privacy Awareness Training (March 2024)

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.

(a) The Government has determined that access to Government information technology is necessary in performance of this contract.

(b) Contractor personnel, including subcontractor personnel, determined to require access to Government information technology in performance of this contract shall successfully complete cybersecurity and

privacy awareness training initially and annually thereafter as well as any supplemental awareness training and exercises required.

(1) Failure of a contractor employee to successfully complete the training in paragraph (b) of this clause may result in their access to Government information technology being revoked until such time the training is successfully completed.

(2) The Government reserves the right to take additional action deemed necessary to protect its interests.

(c) The Government may provide Contractor personnel access to a system for purposes of completing this training electronically.

(d) The Contractor shall ensure all Contractor personnel, including subcontractor personnel comply with the requirements of this clause.

(e) The Contractor shall include the substance of this clause in all subcontracts at any tier where subcontractor personnel will have access to Government information technology.

(End of Clause)

Submission of Security Forms and Related Materials (Aug 2025)

The Treasury Security Manual (TD P 15-71) sets forth investigative requirements for contractors and subcontractors who require staff-like access, wherever the location, to (1) IRS-owned or controlled facilities (unescorted); (2) IRS information systems (internal or external systems that store, collect, and/or process IRS information); and/or (3) IRS sensitive but unclassified (SBU) information.

“Staff-Like Access” is defined as authority granted to perform one or more of the following:

- Enter IRS facilities or space (owned or leased) unescorted (when properly badged);
- Possess login credentials to information systems (internal or external systems that store, collect, and/or process IRS information);
- Possess physical and/or logical access to (including the opportunity to see, read, transcribe, and/or interpret) SBU data; (See IRM 10.5.1 for examples of SBU data);
- Possess physical access to (including the opportunity to see, read, transcribe, and/or interpret) security items and products (e.g., items that must be stored in a locked container, security container, or a secure room. These items include, but are not limited to security devices/records, computer equipment, and identification media. For details see IRM 1.4.6.5.1, Minimum Protection Standards); or,
- Enter physical areas storing/processing SBU information (unescorted)

Staff-like access is granted to an individual who is not an IRS employee (and includes, but is not limited to: contractor/subcontractor personnel, whether procured by IRS or another entity, vendors, delivery persons, experts, consultants, paid/unpaid interns, other federal employee/contractor personnel, cleaning/maintenance personnel, etc.), and is approved upon required completion of a favorable suitability/fitness determination conducted by IRS Personnel Security.

For security requirements at contractor facilities using contractor-managed resources, please reference Publication 4812, Contractor Security & Privacy Controls. The contractor shall permit access to IRS SBU

information or information system/assets only to individuals who have received staff-like access approval (interim or final) from IRS Personnel Security.

Contractor/subcontractor personnel requiring staff-like access to IRS equities are subject to (and must receive a favorable adjudication or affirmative results with respect to) the following eligibility/suitability pre-screening criteria, as applicable:

- IRS account history for federal tax compliance (for initial eligibility, as well as periodic checks for continued compliance while actively working on IRS contracts);
- Selective Service registration compliance (for males born after 12/31/59); Contractors must provide proof of registration which can be obtained from the Selective Service website at www.sss.gov;
- U.S. citizenship/lawful permanent residency compliance; If foreign-born, contractors must provide proof of U.S. citizenship or Lawful Permanent Residency status by providing their Alien Registration Number (“A” Number);
- Background investigation forms;
- Credit history;
- Federal Bureau of Investigation fingerprint results; and,
- Review of prior federal government background investigations.

In this regard, Contractor shall furnish the following electronic documents to Personnel Security (PS) at hco.ps.contractor.security.onboarding@irs.gov within 10 business days (or shorter period) of assigning (or reassigning) personnel to this contract/order/agreement and prior to the contractor (including subcontractor) personnel performing any work or being granted staff-like access to IRS SBU or IRS/contractor (including subcontractor) facilities, information systems/assets that process/store SBU information thereunder:

- IRS-provided Risk Assessment Checklist (RAC);
- Non-Disclosure Agreement (if contract terms grant SBU access); and,
- Any additional required security forms, which will be made available through PS and the COR.

Contract Duration:

a. Contractor (including subcontractor) personnel whose duration of employment is 180 calendar days or more per year must meet the eligibility/suitability requirements for staff-like access and shall undergo a background investigation based on the assigned position risk designation as a condition of work under the Government contract/order/agreement.

b. If the duration of employment is less than 180 calendar days per year and the contractor requires staff-like access, the contractor (including subcontractor) personnel must meet the eligibility requirements for staff-like access (federal tax compliance, Selective Service Registration, and US Citizenship or Lawful Permanent Residency), as well as an FBI Fingerprint result screening.

c. For contractor (including subcontractor) personnel not requiring staff-like access to IRS facilities, IT systems, or SBU data, and only require infrequent access to IRS-owned or controlled facilities and/or equipment (e.g., a time and material maintenance contract that warrants access one or two days monthly), an IRS background investigation is not needed and will not be requested if a qualified escort, defined as an IRS employee or as a contractor who has been granted staff- like access, escorts a contractor at all times while the escorted contractor accesses IRS facilities, or vendor facilities where IRS IT systems

hardware or SBU data is stored. As prescribed in IRM 10.23.2, escorting in lieu of staff-like access for IT systems and access to SBU data (escorted or unescorted) will not be allowed.

The contractor (including subcontractor) personnel will be permitted to perform under the contract/order/agreement and have staff-like access to IRS facilities, IT systems, and/or SBU data only upon notice of an interim or final staff-like approval from IRS Personnel Security, as defined in IRM 10.23.2 – Contractor Investigations, and is otherwise consistent with IRS security practices and related IRMs, to include, but not limited to:

- IRM 1.4.6 – Managers Security Handbook;
- IRM 10.2.14 – Methods of Providing Protection; and,
- IRM 10.8.1 - Policy and Guidance.

Current Investigation Reciprocity: Individuals who possess a prior favorably adjudicated Government background investigation that meets the scope and criteria required for their position may be granted interim staff-like access approval upon verification of the prior investigation, receipt of all required contractor security forms, and favorable adjudication of IRS pre-screening eligibility/suitability checks. If their current investigation meets IRS established criteria for investigative reciprocity, individuals will be granted final staff-like access and will not be required to undergo a new investigation beyond an approved pre-screening determination.

Flow down of clauses: The contractor shall include and flow down, in its subcontracts (or arrangements or outsourced service agreements) that entails 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.

(End of Clause)

Notification of Change in Contractor Personnel Employment Status, Assignment, or Standing (Apr 2024)

The contractor, via e-mail (hco.ps.contractor.security.onboarding@irs.gov), shall notify the Contracting Officer (CO), Contracting Officer's Representative (COR), and Personnel Security within one (1) business day of the contractor (including subcontractor) becoming aware of any change in the employment status, information access requirement, assignment, or standing of a contractor (or subcontractor) personnel under this contract or order – to include, but not limited to, the following conditions:

- Receipt of the personnel’s notice of intent to separate from employment or discontinue work under this contract/order;
- Knowledge of the personnel’s voluntary separation from employment or performance on this contract/order (if no prior notice was given);
- Transfer or reassignment of the personnel and performance of duties under this contract/order, in whole or in part, to another contract/order (and if possible, identify the gaining contract/order and representative duties/responsibilities to allow for an assessment of suitability based on position sensitivity/risk level designation);
- Denial of or revocation of staff-like access as determined by IRS Personnel Security;
- Separation, furlough, or release from employment;
- Anticipated extended absence of more than 45 days;

- Change of legal name;
- Change to employment eligibility;
- Change in gender or other distinction when physical attributes figure prominently in the biography of an individual;
- Actual or perceived conflict of interest in continued performance under this contract/order (provide explanation); or
- Death.

When required by the COR, the contractor may be required to provide the information required by this clause to the IRS using the Risk Assessment Checklist (RAC) or security documents as identified by Personnel Security. The notice shall include the following minimum information:

- Name of contractor personnel;
- Nature of the change in status, assignment or standing (i.e., provide a brief non-personal, broad-based explanation);
- Affected contract/agreement/order number(s);
- Actual or anticipated date of departure or separation;
- When applicable, the name of the IRS facility or facilities this individual routinely works from or has staff-like access to when performing work under this contract/order;
- When applicable, contractor (including subcontractor) using contractor (or subcontractor) owned systems for work must ensure that their systems are updated to ensure personnel no longer have continued staff-like access to IRS work, either for systems administration or processing functions; and
- Identification of any Government Furnished Property (GFP), Government Furnished Equipment (GFE), or Government Furnished Information (GFI) (to include Personal Identity Verification (PIV) credentials or badges – also referred to as SmartID Cards) provided to the contractor personnel and its whereabouts or status.

In the event the subject contractor (including subcontractor) is working on multiple contracts, orders, or agreements, notification shall be combined, and the cognizant COR for each affected contract or order (using the Contractor Separation Checklist (Form 14604 (Rev. 8-2016)) shall be included in the joint notification along with Personnel Security. These documents (the RAC and security forms) are also available by email request to Personnel Security.

The vendor POC and the COR must ensure all badges, Smart Cards, equipment, documents, and other government furnished property items are returned to the IRS, systems accesses are removed, and Real Estate & Facilities Management is notified of federal workspace that is vacant.

As a rule, the change in the employment status, assignment, or standing of a contractor (or subcontractor) personnel to this contract or order would not form the basis for an excusable delay for failure to perform under the terms of this contract, order, or agreement.

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.

(End of Clause)

IRS Specialized Information Technology (IT) Security Training (Role-Based) Requirements (Apr 2024)

(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 10.8.1.3 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 Business Entitlement Access Request System (BEARS).

(c) Prior to accessing any IT system, all contractor/subcontractor personnel must 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 July 1st 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 1st of 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 FISMA Training Compliance 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.

(End of Clause)

Safeguards Against Unauthorized Disclosure of Sensitive But Unclassified Information (Apr 2024)

1. Treasury Directive Publication 15-71 (TD P 15-71), Chapter III – Information Security, Section 24 – Sensitive But Unclassified Information defines SBU information as 'any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (USC) (the Privacy Act) but which has not been specifically authorized under criteria established by an executive order or an act of Congress to be kept secret in the interest of national defense or foreign policy.' SBU may be categorized in one or more of the following groups—

- Federal Tax Information (FTI), including any information on or related to a tax return
- Returns and Return Information
- Sensitive Law Enforcement Information
- Employee and Personnel Information
- Personally Identifiable Information (PII)
- Information Collected or Created from Surveys
- Other Protected Information

2. Tax return or tax return information disclosed to the contractor can be used only for a purpose and to the extent authorized herein, and willful disclosure of any such tax return or tax return information for a purpose and to the extent unauthorized for provision of appraisal services to assist with the valuation of conservation easements constitutes a felony, punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five (5) years, or both, together with the costs of prosecution. Any such knowing or negligent unauthorized disclosure of tax return or tax return information may also result in an award of civil damages in an amount not less than $1,000 plus costs with respect to each instance of unauthorized disclosure. These penalties are prescribed by the Internal Revenue Code, Sections 7213 and 7431; see also 26 CFR § 301.6103(n)-1.

3. Contractors who perform work at contractor (including subcontractor) managed sites using contractor or subcontractor managed IT resources shall adhere to the general guidance and specific privacy and security control requirements contained in Publication 4812, Contractor Security & Privacy Controls, IRM 10.23.2 - Personnel Security, Contractor Investigations, IRM 10.5.1 Privacy Policy, and IRM 10.8.1 - Information Technology (IT) Security, Policy and Guidance. Publication 4812 and IRM 10.5.1, 10.8.1 and 10.23.2 provide comprehensive lists of all security, privacy, information protection and disclosure controls and guidance.

4. Eligibility, Fitness and Suitability. Contractor (including subcontractor) personnel hired for work within the United States or its territories and possessions and who require staff-like access, wherever the location, to IRS-owned or controlled facilities or work on contracts that involve the design, operation, repair, or maintenance of information systems, and/or require staff-like access to SBU information, must meet the eligibility requirements under IRM 10.23.2, Personnel Security, Contractor Investigations, and shall be subject to security screening and investigative processing, commensurate with the position sensitivity level, and in accordance with IRM 10.23.2, and TD P 15-71. Contractor (including subcontractor) personnel must be found both eligible and suitable, and approved for staff-like access (interim or final) by IRS Personnel Security prior to starting work on the contract/order, and before being granted access to IRS information systems or SBU information.

5. General Conditions for Allowed Disclosure. Any SBU information, in any format, made available to or created by the contractor (including subcontractor) personnel shall be treated as confidential information

and shall be used only for the purposes of carrying out the requirements of this contract. Inspection by or disclosure to anyone other than duly authorized officer or personnel of the contractor (including subcontractor) shall require prior written approval of the IRS. Requests to make such inspections or disclosures shall be addressed to the CO. Access to SBU information shall be provided on a "need to know" basis. SBU information shall never be indiscriminately disseminated, and no person shall be given access to (or allowed to retain) more SBU information than is needed for performance of their duties, and for which that individual has been authorized to receive as a result of having been successfully investigated, adjudicated, trained to receive, and what is strictly necessary to accomplish the intended business purpose and mission.

6. Nondisclosure Agreement. Consistent with TD P 15-71, Chapter II, Section 2, and IRM 10.23.2.15 - Nondisclosure Agreement for Sensitive but Unclassified Information, each contractor (including subcontractor) personnel who requires staff-like access to SBU information shall complete, sign, and submit to Personnel Security – through the CO (or COR, if assigned) — an approved Nondisclosure Agreement prior to being granted staff-like access to SBU information under any IRS contract or order.

7. Training. All Contractor personnel assigned to this contract with staff-like access to SBU information must complete IRS-provided privacy and security awareness training, including the Privacy, Information Protection, and Disclosure training, as outlined in IR1052.224-9001 Mandatory IRS Security Training for Information Systems, Information Protection and Facilities Physical Access. Contractor personnel required to take the Unauthorized Access to Taxpayer Data training must attest to understanding the penalties for unauthorized access, as instructed by the COR.

8. Encryption. All SBU information must be protected at rest, in transit, and in exchanges (i.e., internal and external communications). The contractor (including subcontractor) shall employ encryption methods and tools to ensure the confidentiality, integrity, and availability of SBU information.

9. Particularly relevant to this clause are the updated sections to IRM 10.8.1 and Publication 4812 regarding email and text messages, alternative work sites, and incident management:

- For email and text messaging, the contractor shall abide by IRM 10.8.1.4.17.2.2 "Electronic Mail (Email) Security", IRM 10.5.1.6.8 "Email" plus all subsections, and IRM 10.8.2.2.1.18 "Contractor"; or Pub. 4812 section 28.3.1 "Electronic Mail (Email) Security,". Included are requirements on encryption, subject line content, and restrictions on personal email accounts.
- For alternate work sites the contractor shall abide by IRM 10.8.1.4.11.16 "PE-17 Alternate Work Site" or Publication 4812 section 21.16 "PE-17 Alternate Work Site,". Included are requirements for incident reporting, encryption, and secure access.

10. Incident and Situation Reporting. Contractors and subcontractors are required to report a suspected or confirmed breach in any medium or form, electronically, verbally or in hardcopy form immediately upon discovery. All incidents related to IRS processing, information or information systems shall be reported immediately upon discovery to the CO, COR, and CSIRC. Contact the CSIRC through any of the following methods:
CSIRC Contacts:
Telephone: 240.613.3606
E-mail to csirc@irs.gov

In addition, if the SBU information is or involves a loss or theft of an IRS IT asset, e.g., computer, laptop, router, printer, removable media (CD/DVD, flash drive, floppy, etc.), or non-IRS IT asset (BYOD device), or a loss or theft of hardcopy records/documents containing SBU data, including PII and tax

information, the contractor shall report the incident/situation to the Treasury Inspector General for Tax Administration (TIGTA) hotline at (800) 366-4484.

11. Staff-Like Access to, Processing and Storage of Sensitive but Unclassified (SBU) Information. The contractor (including subcontractor) shall not allow contractor or subcontractor personnel to access, process, or store SBU on Information Technology (IT) systems or assets located outside the continental United States and its outlying territories.

Contractors (including subcontractors) utilizing their own IT systems or assets to receive or handle IRS SBU data shall not commingle IRS and non-IRS data.

12. Disposition of SBU Information. All SBU information processed during the performance of this contract, or to which the contractor (or subcontractor) was given staff-like access (as well as all related output, deliverables, or secondary or incidental by-products, information or data generated by the contractor or others directly or indirectly from the source material), regardless of form or format, shall be completely purged from all data storage components of the contractor's or subcontractor facilities and computer systems, and no SBU/Personally Identifiable Information (PII) information will be retained by the contractor either--

- When it has served its useful, contractual purpose, and is no longer needed to meet the contractor's (including subcontractor) other, continuing contractual obligations to the IRS or
- When the contract expires, or is terminated by the IRS (for convenience, default, or cause).

The contractor (including subcontractor) shall completely purge from its systems and any other storage, all SBU data, including PII and tax information (originals, copies, and derivative works) within 30 days of the point at which it has served its useful contractual purpose, or the contract expires or is terminated by the IRS (unless, the CO determines, and establishes, in writing, a longer period to complete the disposition of SBU data including PII and tax information).

The contractor shall provide to the IRS a written and signed certification to the COR that all SBU materials/information (i.e., case files, receipt books, PII and material, tax information, removable media (disks, CDs, thumb drives)) collected by, or provided to, the contractor have been purged, destroyed, or returned.

13. Records Management.

A. Applicability

This language applies to all Contractors whose personnel create, work with, or otherwise handle Federal records, as defined in Section B, regardless of the medium in which the record exists. 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.

B. Definitions

"Federal record" as defined in 44 U.S.C. § 3301, includes all recorded information, regardless of form or characteristics, made or received by a Federal agency under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the United States Government or because of the informational value of

data in them.

The term Federal record:

1. includes [Agency] records;
2. does not include personal materials;
3. applies to records created, received, or maintained by Contractors pursuant to their [Agency] contract; and
4. may include deliverables and documentation associated with deliverables.

C. Requirements

1. Contractor shall comply with all applicable records management laws and regulations, as well as National Archives and Records Administration (NARA) records policies, including but not limited to the Federal Records Act (44 U.S.C. chapters 21, 29, 31, 33), NARA regulations at 36 CFR Chapter XII Subchapter B, and those policies associated with the safeguarding of records covered by the Privacy Act of 1974 (5 U.S.C. 552a). These policies include the preservation of all records, regardless of form or characteristics, mode of transmission, or state of completion.

2. In accordance with 36 CFR 1222.32, all data created for Government use and delivered to, or falling under the legal control of, the Government are Federal records subject to the provisions of 44 U.S.C. chapters 21, 29, 31, and 33, the Freedom of Information Act (FOIA) (5 U.S.C. 552), as amended, and the Privacy Act of 1974 (5 U.S.C. 552a), as amended and must be managed and scheduled for disposition only as permitted by statute or regulation.

3. In accordance with 36 CFR 1222.32, Contractor shall maintain all records created for Government use or created in the course of performing the contract and/or delivered to, or under the legal control of the Government and must be managed in accordance with Federal law. Contractors shall ensure that all IRS data and IRS-derived data are in commercially available or open and non-proprietary format for transition (back to IRS) in accordance with the National Archives and Records Administration (NARA) disposition guidance.

4. IRS and its contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Records may not be removed from the legal custody of IRS or destroyed except for in accordance with the provisions of IRM 1.15.5, Relocating/Removing Records, the agency records schedules and with the written concurrence of the CO. Willful and unlawful destruction, damage or alienation of Federal records is subject to the fines and penalties imposed by 18 U.S.C. 2701. In the event of any unlawful or accidental removal, defacing, alteration, or destruction of records, Contractor must immediately notify the appropriate CO. The CO must report the loss using the PII Breach Reporting Form. Privacy, Governmental Liaison and Disclosure (PGLD, Incident Management) will review the PII Breach Reporting Form and alert the Records and Information Management (RIM) Program Office that a suspected records loss has occurred. The agency must report promptly to NARA in accordance with 36 CFR 1230.

5. The Contractor shall immediately notify the appropriate CO immediately upon discovery of any inadvertent or unauthorized disclosures of information, data, documentary materials, records, or equipment. Disclosure of non-public information is limited to authorized personnel with a need-to-know as described in the [contract vehicle]. The Contractor shall ensure that the appropriate personnel, administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, documentary material, records and/or equipment is properly

protected. The Contractor shall not remove material from Government facilities or systems, or facilities or systems operated or maintained on the Government's behalf, without the express written permission of the Head of the Contracting Activity. When information, data, documentary material, records and/or equipment is no longer required, it shall be returned to IRS control, or the Contractor must hold it until otherwise directed. Items returned to the Government shall be hand-carried, mailed, emailed, or securely electronically transmitted to the CO or address prescribed in the [contract vehicle]. Destruction of records is EXPRESSLY PROHIBITED unless in accordance with Paragraph (4).

6. The Contractor is required to obtain the approval of the CO prior to engaging in any contractual relationship (sub-contractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, contracts. The Contractor (and any sub-contractor) is required to abide by Government and [Agency] guidance for protecting sensitive, proprietary information, and controlled unclassified information.

7. The Contractor shall only use Government IT equipment for purposes specifically tied to or authorized by the contract and in accordance with IRS policy.

8. The Contractor shall not create or maintain any records containing any non-public IRS information that are not specifically tied to or authorized by the contract.

9. The Contractor shall not retain, use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974, Internal Revenue Code section 6103, or that which is generally protected from public disclosure by an exemption to the Freedom of Information Act.

10. IRS owns the rights to all data and records produced as part of this contract. All deliverables under the contract are the property of the U.S. Government for which IRS shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest. Any Contractor rights in the data or deliverables must be identified as required by FAR 52.227-11 through FAR 52.227-20.

11. Training. All Contractor personnel assigned to this contract who create, work with, or otherwise handle records are required to take IRS-provided records management training. The Contractor is responsible for confirming training has been completed according to agency policies, including initial training and any annual or refresher training.

D. Flow down of requirements to subcontractors

1. The Contractor shall incorporate the substance of this language, its terms, and requirements including this paragraph, in all subcontracts under this [contract vehicle], and require written subcontractor acknowledgment of same.

2. Violation by a subcontractor of any provision set forth in this language will be attributed to the Contractor.

3. Other Safeguards. [Insert any additional disclosure safeguards provided by the Program Office/COR or that the CO determines are necessary and in the best interest of the Government and not addressed elsewhere in the contract. If none are entered here, there are no other safeguards applicable to this contract action.]

(End of Clause)

Mandatory IRS Security Training for Information Systems, Information Protection and Facilities Physical Access (Apr 2024)

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 and details that any violation of the Act could result in civil and criminal penalties. 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
- 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,

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 10 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.

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 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 substantially 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.

(End of Clause)

Electronic Invoicing and Payment Requirements for the Invoice Processing Platform (IPP) (Jul 2019)

(a) Definitions:

"Short payment" as used in this clause means the partial payment of an invoice for goods/services actually rendered at the time of payment when the invoice includes additional goods/services that have not yet been provided/rendered.

“Short payment” example: The contract requires the delivery of a set number of items, with the price, delivery location, and delivery due date also specified. The vendor delivers 50% of the items as specified but invoices for 100% of the items. Before implementation of the IPP, the IRS would have paid the vendor for the items delivered and instructed the vendor to re-invoice the IRS when the balances of the items were delivered. In other words, the IRS would "short pay" the invoice since the IRS did not remit

payment for the full invoice amount. With implementation of the IPP, the IRS can no longer do this because the IRS cannot accept an electronic invoice that includes items not yet received. The IRS will reject the invoice. The vendor needs to submit an invoice for only the items received by the IRS (in this case, 50%), and, if these items meet all other contract terms and conditions, the IRS will pay the invoiced amount. The vendor submits subsequent invoice(s) for items as they are delivered and accepted.

(a) The Invoice Processing Platform (IPP) is a secure Web-based electronic invoicing and payment information service available to all Federal agencies and their suppliers. Effective October 1, 2012, invoicing for payment through the IPP will be mandatory for all new contract awards. Additional information regarding the IPP may be found at the IPP website address https://www.ipp.gov. Contractors must complete the contractor point of contact information below and submit it with their proposal submissions. Contractors may contact the IPP Helpdesk for assistance via e-mail at ippgroup@stls.frb.org or via phone at (866) 973-3131. Once a contract award has been made, the contractor will be contacted by the IPP via e-mail to set-up an account. It will be necessary for contractors to login to their IPP accounts every 90 days to keep their IPP accounts active.

(b) Contractor Point of Contact Information

Contractor Name: Palantir Technologies, Inc
Contractor IPP Point of Contact Name: (b)(6)
Contractor Phone Number: (b)(6)
Contractor E-mail Address: (b)(6)

(c) Electronic Invoicing and Payment Requirements

Vendor invoices submitted electronically through the IPP should be in the proper format and contain the information required for payment processing. To be approved for payment, a “proper invoice” must list the items specified in FAR 52.232-25 (a)(3)(i) through (a)(3)(x), or in the case of a Commercial Item Contract, the items included in 52.212-4(g)(1)(i) through (g)(1)(x).

Under this contract, the following documents are required to be submitted as an attachment to the invoice (Contracting Officer fills in additional documentation that must be furnished by the contractor (e.g. timesheet)).

Payment and Invoice Questions

For payment and invoice questions, contact the Ancillary Systems at (304) 254-3372 or via e- mail at cfo.fm.ipp.customer.support@irs.gov.

(b) Waiver

If the Contractor is unable to use the IPP for submitting payment requests starting on October 1, 2012, then a waiver form must be completed and submitted with the contractor’s proposal submission for review and approval by the Contracting Officer based on one of the conditions listed in the waiver. The vendor will be notified prior to award as to whether their request for waiver has been approved or denied. If the waiver is granted, then a copy of the waiver must be submitted with each paper invoice that the vendor submits to the payment office, or the invoice will be returned.

(c) Short Payment

Short payment on vendor submitted invoices will no longer be processed or paid. If any portion of the invoice does not meet the requirements for a proper invoice, the entire invoice shall be rejected and returned to the vendor unpaid.

IRS Invoice Processing Platform (IPP) Waiver Form

The IRS invoicing and payment requirements clause (IR1052.232-9000) requires that all invoices under awards made (or effective) on or after October 1, 2012, be submitted electronically via the IPP unless a waiver is requested and granted. If the Contractor is unable to submit its invoice through the IPP, the Contractor shall complete this waiver form indicating the reason for the waiver request by selecting the appropriate box below and providing a narrative summarizing in detail the circumstances requiring a waiver. For a solicitation, submit the waiver form with the proposal submission. For a modification that incorporates the IPP clause into an existing contract, submit the waiver form with the modification. The CO will notify the vendor via e-mail or another appropriate means of communication prior to award as to whether their waiver has been approved or denied. If the waiver is granted, then a copy of the approved waiver must be submitted with each invoice that the vendor submits to the payment office, or the invoice will be returned.

Reason for requesting a waiver of the requirement to submit an electronic invoice via the IPP:

☐ 1. Submission of invoices through IPP would impose a hardship on an individual (includes employees and sole proprietors) due to: either a physical or mental disability; a geographic, language, or literacy barrier; or an undue financial burden. The requirement to submit invoices through the IPP is automatically waived for all individuals who do not have payment capability using ACH with a U.S. financial institution.

☐ 2. The political, financial or communications infrastructure where the place of business is located does not support access to the IPP for submitting invoices electronically.

☐ 3. The contractor is located within an area designated by the President of the United States or an authorized agency administration as a disaster area. (Please identify area/location.)

☐ 4. The submission of invoices electronically may pose a threat to national security, the life or physical safety of an individual may be endangered, or a law enforcement action may be compromised.

☐ 5. The agency does not expect to receive more than one invoice from the same contractor within a one-year period. i.e., the invoice submission is non-recurring.

☐ 6. The contractor customarily submits a high volume of invoices on a regular basis via file format, not currently supported by the IPP (i.e., uses a file format other than XML or CSV) and the high volume of invoices would cause a significant burden to the contractor if submitted through the IPP individually. If utilizing this exception, please identify the file formats supported by your invoicing system so that the IPP may consider implementing the requested file format at a later date. File format(s) used:

☐ 7. Other - Please explain:

Attach a separate sheet of paper with a summary narrative substantiating the circumstances for the waiver exception selected from above (1 through 7).

Waiver Submitted By:

_____
Contractor Name

_____ _____
Name of Person Submitting Request for Waiver

_____

Title Signature of Person Submitting Request for Waiver

E-ail Address

Phone No.

Contract/Order No.

Date Submitted

Waiver Approved By:

Contracting Officer's Name Printed

Contracting Officer's Signature

Date

(End of clause)

Section 508 Information, Documentation and Support (Dec 2019)

In accordance with 36 CFR, Appendix C to Part 1194, the information and communication technology (ICT) products and product support services documentation furnished in performance of this contract shall be provided at no additional cost. The contractor shall provide information, documentation, and support relative to the supplies and services as described in the statement of work, performance work statement or statement of objectives (select one). The following technical standards and provisions have been determined to be applicable to this contract:

_X__ **Chapter 6: Support Documentation and Service**s
_X__ 601 General
_X__ 601.1
_X__ 602 Support Documentation
_X__ 602.1 _X__ 602.2 _X__ 602.3 _X__ 602.4
_X__ 603 Support Services
_X__ 603.1 _X__ 603.2 _X__ 603.3

(End of clause)

Section 508 Conformance (Apr 2024)

Each information and communication technology (ICT) product and/or product related service delivered under the terms of this contract, at a minimum, shall conform to the applicable accessibility standards at 36 CFR, Appendix C to Part 1194 at the level of conformance as specified in the Attachment entitled, "(Please state where attachment may be found and name of attachment for example, Section J., Voluntary Product Accessibility Template (VPAT) or Section J., Evaluation Matrix)."

The following technical standards have been determined to be applicable to this contract:

__x_ **Chapter 4: Hardware**
_x__ 401 General
___ 401.1
__x_ 402 Closed Functionality

_x__ 402.1 __x_ 402.2(1-6) _x__ 402.3 _x__ 402.4 _x__ 402.5
_x__ 403 Biometrics
_x__ 403.1
_x__ 404 Preservation of Information Provided for Accessibility
_x__ 404.1
_x__ 405 Privacy
_x__ 405.1
_x__ 406 Standard Connections
_x__ 406.1
_x__ 407 Operable Parts
_x__ 407.1 __x_ 407.2 _x__ 407.3 _x__ 407.4 _x__ 407.5 __x_ 407.6 __x_ 407.7 _x__ 407.8
_x__ 408 Display Screens
_x__ 408.1 _x__ 408.2 _x__ 408.3
_x__ 409 Status Indictors
_x__ 409.1
_x__ 410 Color Coding
__x_ 410.1
__x_ 411 Audible Signals
_x__ 411.1
___ 412 ICT with Two-Way Communication
___ 412.1 ___ 412.2 ___ 412.3 ___ 412.4 ___ 412.5 ___ 412.6 ___ 412.7 ___412.8
___ 413 Closed Caption Processing Technologies
___ 413.1
___ 414 Audio Description Processing Technologies
___ 414.1
___ 415 User Controls for Captions and Audio Descriptions
___ 415.1
_X__ **Chapter 5: Software**
_X__ 501 General
_X__ 501.1
_X__ 502 Interoperability with Assistive Technology
_X__ 502.1 _X__ 502.2 _X__ 502.3 _X__ 502.4(A-G)
_X__ 503 Applications
_X__ 503.1 _X__ 503.2 _X__ 503.3 _X__ 503.4
_X__ 504 Authoring Tools
_X__ 504.1 _X__ 504.2 _X__ 504.3 _X__ 504.4
_X__ **Chapter 7: Referenced Standards**
_X__ 701 General
_X__ 701.1
_X__ 702 Incorporation by Reference
_X__ 702.1 ___ 702.2 _X__ 702.3 _X__ 702.4 ___ 702.5 __x_ 702.6 ___ 702.7 ___ 702.8 ___ 702.9 _X__ 702.10

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the ICT be compatible with such software and devices so that it can be made accessible if so, required by the agency in the future.

The following functional performance criteria (36 CFR Chapter 3) apply to this contract.

_X__ **Chapter 3: Functional Performance Criteria**

_X__ 301 General
_X__ 301.1
_X__ 302 Functional Performance Criteria
_X__ 302.1 _X__ 302.2 _X__ 302.3 _X__ 302.4 _X__ 302.5 _X__ 302.6 _X__ 302.7 _X__ 302.8 _X__ 302.9

(End of clause)

Section 508 Services (Apr 2024)

All contracts, solicitations, purchase orders, delivery orders and interagency agreements that contain a requirement of services which will result in the delivery of a new or updated information and communication technology (ICT) item/product must conform to the applicable provisions of the appropriate technical standards in 36 CFR, Appendix C to Part 1194, and functional performance criteria in 36 CFR Chapter 3, unless an agency exception to this requirement exists at E202 General Exceptions .

The following technical standards and provisions have been determined to be applicable to this contract:

_x__ **Chapter 4: Hardware**
_x__ 401 General
_x__ 401.1
_x__ 402 Closed Functionality
__x_ 402.1 _x__ 402.2(1-6) _x__ 402.3 _x__ 402.4_x__ 402.5
_x__ 403 Biometrics
_x__ 403.1
_x__ 404 Preservation of Information Provided for Accessibility
_x_ 404.1
_x__ 405 Privacy
_x__ 405.1
_x__ 406 Standard Connections
_x__ 406.1
__x_ 407 Operable Parts
_x__ 407.1 _x__ 407.2 _x__ 407.3 __x_ 407.4__x_ 407.5 __x_ 407.6 _x__ 407.7 __x_ 407.8
__x_ 408 Display Screens
_x__ 408.1 __x_ 408.2 __x_ 408.3
_x__ 409 Status Indictors
_x__ 409.1
__x_ 410 Color Coding
_x__ 410.1
_x__ 411 Audible Signals
_x__ 411.1
___ 412 ICT with Two-Way Communication
___ 412.1 ___ 412.2 ___ 412.3 ___ 412.4 ___ 412.5 ___ 412.6 ___ 412.7 ___412.8
___ 413 Closed Caption Processing Technologies
___ 413.1
___ 414 Audio Description Processing Technologies
___ 414.1
___ 415 User Controls for Captions and Audio Descriptions
___ 415.1
_X__ **Chapter 5: Software**

_X__ 501 General
_X__ 501.1
_X__ 502 Interoperability with Assistive Technology
_X__ 502.1 _X__ 502.2 _X__ 502.3 _X__ 502.4(A-G)
_X__ 503 Applications
_X__ 503.1 _X__ 503.2 _X__ 503.3 _X__ 503.4
_X__ 504 Authoring Tools
_X__ 504.1 _X__ 504.2 _X__ 504.3 _X__ 504.4
_X__ **Chapter 7: Referenced Standards**
_X__ 701 General
_X__ 701.1
_X__ 702 Incorporation by Reference
_X__ 702.1 ___ 702.2 _X__ 702.3 _X__ 702.4 ___ 702.5 _X__ 702.6 ___ 702.7 ___ 702.8 ___ 702.9 _X__ 702.10

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the ICT be compatible with such software and devices so that it can be made accessible if so, required by the agency in the future.

The following functional performance criteria (36 CFR Chapter 3) apply to this contract.

_X__ **Chapter 3: Functional Performance Criteria**
_X__ 301 General
_X__ 301.1
_X__ 302 Functional Performance Criteria
_X__ 302.1 _X__ 302.2 _X__ 302.3 _X__ 302.4 _X__ 302.5 _X__ 302.6 _X__ 302.7 _X__ 302.8 _X__ 302.9

(End of clause)

Section 508 Accessibility of Information and Communication Technology (100% Compliance) (Apr 2024)

Each information and communication technology (ICT) product or service furnished under this contract shall comply with the Information and Communication Technology Accessibility Standards (36 CFR, Appendix C to Part 1194). If the Contracting Officer determines any furnished products or services are not in compliance with the contract, the Contracting Officer will apply the remedies described under FAR 52.246-2, Inspection of Supplies – Fixed Price or FAR 52.246-4, Inspection of Services – Fixed Price.
The following technical standards and provisions have been determined to be applicable to this contract:
_x__ **Chapter 4: Hardware**
_x__ 401 General
_x__ 401.1
_x__ 402 Closed Functionality
__x_ 402.1 _x__ 402.2(1-6) _x__ 402.3 _x__ 402.4_x__ 402.5
_x__ 403 Biometrics
_x__ 403.1
_x__ 404 Preservation of Information Provided for Accessibility
_x_ 404.1
_x__ 405 Privacy

_x__ 405.1
_x__ 406 Standard Connections
_x__ 406.1
__x_ 407 Operable Parts
_x__ 407.1 _x__ 407.2 _x__ 407.3 __x_ 407.4__x_ 407.5 __x_ 407.6 _x__ 407.7 __x_ 407.8
__x_ 408 Display Screens
_x__ 408.1 __x_ 408.2 __x_ 408.3
_x__ 409 Status Indictors
_x__ 409.1
__x_ 410 Color Coding
_x__ 410.1
_x__ 411 Audible Signals
_x__ 411.1
___ 412 ICT with Two-Way Communication
___ 412.1 ___ 412.2 ___ 412.3 ___ 412.4 ___ 412.5 ___ 412.6 ___ 412.7 ___412.8
___ 413 Closed Caption Processing Technologies
___ 413.1
___ 414 Audio Description Processing Technologies
___ 414.1
___ 415 User Controls for Captions and Audio Descriptions
___ 415.1
_X__ **Chapter 5: Software**
_X__ 501 General
_X__ 501.1
_X__ 502 Interoperability with Assistive Technology
_X__ 502.1 _X__ 502.2 _X__ 502.3 _X__ 502.4(A-G)
_X__ 503 Applications
_X__ 503.1 _X__ 503.2 _X__ 503.3 _X__ 503.4
_X__ 504 Authoring Tools
_X__ 504.1 _X__ 504.2 _X__ 504.3 _X__ 504.4
_X__ **Chapter 7: Referenced Standards**
_X__ 701 General
_X__ 701.1
_X__ 702 Incorporation by Reference
_X__ 702.1 ___ 702.2 _X__ 702.3 _X__ 702.4 ___ 702.5 _X__ 702.6 ___ 702.7 ___ 702.8 ___ 702.9 _X__ 702.10

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the ICT be compatible with such software and devices so that it can be made accessible if so, required by the agency in the future.

The following functional performance criteria (36 CFR Chapter 3) apply to this contract.

_X__ **Chapter 3: Functional Performance Criteria**
_X__ 301 General
_X__ 301.1
_X__ 302 Functional Performance Criteria
_X__ 302.1 _X__ 302.2 _X__ 302.3 _X__ 302.4 _X__ 302.5 _X__ 302.6 _X__ 302.7 _X__ 302.8 _X__ 302.9

(End of Clause)

Staff-Like Access, Use or Operation of IRS Information Technology (IT) Systems By Contractors (Apr 2024)

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

1. IRS Information Technology Security Policy and Guidance. All current and new IRS contractor (including subcontractor) personnel authorized staff-like access to Treasury/IRS owned or controlled facilities and information systems, or work, wherever located, on those contracts, which involve the design, operation, repair or maintenance of information systems and staff-like access to Sensitive But Unclassified (SBU) information shall comply with the IRS Information Technology Security Policy and Guidance, Internal Revenue Manual (IRM) 10.8.1 Policy and Guidance, 10.8.2 IT Security Roles and Responsibilities, and IRS Publication 4812.

Copies of IRM 10.8.1 and 10.8.2 are available at http://www.irs.gov/irm/. This requirement applies to contractors who are using contractor/subcontractor-managed systems, including laptop computers, workstations, servers, and other IT resources at contractor managed facilities. A copy of the most recent version of Publication 4812 is available at https://www.irs.gov/pub/irs-pdf/p4812.pdf.

2. Staff-Like Access Request and Authorization. Within ten (10) business days after contract award or issuance of an order, the contractor shall provide the Contracting Officer's Representative (COR) and Personnel Security, via email to hco.ps.contractor.security.onboarding@irs.gov list of names of all applicable contractor and subcontractor personnel and the IRS location(s) identified in the contract for which staff-like access is requested. Personnel Security will conduct an initial screening to determine eligibility and suitability for staff- like access in accordance with IRM 10.23.2, Contractor Investigations, and Department of the Treasury Security Manual (TD P) 15-71, Chapter II, Section 2.

Contractor and subcontractor personnel are not permitted to begin work on the contract or order until approved for interim staff-like access (at a minimum) as defined in IRM10.23.2. This is consistent with IRS security practices and related IRMs, to include, but not limited to, IRM 1.4.6 – Managers Security Handbook, IRM 10.2.14 – Methods of Providing Protection, and IRM 10.8.1 - Policy and Guidance.

Upon notification of a favorable suitability determination and interim staff-like approval, the COR will complete an Online 5081 (OL5081), Automated Information System User Registration/Change Request, for each prime or subcontractor personnel and require an electronic signature from each such personnel indicating the contractor personnel has read and fully understands the security requirements governing staff- like access to the Service's IT systems.

3. Remote Staff-Like Access. If the contract authorizes staff-like access to IRS IT systems, information, or assets remotely; that is, from the contractor or other facility, office, or site, the requirements of this clause governs, as well as the general guidance and specific security control standards in IRS Publication 4812, Contractor Security Controls. 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.

4. Contractor Acknowledgement. The contractor also acknowledges and agrees: (a) That personnel must comply with all laws, IRS system security rules and security policies, standards, and procedures, and (b) That any one of its personnel unsanctioned, negligent, or willful violation of the laws, system security rules, and security policies, standards, and procedures may result in the revocation of staff-like access to IRS information technology systems, immediate removal from IRS premises and the contract, and may be subject to arrest by Federal law enforcement agents.

5. Limited Personal Use of Government IT Resources.

a. Contractor (including subcontractor) personnel, like Federal employees, have no inherent right to use Government IT resources and this policy does not create the right to use Government IT resources for nongovernmental purposes. See IRM 10.8.27, Exhibit 10.8.27-1, Prohibited Uses of Government IT Resources, for specific examples of prohibited uses. See Title 5 - Code of Federal Regulations (CFR) - Part 734 – Political Activities of Federal Employees, for specific examples of prohibited political activities.

b. Contractors and subcontractors are required to report a suspected or confirmed breach in any medium or form, electronically, verbally or in hardcopy form, immediately upon discovery. All incidents related to IRS processing, information or information systems shall be reported immediately upon discovery to the CO, COR, and CSIRC. Contact the CSIRC through any of the following methods:
Telephone: 240-613-3606
E-mail to csirc@irs.gov

- Information about unclassified cyber security incidents of a sensitive nature shall be transmitted using secure messaging or alternative forms of encryption.
- If the incident involves the loss or theft of an IRS IT asset, e.g., computer, laptop, router, printer, removable media (CD/DVD, flash drive, floppy, etc.), or non-IRS IT asset (BYOD device), or a loss or theft of hardcopy records/documents containing SBU data, including PII and tax information, the contractor shall also report the incident/situation to the Treasury Inspector General for Tax Administration (TIGTA) hotline at 800-366-4484.

6. Replacement Personnel. Contractor personnel who violate any conditions set forth in the clause are subject to removal from performance under the contract. The Government will provide notice to the Contractor of any contractor personnel no longer eligible for performance under the contract. The Contractor shall provide the name of the proposed replacement personnel to the CO and COR within five (5) business days from receipt of notice. The Contractor shall ensure replacement personnel have similar or equal credentials to the personnel being replaced.
7. Monitoring Notification. IRS management retains the right to monitor both the content and the level of access of contractor personnel use of IRS IT systems. Contractor personnel do not have a right, nor should they have an expectation, of privacy while using any IRS information technology system at any time, including accessing the Internet or using e-mail.
8. Security Reports and Information. If any reports are required, the COR may direct the submission of such reports and information through a specific IRS application, to be determined, or the entry of specific information into the application or system.
9. Subcontracts. The Contractor shall incorporate this clause in all subcontracts, subcontract task or delivery orders or other subcontract performance instrument where the subcontractor personnel will require staff-like access, use or operation of IRS information technology systems.
10. Flow down of clauses: The contractor shall include and flow down, in its subcontracts (or arrangements or outsourced service agreements) that entails 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.

(End of Clause)

Information Systems and Information Security Controls for Contracting Actions Subject to Internal Revenue Manual (IRM) 10.8 Series (Apr 2024)

In performance of this contract, the contractor agrees to comply with the following requirements and assumes responsibility for compliance by its personnel and subcontractors (and their personnel):
(a) General. The contractor shall ensure IRS information and information systems are protected at all times. 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) IRM 10.5.1 and 10.8 Series applicability. This contract action is subject to Internal Revenue Manual (IRM) Part 10.8– Information Technology (IT) Security, Policy and Guidance, and IRM 10.5 – Privacy and Information Protection series. The contractor shall adhere to the general guidance and specific security control standards or requirements contained in IRM 10.5 and IRM10.8 series. While the IRM

10.8 series shall apply to the requirements to access systems, and IRM 10.5 series shall apply to access SBU data, IRS Publication 4812, Contractor Security & Privacy Controls, may also govern as addressed in another clause. It will address the requirements related to physical and personnel security that must continue to be maintained at contractor sites.
(c) Based on the Federal Information Security Modernization Act of 2014 (FISMA), and standards and guidelines developed by the National Institute of Standards and Technology (NIST), IRM 10.8 series provides overall IT security control guidance for the IRS, and uniform policies and guidance to be used by each office, or business, operating, and functional unit within the IRS that uses IRS information systems to accomplish the IRS mission.
(d) Contractor Security Representative. The contractor shall assign and identify, in its offer, a Contractor Security Representative (CSR) and alternate CSR to all contracts requiring staff-like access to IRS information, information technology and systems, facilities, and/or assets. The CSR is the contractor's primary point for the Government on all security-related matters and the person responsible for ensuring the security of information and information systems in accordance with the terms and conditions of the contract and all applicable security controls. If required by the Contracting Officer's Representative, 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.
(e) Flow down of clauses. The contractor shall include and flow down, in its subcontracts (or arrangements or outsourced service agreements) that entail staff-like access to SBU information by a subcontractor or agent, at any tier, the substantially 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.

(End of Clause)

Information Systems and Information Security Controls for Contracting Actions Subject to IRS Publication 4812 (Apr 2024)

Publication 4812 is an IRS specific guide to NIST SP 800-53 (version 4.0) when staff- like 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).
The IRS Publication 4812 is a living document and updated annually to reflect changes from Executive Orders, OMB requirements, NIST updates, etc. The most current version (October 2019) of Publication 4812 is located on the irs.gov website.
In performance of this contract, the contractor agrees to comply with the following requirements and assumes responsibility for compliance by its personnel and subcontractors (and their personnel):
1. The contractor shall ensure IRS information and information systems (those of the IRS and/or the contractor, as appropriate) are protected at all times. 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.
(a) 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. Publication 4812 applicability. This contracting action is subject to Publication 4812 – Contractor Security & Privacy Controls. Publication 4812 is available at: https://www.irs.gov/pub/irs-pdf/p4812.pdf
(b) The contractor shall adhere to the general guidance and specific security control standards or requirements contained in Publication 4812. By inclusion of this clause in the contract, the most recent version of Publication 4812 is incorporated into the contract and has the same force and effect as if

included in the main body of the immediate contract.
2. Flowing down from the Federal Information Security Modernization Act of 2014 (FISMA) and standards and guidelines developed by the National Institute of Standards and Technology (NIST), Publication 4812 identifies basic Technical, Operational, and Management (TOM) security controls and standards required of under contracts for services in which contractor (or subcontractor) personnel will either—
(a) Have staff-like access to, develop, operate, or maintain IRS information or information systems on behalf of the IRS (or provide related services) outside of IRS facilities or the direct control of the Service, and/or
(b) Have staff-like access to, compile, process, or store IRS SBU information on their own information systems/Information Technology (IT) assets or that of a subcontractor or third- party Service Provider, or when using their own information systems (or that of others) and on IT, or Electronic Information and Technology (EIT) (as defined in FAR Part 2) other than that owned or controlled by the IRS.
3. Unless the manual specifies otherwise, the IRS-specific requirements in Publication 4812 meet the standard from the latest version of the NIST Special Publication (SP) 800-53 (Version 4.0) – Federal Information Systems and Organizations. The security controls, requirements, and standards described within the Publication 4812 are to be used in lieu of the common, at-large security control standards enumerated in NIST SP 800-53 (Version 4.0).
Publication 4812 also describes the framework and general processes for conducting contractor security reviews – performed by IT Cybersecurity—to monitor compliance and assess the effectiveness of security controls applicable to any given contracting action subject to Publication 4812.
4. Contractor Security Representative. The contractor shall assign and identify, upon award, a Contractor Security Representative (CSR) and alternate CSR to all contracts requiring staff-like access to Treasury/bureau information, information technology and systems, facilities, and/or assets. The CSR is the contractor's primary point for the Government on all security-related matters and the person responsible for ensuring the security of information and information systems in accordance with the terms and conditions of the contract and all applicable security controls.
5. 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. IRS Publication 4812 also applies to subcontractors.

(End of Clause)

Information System and Information Security Control Standards and Guidelines Applicability (Apr 2024)

As part of its information security program, IRS identifies security controls for the organization's information and information systems in the following two key standards and guiding documents:

- Internal Revenue Manual (IRM) 10.8.1 – Information Technology (IT) Security, Policy and Guidance, and
- Publication 4812 – Contractor Security & Privacy Controls.

While IRM 10.8.1 and Publication 4812 are both based on the latest version of NIST SP 800-53, they apply to different operating environments—internal and external to the organization, respectively.
The contractor, by signing its offer, hereby asserts to the best of its knowledge and belief that the security control guideline(s) most suitable and applicable to the immediate contracting action, with due consideration to its proposed approach (and work environment) for fulfilling

the Government's requirements and standards for applicability described herein, is as follows (check only one block):
IRM 10.8.1 Publication 4812 Both IRM 10.8.1 and Publication 4812
Unless IRS Cybersecurity, (Contractor Security Assessment - CSA) determines, through a notification to the Contractor by the CO, that a different (or a second) security control standard or guideline is warranted, the security level selected/applied for by the contractor under IR1052.239-9010 shall stand. In the event IRS Cybersecurity (Contractor Security Assessment - CSA) determines a different (or second) security control standard or guideline is warranted, the CO shall advise the contractor, in writing, of the Government determination, and reflect the correct/appropriate security control standard or guideline in the ensuing contract.

If Publication 4812 is selected (alone or in combination with IRM 10.8.1) as the most suitable security control guideline, the Contractor must identify, as part of its proposal submissions (or its submissions under any modification to an existing contract incorporating this clause), the most suitable security control level within the following hierarchy of security control levels (from lowest or highest):
Software Application Development or Maintenance (SOFT)
Networked Information Technology Infrastructure (NET)

(See Publication 4812, Appendix C for guidance in selecting the security control level most suitable and appropriate to the immediate contracting action. If additional guidance is needed in selecting the security control level, contact IRS Cybersecurity (Contractor Security Assessment - CSA).

The contractor, by signing its offer, hereby asserts to the best of its knowledge and belief that the security control level under Publication 4812 most suitable and applicable to the immediate contracting action, with due consideration to its proposed approach (and work environment) and standards for applicability described herein, is as follows (check only one):

SOFT NET

Unless IRS Cybersecurity (Contractor Security Assessment - CSA) determines that a different (higher or lower) security control level is warranted for contracts subject to the most recent version of Publication 4812, the security level selected/applied for by the contractor will govern throughout the life of the contract. In the event the IRS Cybersecurity (Contractor Security Assessment - CSA) determines a different (higher or lower) security level is warranted, the CO will advise the contractor, in writing, of the Government determination. At the end of the contract, for all security levels, the contractor must provide a plan and document the implementation of this plan to ensure that all hard copy and electronic data is returned to the IRS, sanitized, or destroyed.
Failure by the contractor to check any block will result in the use of both guidelines (for the Publication 4812 portion, use of the most stringent security control level (Software)) until and unless IRS Cybersecurity (Contractor Security Assessment - CSA), determines otherwise via notification to the Contractor by the CO.

If required by the Contracting Officer's Representative (COR), 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.
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 substantially 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.

(End of Clause)

ORDER FOR SUPPLIES OR SERVICES

2026 05526 0000022958 UNCLASSIFIED 5/28/2026

PAGE 1 OF PAGES 20

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER: 09/24/2025	2. CONTRACT NO. *(If any)*: 2023H2-25-A-00002
3. ORDER NO.: 205AE9-25-F-00202	4. REQUISITION/REFERENCE NO.: 5000219526

5. ISSUING OFFICE *(Address correspondence to)*:
Office of Procurement Operations-Application Development Branch
51 Haddonfield Road
Cherry Hill, NJ 08002
Attn: Rayshiena Shelly
Tel: Email: (b)(6)

7. TO:

a. NAME OF CONTRACTOR: PALANTIR TECHNOLOGIES INC.

b. COMPANY NAME:

c. STREET ADDRESS: 1200 17th Street, Floor 15

d. CITY	e. STATE	f. ZIP CODE
Denver	CO	80202

6. SHIP TO:

a. NAME OF CONSIGNEE: See Attached Delivery Schedule

b. STREET ADDRESS:

c. CITY	d. STATE	e. ZIP CODE

f. SHIP VIA:

8. TYPE OF ORDER

☐ a. PURCHASE
REFERENCE YOUR:
Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.

☐ b. DELIVERY -- Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA: See Attached Schedule(s)

10. REQUISITIONING OFFICE:

11. BUSINESS CLASSIFICATION (*Check appropriate box(es)*)
☐ a. SMALL ☒ b. OTHER THAN SMALL ☐ c. DISADVANTAGED ☐ d. WOMEN-OWNED ☐ e. HUBZone
☐ f. SERVICE-DISABLED VETERAN-OWNED ☐ g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM ☐ h. EDWOSB

12. F.O.B. POINT:

13. PLACE OF a. INSPECTION	13. PLACE OF b. ACCEPTANCE	14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE *(Date)*	16. DISCOUNT TERMS

17. SCHEDULE ***(See reverse for Rejections)***

ITEM NO (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	See Attached Schedule(s)					

SEE BILLING INSTRUCTIONS ON REVERSE

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.		17(h) TOT. *(Cont. pages)*

21. MAIL INVOICE TO:
a. NAME: Invoices must be submitted via IPP
b. STREET ADDRESS *(or P.O. Box)*:
c. CITY | d. STATE | e. ZIP CODE

$14,244,448.96 — 17(i) GRAND TOTAL

22. UNITED STATES OF AMERICA BY *(Signature)*: Rayshiena N. Shelly
Digitally signed by Rayshiena N. Shelly
Date: 2025.09.24 08:59:27 -04'00'

23. NAME *(Typed)*: Rayshiena N. Shelly
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 347 (REV. 2/2012)
Prescribed by GSA/FAR 48 CFR 53.213(f)

SECTION B

Line Item Table

Item No.	FSC	Item Description	QTY	Unit	Unit Price	Total Value
0001	DE01	UAPI and EDP Core Functionality 09/24/2025-09/23/2026	(b)(4)			

Accounting and Appropriation Data

ACCT. Line No.	Accounting and Appropriation Data	Amount
0001-0001	(b)(4)	

Delivery Schedule

Delivery Address	Item No.	QTY	Delivery Date
	0001	(b)(4)	09/23/2026

52.217-8 Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 60 days.

(End of clause)

Performance Work Statement (PWS) for the API Layer and Platform Engineering Horizontal - Palantir Software Solutions Unified API and Core Functionality

1.0 INTRODUCTION

The purpose of this Performance Work Statement is to acquire contractor support for the implementation, deployment, and sustainment of a secure, ontology-driven data integration platform that enables IRS led initiatives to modernize data access, enhance cross-system interoperability, and provide a standardized Unified API framework. The initiative supports legislative mandates, Executive Orders, and IRS modernization efforts aimed at transforming taxpayer experience and improving compliance operations through semantic data modeling, API exposure, and secure cloud-ready infrastructure. The initiative will build a secure, scalable data ecosystem using Palantir Foundry, delivering integrated access to mission-critical IRS data assets via a Unified API and a semantically driven enterprise data model.

The contractor shall provide licensing, configuration, integration, training and support for the Palantir platform to enhance operational efficiency, compliance, and mission execution.

2.0 OBJECTIVES

The objective of the Unified API project is to make IRS data easily accessible to any app by providing a semantic layer that standardizes data across the enterprise, enabling seamless access and collaboration, exposing curated, contextualized data through OpenAPI-compliant interfaces, and accelerating integration with modern applications and services.

As the IRS' mission expands as a result of legislative mandates, taxpayer expectations, and oversight requirements, IRS data systems have become increasingly complex and siloed; this creates an opportunity to modernize data access, enhance secure information sharing across business operations, and accelerate compliance capabilities.

Recognizing the opportunity to enhance interoperability and data driven operations, the IRS is pursuing the implementation of a Unified API framework supported by an authoritative enterprise data architecture. This approach will allow IRS to integrate multiple IRS systems to provide an enterprise data model for IRS and will become the data foundation for modeling key tax administration entities. This solution will enable cross -system interoperability and shared understanding across the enterprise.

3.0 SCOPE OF WORK

The contractor shall deliver end-to-end support for the implementation, integration, and operational sustainment of a Palantir Foundry-based Unified API platform for the IRS led initiatives. This platform will standardize and expose IRS data through a semantic layer that ensures interoperability, traceability, and secure access across the enterprise. The solution must enable both pro-code and low-code development workflows, support cross-platform data availability, and accelerate integration with modern IRS applications and services.

Scope includes:

- Designing and deploying a secure, scalable data integration environment within Palantir Foundry.
- Developing and operationalizing semantic ontologies to support consistent enterprise-wide data definitions.
- Integrating diverse legacy and modern data sources, including structured and unstructured datasets.
- Exposing curated, contextualized datasets via OpenAPI-compliant interfaces with fine-grained access control.
- Enabling federated access and lineage-aware analytics for mission-critical use cases.
- Supporting user onboarding and training, including knowledge transfer for IRS platform builders and analysts.
- Ensuring compliance with IRS governance, cybersecurity frameworks, and cloud-readiness requirements.
- Designing, developing, and operationalizing a secure, ontology-enabled data platform.
- Integrating, mapping, and hydrating data across IRS mission domains.
- Create a robust testing strategy covering both unit, system integration and performance testing,
- Ensure all performance metrics are meat and requirements are delivered as per agreed up on SLA’s.
- Provide support for automated ingestion pipelines, build APIs, and enable legacy app migration.
- Implementing scalable production environments and performance monitoring tools.
- Provide guidance and work on building an end-to-end reference architecture and Path to Prod (Dev/Test/Prod) systems implementation covering all aspects of systems design and best practices with a robust CI/CD pipeline.

4.0 REQUIREMENTS:

- The contractor shall provide support for data mapping and hydration exercises
- The contractor shall provide support for object creation and object linkages
- The contractor shall provide support for synthetic data creation
- The contractor shall provide support for automation of the data pipelines for timely and accurate data availability

- The contractor shall create a shared development environment for Palantir and IRS developers to work on the scripts and other development works. All artifacts should be version controlled.
- The contractor shall report on project status and estimated completion dates for data mapping, hydration, object creation and function creations and associated API specs
- The contractor shall provide support for validating and ensuring the quality and accuracy of the data
- The contractor shall provide authority and access to use all functions and controls for comprehensive platform management
- The contractor shall provide function development and API specification documentation
- The contactor shall provide support to achieve and maintain the ATO and other policy requirements like Cyber, SSO, NTIN, OneSDLC etc.
- The contractor shall implement platform-level security controls, including role-based access, encryption, data masking, and audit logging, in accordance with FISMA High and IRS-specific data protection requirements.
- The contractor shall provide support for Performance and to size and build the production environment capable of meeting the required SLAs and expected year over year growth
- The contractor shall automate and provide a production monitoring dashboard including alerts
- The contractor shall provide resource training on the platform
- The contractor shall provide resource mentoring on the platform
- The contractor shall provide the software licenses and engineering resources necessary to fully deploy a Unified API and EDP Core Functionality Platform.
- The contractor shall support replicating legacy command codes by delivering functionally equivalent production-grade APIs via the Unified API platform. These APIs shall replicate the behavior, access patterns, and outputs of specific command codes used in IRS legacy systems. The contractor shall support the delivery of prioritized business focused verticals and horizontal foundational areas outcomes by curating, modeling, and exposing relevant data through Unified API (UAPI) endpoints within Palantir.
- The contractor shall provide maintenance support of published API endpoints.
- The contractor shall support the sustainment of quick wins APIs delivered in the original POPs including issue resolution but excluding additional development like new data elements or new endpoints
- The contractor shall provide the necessary environments and enablement/builder support for IRS UAPI with training and office hours as mutually agreed upon
- The Contractor shall establish and maintain functioning bi-directional connections to IRS Palantir Platform to perform Compliance Hub data pipelines, to include but not limited to: Development, Test, Pre-Production, and Production.
- The Contractor shall support Back-End operational needs of the Compliance Hub including, but not limited to:
    - RRP GP retirement
    - RRP Legacy retirement

- RRPLC Legacy retirement
- IRS Palantir Platform
- Future Compliance Hub initiatives (as directed)

5.0 PERFORMANCE TASKS

5.1 Platform Implementation/Platform Development

- Design, develop, and maintain secure, scalable, OpenAPI-compliant RESTful APIs that replicate and modernize legacy IRS command code behavior.
- Ensure APIs are semantically aligned with the IRS ontology and provide secure, role-based access in support of real-time or near-real-time operations.
- Establish robust API lifecycle processes including versioning, monitoring, documentation, and deprecation strategies.
- Integrate APIs with IRS cloud-native platforms and developer ecosystems, ensuring alignment with IRS SDK and Palantir interface standards.
- Support seamless integration of APIs into modern IRS user tools and workflows, enabling the decommissioning of legacy interfaces.
- Develop tooling, stubs, and test harnesses to facilitate unit testing, CI/CD deployment, and automated validation of API behavior.
- Collaborate with IRS stakeholders to enable smooth transition from legacy command codes to API-based interfaces, including training and user support.
- Ensure APIs comply with IRS cybersecurity, audit logging, and data access control frameworks.
- Work closely with data platform teams to expose APIs that interface with structured and unstructured data, supporting both transactional and analytical use cases.
- Support operational reliability through API observability, metrics instrumentation, and incident response readiness.
- All code within foundry is able to be integrated with IRS Enterprise Git Repository

5.2 Platform Deployment & Configuration

- Configure the platform for ontology-based data modeling, ingestion, transformation, lineage, and visualization.
- Deploy a scalable infrastructure supporting federated access and real-time analytics.

5.3 Data Onboarding & Integration

- Onboard high-value IRS data sources using secure pipelines with metadata capture and quality validation.
- Integrate data from legacy systems, cloud environments, and structured/unstructured sources using near-real-time and batch processing.
- Deploy an enterprise-wide dynamic data model integrated with the IRS Enterprise Data Platform (EDP) and other authoritative sources.
- Ensure secure network connectivity for ongoing operations.
- Set up virtual access to source data tables in EDP while enforcing access controls for sensitive records.

5.4 Ontology & Semantic Modeling

- Implement ontology-based data modeling to support reusable concepts, business alignment, and federated discovery.
- Map IRS data to approved ontologies and maintain version-controlled mapping documentation.
- Migrate and modernize legacy applications to leverage Palantir semantic capabilities.

5.5 Unified API Enablement

- Expose semantically aligned data through a Unified API that supports OpenAPI specifications.
- Ensure APIs include role-based access controls, auditing, and cybersecurity compliance per NIST 800-53 and IRS policy.

5.6 Business Consumer Outcome Delivery

- The Contractor team will sustain endpoints delivered for TP360 and Zero Paper efforts and will support IRS business use cases through command code deprecation efforts.

5.7 Security, Governance & Compliance

- Implement robust platform-level controls: role-based access, encryption, masking, logging.
- Integrate data governance workflows including stewardship, approvals, lineage tracking, and metadata cataloging.
- Enforce platform-level security including RBAC, encryption, masking, and audit logging.
- Support compliance with FISMA High, ATO, NTIN, SSO, and OneSDLC requirements.
- Provide documentation and evidence to support ongoing security authorization
- Ensuring all APIs are integrated with access controls, audit logging, and aligned with IRS cybersecurity and governance standards.

5.8 Platform Support & Training

- Provide ongoing platform administration and Tier 1–3 support to IRS data stewards and users.
- Conduct onboarding, technical training sessions, and deliver user documentation and operational playbooks.
- Provide training, documentation, and mentorship to IRS data engineers and analysts.
- Facilitate onboarding and best practice workshops for users across technical levels.
- Develop training materials and conduct training sessions for end-users.
- Provide helpdesk and technical support services, including troubleshooting and system updates.
- Offer ongoing platform updates and enhancements based on operational needs of IRS and Treasury users.

5.9 Automation and Monitoring

- Automate data pipelines with quality validation gates.
- Implement production monitoring dashboards with alerting mechanisms.
- Perform system sizing and scalability analysis to support growth expectations.

5.10 Development Environment and Tools

- Establish a shared, version-controlled development workspace for IRS and contractor teams.
- Support collaborative script development and object configuration lifecycle.
- Maintain traceability of changes and ensure reusable object management.
- Expose supporting Ontology, function and API documentation to external partners via Github and/or other technical solutions.
- Integrate with IRS data catalog tools such as informatica enterprise data catalog EDC or Databricks unity catalog

5.11 Maintenance and Support

- Provide licenses, development support, and help desk services.
- Ensure full lifecycle maintenance to avoid system downtime.
- Deliver ongoing updates aligned with LCA project requirements and technical evolution.
- Support the incident management process while adhering to all SLAs associated with each priority of ticket Support the production P1-P4 incidents through the standard IRS
- Support problem investigation and diagnosis, analysis and trending of problems including root cause analysis, and resolve problems in accordance with IRM 2.14.2 Enterprise Problem Management Standards
- Respond to any P1/P2 incidents according to SLAs; participate in IM Assessment calls and support IRS personnel to resolve P1/P2 incidents

6.0 DELIVERABLES

The contractor shall be responsible for, and its performance will be measured by, the timeliness and quality of the deliverables set forth below.

6.1 Task Order Kickoff Meeting

Within five (5) business days of task order award, the contractor shall meet with Government representatives at a mutually agreed upon location or via teleconference. The intent of this meeting is to initiate the communication process between the IRS and the contractor by introducing key task order participants, explaining their roles, reviewing communication ground rules, and assuring a common understanding of task order requirements and objectives.

The completion of this briefing shall result in the following:

- The contractor and Government personnel who will perform work under this task order will be introduced.
- The IRS may show the applicable facilities to the contractor, if work will be performed on at an IRS site.
- The Government may provide any GFP to the contractor at this time.
- Any issues concerning the contractor employee security clearances will be discussed.

- The contractor shall demonstrate confirmation of their understanding of the work to be accomplished under this Statement of Work.
- The contractor shall provide the accounting period end dates to be used for the term of this task order.
- The contractor shall provide meeting notes (inclusive of any follow-up actions) to the Government within five (5) business days after the meeting.

6.2 Schedule of Deliverables

The contractor shall provide the deliverables as described in Table 1 below during the performance of this Task Order. All contractor deliverables or work products shall remain categorized as "Official Use Only." The release of any portion must be authorized in writing by the Government. The deliverables and work products shall be provided in electronic format and shall comply with all applicable standards of Section 508 of the Rehabilitation Act.

The final format and content requirements, if not stated in the Performance Work Statement (PWS), may be mutually developed and agreed upon among the IRS Program Manager (PM), the contractor and the contracting officer's representative (COR).

Table 1: Schedule of Deliverables

Schedule of Deliverables	
Deliverable	**Due Date/Frequency**
Kickoff Meeting (Virtual)	Within 5 days after Award
Test Management, Security Tooling, Monitoring and Platform Orchestration Configuring Reports	Within 30 days of award/monthly Updates
Program Status Reports	Monthly
Operational Playbooks & Training Materials to include IRS Resource Training Sessions	Bi- Monthly
Updated Enterprise Data Model Design	Quarterly
Lessons Learned and Retrospective Report	Quarterly
API Specs & Interface Maps	Per application migration schedule
Ontology Mapping Documentation	Upon Request
Replace a minimum of 5Legacy Command Codes	Annually, with weekly updates

Deliver a minimum of 100 reusable Foundry functions of medium complexity per year to enable standardized access, transformation, and presentation of ontology-linked data for downstream business applications and analytic workflows	Annually, with weekly updates
Technical Support Services	Throughout the period of performance

7.0 PERIOD OF PERFORMANCE The period of performance for this contract shall be one base year, from 9/24/2025 – 9/23/2026.

8.0 PLACE OF PERFORMANCE

Work shall be performed at the government's designated locations and/or remotely as needed. Specific deployment locations will be determined upon contract award.

8.1 PLACE OF PERFORMANCE/ACCESS TO GOVERNMENT FACILITIES

The Contractor shall generally work remotely. Onsite presence at IRS locations will occur only at the explicit request of the IRS, such as to support improved delivery through direct collaboration. The nature of this work may require effort outside the normal workday to minimize the impact of application changes upon the user community. Contract employees shall be provided with secure remote access to the IRS network via whatever technology is approved for that purpose (currently Enterprise Remote Access Project (ERAP)). These employees will also be granted occasional, "as-needed" access to an IRS facility near their location to obtain services only available in IRS offices (e.g., computer hardware repair or replacement).

- ☒ **(Provide 10%) Government's site:** The primary site of performance is the New Carrollton Federal Building 5000 Ellis Road, Lanham, MD and the IRS main facility at 1111 Constitution Avenue, Washington, DC.
- ☒ **(Provide 90%) Contractor's site**, with reasonable access to government site (Contractor personnel may be required to travel to government site for meetings within 24 (24) hours' notice and at reasonable travel costs.)

The Contractor is allowed limited access to the IRS Government facilities, as specified below:

1.) IRS New Carrollton Office (NCFB)
5000 Ellin Road, Lanham MD 20706

2.) IRS Main Building
1111 Constitution Avenue, NW, Washington DC 20224

9.0 GOVERNMENT FURNISHED EQUIPMENT (GFE) & INFORMATION (GFI)

The government will provide access to necessary systems, data, and IT infrastructure to include but not limited to a government issued IRS (non-CI) Laptop and PIV Card.

10.0 PERFORMANCE METRICS

Metric	Measurement Criteria
Platform environment stood up and operational	Within 30 days of award
Number of data sources onboarded as VT, if made available with HPTIN filters applied	≥ 10 per quarter
Data hydration for legacy systems	90% of identified sources
Data quality score (completeness, accuracy)	≥ 95% on validation tests
Timeliness of data ingestion pipelines	≥ 98% SLA compliance
Time to update ontology for new data domain	≤ 15 business days
Semantic alignment of new datasets	≥ 90% accuracy vs. baseline ontology
Number of APIs delivered	≥ 200 per year
API uptime/availability	≥ 99.9%
Average response time for APIs	≤ 300 MS
Number of IRS users trained	≥ 100 per year
Time to deploy platform updates/patches	≤ 7 business days post-release
Support Response Times • Severity 1 (Critical outage):	1 hour; resolution within 4–8 hours
Support Response Times • Severity 2 (Degraded performance):	4 hours; resolution within 1 business day
Support Response Times • Severity 3 (Minor issue):	1 business day; resolution in 3–5 days
Percent on-time incident ticket resolution	90% on-time

11.0 ACCEPTANCE CRITERIA

The government will review all deliverables for compliance with contract requirements. Acceptance will be based on successful implementation, performance against agreed metrics, and end-user satisfaction.

11.1 Inspection

Inspection will be at the same place as performance and delivery, unless otherwise specified. Submission of all deliverables should be sent to the COR.

11.2 General Acceptance Criteria

The general quality measures as set forth below will be applied to each work product received from the Contractor under this task order.

- Accuracy - work products shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity - work products shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand and relevant to the supporting narrative.
- Specifications Validity - All work products shall satisfy the requirements of the Government as specified herein.
- Format - work products shall be submitted in hard copy (where applicable) and in media defined in the PWS. The work product format is defined in this PWS. Hard copy formats shall follow Department of the Treasury and IRS Directives and shall be consistent with other similar efforts. All text and diagrammatic files shall be editable by the Government.

Timeliness - work products shall be submitted on or before the due date specified in this task order, or submitted IAW a later, scheduled date determined by the CO.

12.0 SURVEILLANCE

The surveillance process will be included in the Quality Assurance Surveillance Plan (QASP). The Contractor shall establish and maintain a complete Quality Control Plan (QCP) IAW the QASP. This links the Government and Contractor's quality assurance efforts into an integrated package with shared objectives.

Contractor shall deliver a QCP briefing during the orientation briefing to explain how quality of Contractor is implemented in addition to delivering a written QCP to the COR within 14 (fourteen) business days after award.

13.0 SECURITY

All contractor staff proposed for work under this task order must undergo successful background investigations that corresponds with tasks performed. The TSO Organization will partner with and rely on the IRS Cyber-Security Office to provide guidance and ensure compliance with all IRS security requirements and considerations including contractor access to IRS systems, data and secure facilities.

13.1 Personnel Security

All contactor personnel will undergo the appropriate background investigation commensurate with their roles and responsibilities supporting this task order.

13.2 Physical Security

The contractor shall:

a) Comply with all pertinent facility regulations and procedures for Federal agencies, unless the Government grants a waiver,

b) Make recommendations for improving protection for contractor staff if there is a security issue,

c) Promptly report unlawful acts committed on or against property under the charge and control of their contract. All such reports should be submitted through the COR to Treasury's Chief Information Security Officer or designee, and
d) Provide planning and training to contractor and sub-contractor personnel on matters relating to protection and emergency response if funded by the Government.

13.3 Desktop Security

The contractor shall screen all electronic deliverables or electronically provided information for malicious code using Treasury approved anti-virus software prior to delivery to the government. The contractor shall utilize appropriate controls (firewalls, password protection, encryption, digital certificates, etc.) at all times to protect contract related information processed, stored or transmitted on the contractor's and government's computers/servers to ensure confidentiality, integrity, availability, authentication and non-repudiation. This includes ensuring that provisions are in place that will safeguard all aspects of information operations pertaining to this contract in compliance with all applicable PWS references.

The contractor shall be responsible for policy, practice, and compliance by its personnel, subcontractors, and representatives regarding the storage and removal of electronic and printed materials considered sensitive in nature (i.e., system password and user identification access codes) from printers, desktops, laptops, furniture, presentation equipment, and any other form of information housing. This is so that the information is not accessible by unauthorized personnel and so that disposal follows Treasury information security practices. The contractor must ensure that contractor, sub-contractor, or business partner personnel protect all sensitive and secure documents to the extent possible from either inadvertent or deliberate compromise.

13.4 Solution Information/Data/Content Security and Protection

The contractor shall support the compliance and promotion of policy, guidance, and practices for the protection of those cyber systems, databases, and/or web sites to ensure system content, data, and information repositories developed and maintained. This protection shall include inadvertent events/acts, overt internal and external acts, system failure, cyber-attacks, or acts of nature.

14.0 POINTS OF CONTACT

(b)(6)

Contracting Officer: Rayshiena Shelly - Contract Specialist

(b)(6)

The following Section 508 Procurement Clauses are included in the task order:

IR1052.239.9002 Section 508 Services

For Development or Customization: All contracts, solicitations, purchase orders, delivery orders and interagency agreements that contain a requirement of services which will result in the delivery of a new or updated information and communication technology (ICT) item/product must conform to the applicable provisions of the appropriate technical standards in 36 CFR, Appendix C to Part 1194, and functional performance criteria in 36 CFR Chapter 3, unless an agency exception to this requirement exists at E202 General Exceptions.

IR1052.239-9001 Section 508 Conformance

When Less than Fully Conforming: Each information and communication technology (ICT) product and/or product related service delivered under the terms of this contract, at a minimum, shall conform to the applicable accessibility standards at 36 CFR, Appendix C to Part 1194 at the level of conformance as specified in the Attachment entitled (Please state where attachment may be found and name of attachment for example, Section J., Voluntary Product Accessibility Template (VPAT) or Section J., Evaluation Matrix).

IR1052.239-9003 Section 508 Accessibility of Information and Communication Technology (100% Compliance)

When Fully Conforming: Each information and communication technology (ICT) product or service furnished under this contract shall comply with the Information and Communication Technology Accessibility Standards (36 CFR, Appendix C to Part 1194). If the Contracting Officer determines any furnished products or services are not in compliance with the contract, the Contracting Officer will apply the remedies described under FAR 52.246-2, Inspection of Supplies – Fixed Price or FAR 52.246-4, Inspection of Services – Fixed Price.

The following technical standards have been determined to be applicable to this contract (Reference - ICT Accessibility 508 Standards):

Chapter 5: Software
502 Interoperability with Assistive Technology

- 502.1 General
- 502.2 Documented Accessibility Features
- 502.2.1 User Control of Accessibility Features
- 502.2.2 No Disruption of Accessibility Features

502.3 Accessibility Services

- 502.3.1 Object Information
- 502.3.2 Modification of Object Information
- 502.3.3 Row, Column, and Headers
- 502.3.4 Values
- 502.3.5 Modification of Values
- 502.3.6 Label Relationships
- 502.3.7 Hierarchical Relationships
- 502.3.8 Text

- 502.3.9 Modification of Text
- 502.3.10 List of Actions
- 502.3.11 Actions on Objects
- 502.3.12 Focus Cursor
- 502.3.13 Modification of Focus Cursor
- 502.3.14 Event Notification
- 502.4 Platform Accessibility Features

503 Applications

- 503.1 General
- 503.2 User Preferences
- 503.3 Alternative User Interfaces
- 503.4 User Controls for Captions and Audio Description
- 503.4.1 Caption Controls
- 503.4.2 Audio Description Controls

504 Authoring Tools

- 504.1 General
- 504.2 Content Creation or Editing
- 504.2.1 Preservation of Information Provided for Accessibility in Format Conversion
- 504.2.2 PDF Export
- 504.3 Prompts
- 504.4 Templates

Chapter 7: Referenced Standards
702.10.1 WCAG 2.0

- 1.1.1 Non-text Content
- 1.2.1 Audio-only and Video-only (Pre-recorded)
- 1.2.2 Captions (Pre-recorded)
- 1.2.3 Audio Description or Media Alternative (Pre-recorded)

- 1.2.4 Captions (Live)
- 1.2.5 Audio Description (Pre-recorded)
- 1.3.1 Info and Relationships
- 1.3.2 Meaningful Sequence
- 1.3.3 Sensory Characteristics
- 1.4.1 Use of Color
- 1.4.2 Audio Control
- 1.4.3 Contrast (Minimum)
- 1.4.4 Resize Text
- 1.4.5 Images of Text
- 2.1.1 Keyboard
- 2.1.2 No Keyboard Trap
- 2.2.1 Timing Adjustable
- 2.2.2 Pause, Stop, Hide
- 2.3.1 Three Flashes or Below
- 2.4.1 Bypass Blocks
- 2.4.2 Page Titled
- 2.4.3 Focus Order
- 2.4.4 Link Purpose (in Context)
- 2.4.5 Multiple Ways
- 2.4.6 Headings and Labels
- 2.4.7 Focus Visible
- 3.1.1 Language of Page
- 3.1.2 Language of Parts
- 3.2.1 On Focus
- 3.2.2 On Input
- 3.2.3 Consistent Navigation
- 3.2.4 Consistent Identification
- 3.3.1 Error Identification
- 3.3.2 Labels or Instructions
- 3.3.3 Error Suggestion

- 3.3.4 Error Prevention (Legal, Financial, Data)
- 4.1.1 Parsing
- 4.1.2 Name, Role, Value

The standards do not require the installation of specific accessibility-related software or the attachment of an assistive technology device, but merely require that the ICT be compatible with such software and devices so that it can be made accessible if so required by the agency in the future.

Chapter 3: Functional Performance Criteria

The following functional performance criteria (36 CFR Chapter 3) apply to this contract.

- 302.1 Without Vision
- 302.2 With Limited Vision
- 302.3 Without Perception of Color
- 302.4 Without Hearing
- 302.5 Without Limited Hearing
- 302.6 Without Speech
- 302.7 With Limited Manipulation
- 302.8 With Limited Reach and Strength
- 302.9 With Limited Language, Cognitive, and Learning Abilities

IR1052.239-9000 Section 508 Information, Documentation and Support

In accordance with 36 CFR, Appendix C to Part 1194, the information and communication technology (ICT) products and product support services documentation furnished in performance of this contract shall be provided at no

additional cost. The contractor shall provide information, documentation, and support relative to the supplies and services as described in the statement of work, performance work statement or statement of objectives (select one). The following technical standards and provisions have been determined to be applicable to this contract:

Chapter 6: Support Documentation and Services
Support Documentation

- 602.2 Accessibility and Compatibility Features
- 602.3 Electronic Support Documentation
- 602.4 Alternate Formats for Non-Electronic Support Documentation

Support Services

- 603.2 Information on Accessibility and Compatibility Features
- 603.3 Accommodation of Communication Needs

IRAP Website

Information Resources Accessibility Program (IRAP) | IRS §508 Program Office

For assistance with incorporating Section 508 standards in the procurement cycle, contact *508 Requisition Review (508.requisition.review@irs.gov).

ORDER FOR SUPPLIES OR SERVICES

2026 05526 9000082641 UNCLASSIFIED 5/28/2026

PAGE 1 OF PAGES 19

IMPORTANT: Mark all packages and papers with contract and/or order numbers.

1. DATE OF ORDER: 09/24/2025	2. CONTRACT NO. *(If any)*: 2023H2-25-A-00002
3. ORDER NO.: 205AE9-25-F-00203	4. REQUISITION/REFERENCE NO.: 5000218802

5. ISSUING OFFICE *(Address correspondence to)*:
Office of Procurement Operations-Application Development Branch
51 Haddonfield Road
Cherry Hill, NJ 08002
Attn: Rayshiena Shelly
Tel: Email: (b)(6)

7. TO:

a. NAME OF CONTRACTOR: PALANTIR TECHNOLOGIES INC.

b. COMPANY NAME:

c. STREET ADDRESS: 1200 17th Street, Floor 15

d. CITY	e. STATE	f. ZIP CODE
Denver	CO	80202

6. SHIP TO:

a. NAME OF CONSIGNEE: See Attached Delivery Schedule

b. STREET ADDRESS:

c. CITY	d. STATE	e. ZIP CODE

f. SHIP VIA:

8. TYPE OF ORDER

☐ a. PURCHASE
REFERENCE YOUR:
Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.

☐ b. DELIVERY -- Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.

9. ACCOUNTING AND APPROPRIATION DATA: See Attached Schedule(s)

10. REQUISITIONING OFFICE:

11. BUSINESS CLASSIFICATION (*Check appropriate box(es)*)
☐ a. SMALL ☐ b. OTHER THAN SMALL ☐ c. DISADVANTAGED ☐ d. WOMEN-OWNED ☐ e. HUBZone
☐ f. SERVICE-DISABLED VETERAN-OWNED ☐ g. WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOSB PROGRAM ☐ h. EDWOSB

12. F.O.B. POINT:

13. PLACE OF a. INSPECTION	13. PLACE OF b. ACCEPTANCE	14. GOVERNMENT B/L NO.	15. DELIVER TO F.O.B. POINT ON OR BEFORE *(Date)*	16. DISCOUNT TERMS

17. SCHEDULE ***(See reverse for Rejections)***

ITEM NO (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	See Attached Schedule(s)					

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.		17(h) TOT. *(Cont. pages)*

SEE BILLING INSTRUCTIONS ON REVERSE

21. MAIL INVOICE TO:
a. NAME: Invoices must be submitted via IPP
b. STREET ADDRESS *(or P.O. Box)*:
c. CITY | d. STATE | e. ZIP CODE

$13,325,955.30 — 17(i) GRAND TOTAL

22. UNITED STATES OF AMERICA BY *(Signature)*: Rayshiena N. Shelly
Digitally signed by Rayshiena N. Shelly
Date: 2025.09.24 09:13:40 -04'00'

23. NAME *(Typed)*: Rayshiena N. Shelly
TITLE: CONTRACTING/ORDERING OFFICER

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION NOT USABLE

OPTIONAL FORM 347 (REV. 2/2012)
Prescribed by GSA/FAR 48 CFR 53.213(f)

SECTION B

Line Item Table

Item No.	FSC	Item Description	QTY	Unit	Unit Price	Total Value
0001	DE01	Compliance Hub Software 09/24/2025-09/23/2026	(b)(4)			

Accounting and Appropriation Data

ACCT. Line No.	Accounting and Appropriation Data	Amount
0001-0001	(b)(4)	

Delivery Schedule

Delivery Address	Item No.	QTY	Delivery Date
	0001	(b)(4)	09/23/2026

52.217-8 Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 60 days.

(End of clause)

Compliance Hub Performance Work Statement (PWS)

Internal Revenue Service (IRS), Compliance Tech: Case Selection Vertical – Compliance Hub Task Order
Base Period: September 24, 2025 – September 23, 2026

---

1. INTRODUCTION AND BACKGROUND

The IRS requires a contract to operate and enhance the Compliance Hub, a cloud-based system providing workload identification, case selection, and examiner assistance capabilities. The system must align with IRS business, network, technical, and security requirements, supporting mission-critical filing season operations.

Compliance Hub is the cornerstone of the IRS modernization effort, consolidating fragmented case selection systems into a single platform for data ingestion, noncompliance detection, research, and workflow integration.

1.1 PURPOSE

This Task Order (TO) will deliver operational and technical capabilities necessary to modernize and consolidate IRS case selection. Compliance Hub provides IRS personnel with integrated workflows, AI-driven case identification, and secure data management aligned with IRS mission needs.

1.2 AGENCY MISSION

The mission of the IRS is to provide America’s taxpayers top-quality service by helping them understand and meet their tax responsibilities and to enforce the law with integrity and fairness. This TO supports that mission by:

- Consolidating disparate case selection systems into a unified Compliance Hub.
- Providing secure, auditable, and explainable AI-driven detection of taxpayer noncompliance.
- Enhancing examiner efficiency by delivering intuitive case management workflows.
- Ensuring audit-ready oversight for GAO, TIGTA, Treasury, and Congress.
