2. SCOPE

The Contractor shall provide licenses, software, services, and consulting resources to operate Compliance Hub for up to 1,000 IRS users across Development, Test, Pre-Production, and Production environments. Scope includes:

- Automated ingestion of tax returns, information returns, income documents, and third-party data.
- Deployment and maintenance of legacy and new models/rules within Compliance Hub.
- Delivery of case selection GUIs and examiner-facing assistants.
- Bi-directional integration with IRS Case Management, AMS, ECM, and other legacy systems, as needed to support a specific workflow that is not part of the shared EDP data assets/UAPI.
- Support for training, disaster recovery, surge requirements, and legislative updates.
- Provide IRS with full ownership of data and configuration artifacts, including open-format exports.

---

3. CURRENT INFORMATION TECHNOLOGY (IT)/NETWORK ENVIRONMENT

Compliance Hub must operate within IRS's enterprise architecture and security requirements. The current environment includes:

- **Platforms**: Palantir Foundry suite, Agentic AI (AIP Agent Studio), Databricks, AWS GovCloud, IRS-hosted infrastructure.
- **Environments**: Development (synthetic data), Test (functional and integration with masked datasets), Pre-Production (release readiness, mirrors Production), Production (live IRS data, FIPS-199 High compliant).
- **Standards**: FIPS-199 High, FedRAMP High, NIST RMF, NIST SP 800-137 (continuous monitoring).
- **Integrations**: IRS Case Management, AMS, ECM, PUMAS, BEARS, ESAT, and legacy systems.
- **Challenges**: Fragmented legacy systems (RRP, EFDS), manual workflows, redundant case selection logic.

---

4. OBJECTIVES

The Contractor shall provide production-ready Compliance Hub capabilities. Objectives include:

- Deploy and maintain 10 new compliance case selection methods annually and AI-based assistants for AUR, Correspondence Exam, and RICS.
- Deploy and maintain legacy and new models, rules, and filters.
- Deliver functional GUI for case selection and fraud detection workflows.
- Establish audit logging, drift detection reviews (every 90 days), and Zero Trust enforcement with annual validation.
- Provide IRS with full ownership of data and artifacts in open formats.
- Obtain accreditation under FedRAMP High.
- Document IRS end-user sign-off for production readiness.

Exit Criteria: A capability is production-ready when testing is completed across functional, integration, performance, and security domains; accreditation is obtained under NIST RMF FedRAMP High; and IRS end-user sign-off is documented.

---

5. TASKS

5.1 Task 1 – General Framework, Support, and Operational Capability

Provide licenses, services, and consulting resources for up to 1,000 IRS users. Maintain logical separation between Development, Test, Pre-Production, and Production environments. Provisioning SLAs: onboarding within 3 business days, offboarding within 24 hours. Maintain searchable data dictionary updated within 14 days of schema changes as inherited by IRS IdP.

5.1.1 Data Integration and Research Requirements

The Contractor shall:

- Provide automated and manual research capabilities with intuitive interfaces for IRS analysts.
- Support ad-hoc queries and data visualization across structured and unstructured data.
- Maintain detailed data dictionaries mapping tax forms, line items, and database fields.
- Enable audit logging of sensitive queries (e.g., NTIN/HPTIN checks) with redaction and monitoring.
- Support data lineage, governance, and traceability, ensuring availability for current year + 4 prior years.

Desired Outcomes:

- IRS analysts can seamlessly access, analyze, and visualize data.
- Audit logs provide complete accountability for sensitive queries.
- Data lineage and dictionary provide clarity and compliance for research and reporting.

5.2 Task 2 – Deployment of Case Selection Methods

1. Develop and deploy up to 10, out of the 10 total allotted workflow slots, AI or rule-based orchestration workload identification methods. Methods must run at operational cadence, feed downstream systems via secure APIs, and include test data, plans, and performance criteria. Additionally, the Contractor shall provide an environment to support the re-architecture of RRPLC fraud detection use cases, leveraging data from the Enterprise Data Platform (EDP) shared data asset. Palantir shall be responsible only for hosting this environment and providing support for its operation. Workflow, data integration, ontology, etc. configurations maintenance and sustainment (including user identified issues, user trainings, or issues with upstream data tables) for RRPLC will be delivered by the IRS or other designated service providers within the Platform. Access to these workflows will be granted to approved IRS personnel and designated service providers, which includes but is not limited to:

    - Hosted environment for delivery of RRPLC use cases.
    - Weekly office hours to support IRS RRPLC builders.
    - Required RRPLC data made available through the shared EDP data asset.

2. **Desired Outcomes**

    - Selected case identification methods deployed and delivering usable outputs.
    - RRPLC fraud detection use cases fully re-architected and supported through EDP.
    - Seamless delivery of outputs into downstream IRS systems.

5.3 Task 3 – Deployment of AI-Based Assistants

Develop and deploy up to 5, out of the 10 total allotted workflow slots, AI-enabled assistants for an IRS determined problem space. Ensure assistants replicate or improve IRS logic, integrate with downstream systems, and preserve decision authority.

Desired Outcomes:

- IRS examiners are supported by AI assistants replicating business logic.
- Treatment recommendations delivered seamlessly to IRS case systems.
- Workload efficiency improved without loss of examiner oversight.

5.4 Task 4 – Training

Deliver structured training: in-person sessions, Lunch-and-Learns, training videos, and train-the-trainer programs. Provide quarterly updates to training materials reflecting system changes. All training materials remain IRS-owned.

Desired Outcomes:

- IRS staff receive consistent, updated training across all delivery formats.
- IRS SMEs equipped to deliver ongoing training via train-the-trainer approach.
- IRS retains full ownership of training materials for future reuse.

5.5 Task 5 – SaaS Managed Service

Operate Compliance Hub as SaaS with disaster recovery SLAs: RTO ≤ 12 hours during filing season. Conduct annual DR exercises, provide on-call and available to proactively receive, respond to, and remediate priority 1 and 2 (i.e., P1 and P2) incidents and issues on a 24/7/365 basis, incident response, monitoring, and observability. Notify upgrades at least 30 days in advance.

Desired Outcomes:

- Compliance Hub operates continuously with minimal downtime.
- Disaster recovery tested annually with validated results.
- IRS staff receive timely support for incidents and service issues.

5.6 Task 6 – Program Management & Integration

The Contractor shall support 6 Assisted Builds Projects, built, maintained, and sustained (including user identified issues, user trainings, or issues with upstream data tables) by IRS personnel (or another 3rd party contractor IRS identifies)– supporting collaborative development between IRS personnel (including Compliance, RAAS, and IT Data Scientists) and Palantir technical experts. Under this licensing model:

- Assisted builder projects are inclusive of application development, data integration, ontology building, and AIP tooling. This assumes AI/model development and training occurs in other platforms.
- The Contractor shall provide direct technical assistance throughout the development process, including guidance on best practices, troubleshooting, and resolving code or configuration issues. Provide additional, hands-on Palantir team support for an 8-week period including weekly scoping guidance, office hours, bootcamp support, and reviewing proposed changes to main pipelines, objects as needed. After the 8-week period, builders may continue to join the weekly Assisted Builder office hour even after the conclusion of the 8-week period for additional support, as required. The platform must enable real-time collaboration, allowing both IRS and Contractor personnel to validate code logic, dependencies, and model structure, with access to error reporting, diagnostics, and debugging tools.

5.6.1 Section 508 Assisted Testing Standards

The Contractor shall:

- Conduct assisted testing with IRS-approved tools including JAWS, ZoomText, and Dragon Naturally Speaking.
- Ensure compliance with IRS Information Resources Accessibility Program (IRAP) standards.
- Deliver accessibility certification for all user-facing interfaces.

Desired Outcomes:

- Strong program governance, risk management, and oversight of deliverables.
- Section 508 compliance validated through assisted testing.
- All Compliance Hub features accessible to IRS employees.

5.7 Task 7 – Cybersecurity Requirements

Integrate MFA with IRS PUMAS and BEARS. Enforce phishing-resistant MFA. Implement DLP controls for cloud environments. Provide SBOM attestations with each major release. Enforce audit logging standards (ESAT integration, 5-year retention). Guarantee U.S.-only data residency. Conduct annual Zero Trust validation exercises.

5.7.1 Security Operations

- Monitor, detect, and respond to threats 24/7/365.
- Maintain situational awareness across all systems, correlating security data.
- Conduct incident handling, forensic analysis, and vulnerability management.
- Implement separation of duties, patch management, and change management.

5.7.2 Continuous Monitoring

- Operate in alignment with NIST 800-137 continuous monitoring standards.
- Provide POA&Ms, vulnerability scans, and incident simulation reports.
- Support IRS Security Control Assessments (SCA) and annual tabletop exercises.

5.7.3 Security Reporting

- Provide monthly security status reports, vulnerability analyses, and incident summaries.
- Report situational awareness, risks, mitigations, and compliance metrics.
- Deliver detailed forensic and audit logs to IRS Cybersecurity.

Desired Outcomes:

- Compliance Hub consistently meets IRS and federal security standards.
- Continuous monitoring and incident response keep IRS data secure.

- IRS receives transparent, timely reporting of security posture.

5.8 Task 8 – IRS Tax Dataset Processing & Maintenance

Support ingestion, refresh, archival, and presentation of datasets. Maintain online retention of at least five years, extendable at IRS discretion. Provide IRS with on-demand ability to download entire dataset holdings. Ensure full data lineage, traceability, and integrity.

Desired Outcomes:

- IRS retains complete control and access to all tax datasets.
- Compliance Hub preserves lineage and traceability for 5+ years.
- IRS can refresh or archive data without disrupting operations.

5.9 Task 9 – Surge / Legislative Change Support

Maintain on-call SMEs for surge requirements. Respond within 72 hours to IRS notifications of legislative or emergency needs. Ensure workflows updated without disrupting filing season operations.

Desired Outcomes:

- IRS receives rapid response to legislative or emergency requirements.
- Surge support provided without filing season disruption.
- Flexibility for IRS to integrate new workflows and requirements.

5.10 Task 10 – Transition-In

Provide a Transition-In Plan within 30 days of award. Ensure minimum service disruption and no service degradation. Implement transition activities within XX calendar days of project start.

Desired Outcomes:

- Smooth transition into Compliance Hub operations.
- Zero or minimal disruption to IRS mission-critical functions.
- Transition-In Plan delivered and validated by IRS.

5.11 Task 11 – Transition-Out

Provide a Transition-Out Plan within six months of project start. Plan must facilitate seamless transition of knowledge, staffing, documentation, ongoing initiatives, and system processes. Update annually and quarterly during final option period. Maintain effective communication with incoming contractor/Government personnel.

Desired Outcomes:

- Transition-Out executed with minimal disruption.
- IRS and incoming contractor retain full continuity of knowledge.
- IRS mission protected during contract turnover.

5.12 Task 12 – Government Furnished Property, Travel, and Inspection

- **Government Furnished Property/Information**: The IRS may provide materials, equipment, or information necessary to complete tasks. Contractor must return all GFP/GFI upon request and ensure compliance with FAR Part 45.
- **Travel**: Anticipate up to three site visits to Washington D.C. IRS offices, coordinated with GTM/COR.
- **Inspection**: Deliverables will be inspected at place of performance unless otherwise specified. All products must meet IRS acceptance criteria.

Desired Outcomes:

- IRS-provided resources used efficiently and returned properly.
- Travel conducted only when approved and essential.
- Deliverables inspected and accepted with full compliance.

---

6. ACCEPTANCE CRITERIA

Deliverables must meet IRS standards for:

- Accuracy
- Clarity
- Validity
- Timeliness
- Format

---

7. SURVEILLANCE & QUALITY CONTROL

The Contractor shall deliver a Quality Control Plan (QCP) within 14 days of award, aligned with QASP. Surveillance will evaluate timeliness, accuracy, training delivery, support responsiveness, and audit compliance. Corrective actions and reporting mechanisms must be included.

---

8. SKILL REQUIREMENTS

The Contractor must demonstrate expertise in:

- Palantir systems and Agentic AI.
- Agile project delivery.
- IRS integrations and UI design.
- Databricks and AWS ecosystems.
- IRS security, Section 508, and accessibility standards.

---

9. DOCUMENTATION QUALITY

The Contractor shall provide all deliverables in compliance with IRS standards and guidelines. Deliverables must demonstrate:

- **Completeness** – sufficient detail to show understanding of requirements, environment, and design.
- **Feasibility** – valid, practical information achievable within time constraints.
- **Understandability** – clear, clean, and logically structured documentation.
- **Accuracy** – precise, technically correct, and internally consistent.
- **Practicality** – implementable guidance relevant to IRS maturity and environment.

---

10. DELIVERABLES TABLE

DEL #	Milestone/Deliverable	PWS Reference	Date of Completion/Delivery	Gov't Rights
1	Project Start (PS)	TO Award	At TOA	N/A
2	Project Kick-Off Meeting	Task 1	Within 25 workdays of TOA	N/A
3	Project Kick-Off Minutes	Task 1	NLT 3 workdays post-KO	UR
4	Monthly Status Report	Task 6	10th day of following month	UR
5	Project Management Plan	Task 6	At Kick-Off; updated annually	UR
6	Quality Control Plan (QCP)	Task 7	14 days after award	UR
7	Transition-In Plan	Task 10	30 days after award	UR
8	Transition-Out Plan	Task 11	6 months after PS; annual updates	UR
9	Quarterly Delivery Report	Task 6	Quarterly	UR
10	Disaster Recovery Exercise	Task 5	Annual	UR

DEL #	Milestone/Deliverable	PWS Reference	Date of Completion/Delivery	Gov't Rights
11	Training Delivery/Materials	Task 4	Quarterly updates	UR
12	AI Workload Deployment Reports	Task 2/3	Quarterly	UR
13	Legislative Surge Reports	Task 9	As needed (≤72 hrs)	UR
14	Security Status Reports	Task 7	Monthly	UR
15	Documentation Quality Review	Task 9	Annual	UR

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).

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS

OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER	PAGE 1 OF 29
5600226337	

2. CONTRACT NO.	3. AWARD/EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
2023H2-25-A-00002	03/27/2026	205AE9-26-F-00047	2023H2-25-A-00002	03/03/2026

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER *(No collect calls)*	8. OFFER DUE DATE/ LOCAL TIME
	Rayshiena Shelly		03/04/2026

9. ISSUED BY CODE 2050

Office of Procurement Operations-Application Development Branch
51 Haddonfield Road
Cherry Hill, NJ 08002
Attn: Rayshiena Shelly
Tel: Email: (b)(6)

10. THIS ACQUISITION IS ☒ UNRESTRICTED OR ☐ SET ASIDE: % FOR:

- ☐ SMALL BUSINESS
- ☐ HUBZONE SMALL BUSINESS
- ☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS
- ☐ WOMEN-OWNED SMALL BUSINESS (WOSB) ELIGIBLE UNDER THE WOMEN-OWNED SMALL BUSINESS PROGRAM
- ☐ EDWOSB
- ☐ 8 (A)

NAICS: 513210

SIZE STANDARD:

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED	12. DISCOUNT TERMS	13a. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)	13b. RATING / 14. METHOD OF SOLICITATION
☐ SEE SCHEDULE		☐	☐ RFQ ☐ IFB ☐ RFP

15. DELIVER TO CODE

See Attached Delivery Schedule

16. ADMINISTERED BY CODE

Office of Procurement Operations-Application Development Branch
51 Haddonfield Road
Cherry Hill, NJ 08002
Attn: Rayshiena Shelly
Tel: Email: (b)(6)

17a. CONTRACTOR/ OFFEROR CODE FACILITY CODE

PALANTIR TECHNOLOGIES INC.
1200 17TH STREET
FLOOR 15
DENVER, CO 80202-5835

TELEPHONE NO.

18a. PAYMENT WILL BE MADE BY CODE

Invoices must be submitted via the Invoice Processing Platform at www.ipp.gov

☐ 17b. CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Selection and Analytics Platform (SNAP) Period of Performance: 03/27/2026 - 06/26/2026 This order confirm the Contracting Officer's email authority to proceed dated 03/27/2026. *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA

See Attached Schedule(s)

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*

$2,250,363.27

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☒ ARE NOT ATTACHED

☐ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☒ ARE NOT ATTACHED

☒ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN 1 COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED

☐ 29. AWARD OF CONTRACT: REF. _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR

(b)(6)

31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*

Rayshiena N. Shelly Digitally signed by Rayshiena N. Shelly Date: 2026.03.31 12:20:40 -04'00'

30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)*	31c. DATE SIGNED
(b)(6)	March 31, 2026	Rayshiena N. Shelly	03/31/2026

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT

32a. QUANTITY IN COLUMN 21 HAS BEEN

RECEIVED INSPECTED ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED:

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELPHONE NUMBER OF AUTHORZED GOVERNMENT REPRESENTATIVE 32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER PARTIAL FINAL	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT COMPLETE PARTIAL FINAL	37. CHECK NUMBER

38. S/R ACCOUNT NO.	39. S/R VOUCHER NUMBER	40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

SECTION B

Line Item Table

Item No.	FSC	Item Description	QTY	Unit	Unit Price	Total Value
0001	DA01	Selection and Analytics Platform (SNAP) Period of Performance 03/27/2026 - 06/26/2026	(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)	06/26/2026

PERFORMANCE WORK STATEMENT FOR THE SUPPORT OF THE
SELECTION AND ANALYTICS PLATFORM (SNAP)
Last Revised March 2026

1. Introduction and Background

The Internal Revenue Service requires a replacement for Discoverer due to the capability being at the end of life and requests the contractor provide a solution that meets the business requirements as well as IRS network, technical, operational, and security requirements.

2. Objectives

The Contractor shall provide a solution for a Discoverer replacement that includes project management support, preparation of all technical documentation and required Enterprise Lifecycle documentation, cybersecurity management, configuration management, incidence management, disaster recovery, risk management, schedule management, preparation of reports and briefings, and representing the project at meetings, and providing analytical support, including data import, data modeling, data analysis, and user workflow support.

3. Scope of Work and Description of Task

The Oracle Discoverer in EFDS is the primary tool currently being used by RICS and CI analysts to manually identify and confirm fraud. One of its key features is to provide Business the ability to perform ad-hoc queries, supporting manual research on a copy of the EFDS database, and to identify new and emerging fraud. Oracle discontinued the Discoverer product in June 2017, and it has been operating at risk beyond end of life since then.

This Task order is to obtain a COTS solution from the Contractor to replace Discoverer based Manual Research and Fraud selections. The COTS Solution should satisfy RICS and CI analyst needs by ingesting IRS internal and external data, storing and organizing it for searching and identifying the fraud patterns. Users should be able to analyze and visualize large amounts of disparate data, both structured and unstructured, within a single, data agnostic platform.

The Contractor shall provide the full life cycle of COTS solution implementation including the helpdesk and maintenance support in a managed service operating model.

3.1. TASK 1, Discoverer Replacement Solution (SNAP)

The Contractor shall provide the software licenses and associated resources as necessary to fully deploy an advanced data exploration and analytical platform, integrate all relevant tax and non-tax data sources, train users on the platform, provide analytical and help desk support, provide IT system development lifecycle support and expertise and provide filing season support.

The Contractor shall provide SNAP support using the Foundry Operating System and Contour application commercial licensing purposed for supporting the IRS' Manual Research and Fraud Selections. Under this requirement, the Contractor shall deliver a fully managed Software as a Service (SaaS) model that integrates software licensing, system operations and

maintenance (O&M), advanced data integration, analytical consulting, help desk support, cybersecurity compliance, and lifecycle development expertise. The objective is to provide IRS business users with a modernized, secure, and scalable analytical environment capable of integrating tax and non-tax data sources into a single, data-agnostic platform.

3.1.1. Data Integration and Manual Research

The Contractor shall provide the capability to provide users with access to a wide variety of IRS tax data sources. This includes but is not limited to timely access to the following IRS Data: IMF, BMF, IRMF, referrals, STARS, WMS, CASE, EFDS Audit and Production Data, RRP Selection Data, IRDB, System Audit, System History, EUL metadata, TPDS and User Admin Data, Return Information, and P1-P3 EFDS Processing. For initial Discoverer replacement, the scope is limited to the data sets listed in the PWS. The Contractor shall provide and maintain a detailed Data Dictionary and make it available to users conducting research.

- The system shall integrate existing IRS analytic systems such as RRP. The system shall be based on open standards and support standard integration patterns. For initial Discoverer replacement, the scope is limited to RRP and EFDS integration.
- The system shall make all datasets that are available in Discoverer currently by matching current data latency or improving it with increased frequency of updates. In the case that data can't be made available as quickly as the legacy system because of source system constraints, data will be provided as soon as possible after it is received. Wherever possible, it shall use authoritative data sources to load related data. For a list of current data sets, please refer to Table 3.1.1 "Data Sets and Frequency".
- The contractor shall index all integrated data and provide a full suite of robust search capabilities.
- The Contractor shall implement fine-grained access controls according to specific data classifications and user access levels.
- The system shall provide the means to quickly view the narrative associated with any given search result. The user should be able to derive the outcome through the search result, which could be one or many columns depending on the search/query.
- The system shall provide access to all acquired source data for the current year and three prior years in an online system. There may be exception to this rule based on existing cases and specific datasets where the data may need to be kept available for longer duration

Table 3.1.1 Data Sets and Frequency

Source	Data Type	Data Format	Frequency
DDB	ID Theft Returns		Daily
NAP	Entity Data (Individual +Business)	Flat File	Daily & Weekly
MeF	Individual Return Data (As Submitted)	XML	Hourly
MeF	Individual Return Data (Rejected as Submitted)	XML	Hourly

Source	Data Type	Data Format	Frequency
IRMF	Information Returns Master File Processing (IRMF)	Flat File	Weekly
•	Balancing Information for taxpayer letters	N/A	N/A
BMF	Business Returns (Electronic + Paper + Amended)	Flat File	On Event
TPDS	Individual filers and transmitters numbers	Flat File	Weekly
ERS	QRP (Questionable Return Program)	Excel	Daily
GAP	Non-Pipeline Questionable Return (Business Unit)	AMS	Multiple times
	AM (Accounts Management) or TAS (Taxpayer Advocate Service)		
RRPLC	STARS data	Relational	New
RRPLC	CASE data	Relational	New
RRPLC	Notes	Relational	On Event
RRPLC	Disposition (process status)	CSV	On Event
RRPLC	Cluster	Relational	On Event
RRP	Analytical Result	Relational	Multiple times / day
Compliance Hub (EDP)	Analytical Result on EDP	Databrick	Multiple times / day
RRPLC	SCC (Select Characteristics Code)	Flat File	Multiple times / day
COMPASS	STARS/CASE/Notes/Disposition	Palantir	Multiple times/ day
RRP	RRP Selections Data	Relational	Daily
RRP	RRP resequencing transactions	Relational	Daily
RRP	RRP Scores & Analytical data	Relational	Daily
GMF	GMF 1609 data	Flat File	Daily
IPM	GMF 1609 data	Flat File	Weekly
TPLD	Third Party Lead	Flat File	Daily
DDB	Dependent Data (Child Support)	Flat File	Yearly
BOP	Prisoner and Prison data	Flat File	Yearly
HHS	W4 Data-QW Output records (Qualifying Widow/ Widower)	Flat File	Daily
External	There are 18 to 20 other External leads data used by RRPLC users	XML, Flat File	On Event

3.1.2. **Data Access and Analysis**

The system shall provide the capability to manually identify the anomaly detection for both pre-refund and post-refund fraud. The system should support the data and analytical needs of both civil and criminal investigative employees with a role in criminal prosecution and revenue protection by acting as the platform for analytics.

The system shall have the capability to provide users with access to all data sets ingested into the system, which includes but is not limited to tax and income documents as well as internal transactional data such as case selections and dispositions, referrals, audit tables, scheme management etc.

The system shall provide the following search (query) and analysis capabilities.

3.1.2.1. **Build and Manage Searches**

- The system shall provide the capability to build and manage complex searches, sub-searches (or running different filters in combinations to assist users narrow down the search result from different perspectives), or pre-defined searches (or equivalent capabilities) across multiple data sources/tables in a point and click interface.
- The system shall include the ability but not limited to aggregate mathematical operations/statistical analysis or functions across columns/rows, manage and configure varying level of complexity for searches, prevent users from defining invalid searches, specify multiple search parameters, or specify date ranges for data to be included in search results.
- The system shall allow Users to access any data element and data sets that they are authorized to access and in addition, system shall have the capability to prevent users from defining invalid queries by presenting relevant data only when a user is building a query.
- The system shall have the equivalent capability to query/search against a bulk list of search terms.
- The system shall have the equivalent capability to allow users to select whether newly available data should be displayed when they run an existing query/search.
- The system should display the “expected time” for any long-running queries such as data extracts, as needed.
- The system shall have the capability to display to the user when there is an error executing or scheduling a query/report.

3.1.2.2. View, Analyze, and Manage Data or Search Results

- The system shall provide the capability to allow users to view, analyze, organize, visualize, consume, manipulate or reproduce data or search results. This includes the ability to view and manage data in a tabular format, provide user friendly column names, convert data from one format to another, view a minimum of at least 200 columns at a single time, identify patterns in data, search/sort/filter on all fields, view related return data or information document data or view the query/search parameters used to generate produce data/search results, perform analysis against multiple data sets, as well as to keep and track the history of the search steps.

3.1.2.3. Import Search Parameters

- The system shall provide the capability to allow users to import search parameters. This includes importing a set of search criteria (e.g. equivalent to SQL statement of relational database) or list of search parameters.

3.1.2.4. Export Data Search Parameters or Results

- The system shall provide the capability to allow users to export search parameters, select data, search criteria, or search results with limited sensitive data for use in other applications (TIGTA Audit, Excel). This includes the ability to export records using open standard formats or tabular formats, export the original search parameters, export search results, or export results with limited sensitive information for use by other applications (which can be other downstream systems or EFDS components like ACGM). The Contractor will configure a user interface to allow analysts to associate queries with cases in EFDS. Additionally, the contractor will configure a regular export of query results associated with cases in a mutually agreed upon open standard format.

3.1.2.5. Collaborate Searches

- The system shall have the capability to allow users to share the queries/search parameters with another user that are in same group. In addition, it shall have the equivalent capability to identify users working on a similar set of returns.

3.1.2.6. Data Visualization

- The system shall have the capability to allow data to be viewed and consumed in tabular and intuitive formats such as crosstabs, graphs and charts.
- The system shall have the equivalent capability to provide the user with the ability to manipulate the layout of the data and allow users to search, sort, and filter on all fields. The system shall have the capability to allow users to view many columns at a single time.
- The system shall have the capability to allow users to view the query used to generate their data visualization.

3.1.3. *Business Intelligence and Operational Reporting*

The system shall provide the capability to execute and manage ad-hoc/predefined reports.

3.1.3.1. *Standard Reports & Dashboards*

- The system shall have the capability to allow users to develop and execute the ad-hoc reports. The system shall also have capability to manage, execute and print any of the available pre-defined reports.
- The system shall have ability for users to develop dashboards and scheduled reports to provide visibility into systematic processing, analytics and business metrics.

3.1.3.2. *Operational Reporting*

- The system shall provide accurate and repeatable data collection, tracking, and reporting analyses for Service Level Objective reporting in accordance with the QASP.
- The system shall provide visibility into underlying metrics supporting Service Level Objective reporting.
- The system shall allow IRS visibility into the collection, tracking, and reporting of system metrics.
- The system shall provide the capability to produce reports, including historical trend reports, using both online and archived operational data.
- The system shall support ongoing IRS requests for ad-hoc reporting capabilities and should expect to support 6 hours of ad-hoc reporting activities per quarter as part of ongoing O&M activities.

3.1.4. *Security – Access, Data and Audit*

- System shall integrate with the most current available ES-Single Sign On (SSO) for IRS Employee Authentication which is the future target state design pattern.
- The system shall be compliant with requirements from the IRS Privacy Government Liaison and Disclosure (PGLD) organization.
- The system shall implement automated data level security mechanisms such as Negative Taxpayer Identification Number (NTIN) checks. The system shall also have the ability to collect, save and transmit the Negative TIN check data to ESAT for auditing when user accesses any PII data
- According to IRM #10.8.6.3.8(1), A security incident response shall be followed for application. For more details of the incident response, see http://irm.web.irs.gov/Part10/Chapter8/Section1/IRM10.8.1.asp#10.8.1.4.8
- The system shall support the audit records to be retained according to TD P 80-05. For more detailed guidance, see IRM#10.8.1.4.3.10
- The system shall comply with audit logging security standards, keep an audit log of user activity, and contain an audit log for all system action and data accessed. The system shall have the ability to audit and monitor any imports/exports.
- The system shall provide the ability for an authorized user to query the audit log for all user activities (e.g., searching, querying, reporting, dashboard creation, exporting, and importing) and system activities.
- The system shall follow a security policy for the application by default to deny all permissions and access privileges. The system shall have the ability to control data access by user, user role, user organization and data context.
- The system shall protect the application resources (i.e., configuration and executable files) to allow only an application administrator to modify the configuration and files.

- The system shall not allow any unauthorized user to gain access to restricted functions.
- The system shall allow only the authorized administrator to authorize or change privileges assigned to users.
- Users will be provided with training, documentation and change management support to use applications effectively and securely.
- The system shall support encryption and masking of selective PII data in transit and at rest (database).
- The system shall have ability to monitor security testing tools and static analysis code scanning tools to test against the following classes of code vulnerabilities:
  - Security-related functions.
  - Input-output validation and encoding errors.
  - Error handling and logging vulnerabilities.
  - Insecure components or API connections.
  - Coding errors.
- The system shall implement IRS Cyber's general guidance related to Databases that includes but is not limited to:
  a. Development databases shall not co-reside with production databases.
  b. Database links shall NOT be created or used between production and development database systems.
  c. Applications and databases under development shall not access production databases.
  d. Development databases created from production databases shall be sanitized to remove sensitive data immediately after import to the development database.
  e. Proposed solution environment and network meets security accreditation requirements of FIPS-199 Moderate at time of implementation and achieve FIPS-199 High upon notification from IRS within two fiscal years from written notification by the Contracting Officer, following the intent of the base Task Order2032H5-19-F-00270.

3.1.5. *Section 508 Compliance*

- All user-facing system interfaces and user-facing web pages shall be Section 508 compliant and certified by IRS Information Resources Accessibility Program (IRAP) office. Further guidance and requirements from IRAP shall be met by the system. The link to the IRM to locate specific requirements to comply with Section 508 is: http://irm.web.irs.gov/Part2/Chapter25/Section5/IRM2.25.5.asp

3.1.6. *System Performance and Alternate Site Processing (ASP)*

- The system shall be able to scale both horizontally (scale-out) and vertically (scale- up) to accommodate the 10% yearly increase in data volume and anticipated growth of 4% of user base in every year as an optional line item.
- The system shall ingest, store and organize all the data sets that's needed to support Manual Research. For list of current data sets that are used, please refer to Table 3.1.1 "Data Size and Volumes".
- The system shall be available to the users 99.9% of the time seven days a week 6:00 AM

to 4:00 AM (next day) EST excluding scheduled down time.

- The system shall support up to 1500 total users (including 50-100 Research Analysts) and 270 concurrent users from various Business units (CI, RICS, SBSE) to access the system.
- The system shall be able to sync with multiple systems so that it has ability to load daily all current and historical data to support fraud and non-compliance detection for us in queries, reports, searches and dashboards.
- The system shall be able to process and ingest 380 million tax returns a year and 12.2 million records on a peak day in filing season.
- The system shall be able to monitor, capture and forecast statistics of usage.
- The system shall support a "Recovery Time Period" of 10 hours. The system shall support a "Recovery Point Objectives" of 2 hours.
- Current contingency planning policy and procedures shall be reviewed and update every three years.
- The system shall follow "Non-Functional Requirement (NFR)" NFR-4DR document for "Disaster Recovery" Plan.

3.1.7. *Data Governance and Ownership*

- The Contractor shall ensure IRS solely owns all of the data stored and transmitted through Discoverer replacement solution and none of the data shall be used outside IRS business processes.
- All of the IRS data shall be maintained in an industry standard such as XML without any proprietary formatting, so that data can be imported into open source tools and frameworks.
- The system shall provide capability for IRS to download all of the data that's ingested and generated in Discoverer replacement solution. This data can be in raw format and includes but is not limited to tax returns, income documents, leads, transactional data, system usage data and performance data.
- The system shall keep an archive of all acquired source data in order to maintain traceability. And system shall collect metrics to track data governance activities and compliance with policies.
- The system shall document detailed procedures for monitoring and control of O&M activities like data loads, CRs, etc.
- The system shall report any data related incidents and resolutions to the data governance board.
- The system shall retain all acquired source data for the current year and three prior years in an online system. There may be exceptions to this rule based on existing cases and specific datasets where the data may need to be kept available for longer duration.
- The system shall archive data that is not actively needed to support application processes to a secondary storage area or partition existing database tables.
- The system shall provide the capability to allow authorized users to manage data integrity, accept or discard changes, and support mapping of additional data. This includes the ability to accept or discard changes made to the data prior to it being made available or being scalable to support additional data mapping for data in the database.
- The system shall annually remove operational data that is older than the required IRS retention period from active systems and provide the downloaded data to the IRS.

3.1.8. *Security - Data Quality Management*

- The system shall provide warnings and notifications to the FedRAMP ISSO via multiple channels as defined for the system. Any material warnings or notifications will be passed on to the relevant IRS individuals via the security incident reporting process outlined below.
- The system information shall provide the capability for the SA and ISSO to change the auditing to be performed on information system components based on configurable event criteria within defined time thresholds
    - The system shall identify the Records Control Schedule (RCS) for record retaining, archiving and destroying PII.
    - The system shall periodically purge the data in all data representations/models based on data retention policy.
    - The system shall back up audit records onto a different physical system or component besides the component being audited.
    - The system shall capture all data quality related errors in a format that can be communicated to the data steward.
    - The system shall define valid values for various data elements and report inconsistencies.
    - The system shall define data quality business rules to identify anomalies.
    - The system shall not be exploited to bypass database management system access controls. The primary roles and responsibilities for IRS accessibility guidance belong to Information Resources Accessibility Program (IRAP)
    - The system shall use mechanisms that assure the integrity of all transmitted information, including labels and security parameters.
    - The system shall have the capability to mask sensitive data elements

3.1.9. *User Onboarding and Provisioning*

- The system and Contractor shall define user onboarding process and support in provisioning users with access to the application with right role and privileges.
- The system and Contractor also shall define offboarding users and removing them and their access when no longer needed or employed.
- The system shall provide the capability to specify and manage access to data or features based on defined user groups. This includes the ability but not limited to create user groups, restrict or limit access to relevant data sets based on role based permissions.
- The system shall provide user provisioning capability for MDD organization in managing the RICS and CI analysts with access to the system. This shall include the capability of creating user groups and restrict or limit access to relevant data sets based on the roles.
- The system shall either integrate with OL5081 for user groups and role based access approval workflow or provide the capability within the system and migrate the current OL5081 data into the system.

DESIRED OUTCOME:

- Palantir proposed managed service that replaces Discoverer and meets IRS technical,

operational, and security network user requirements. Proposal will include:

- Provide fully managed service, including maintenance for all components of the Discoverer replacement solution to ensure no unplanned system down-time or user interruption is experienced as reasonably possible.
- Solution will meet IRS data access, data formatting/coding, and storage requirements, as well as disaster recovery requirements.
- Proposal will address IRS ownership of all data and ability for full continued use and future access to all data
- Proposed solution environment and network meets security accreditation requirements of FIPS-199 Moderate at time of implementation and achieve FIPS-199 High within one (1) year from date of award
- Provide a solution that complies with Internal Revenue Code 6103 for protection of Taxpayer data, protecting PII, email Privacy, and meet requirements of all IRS privacy policies including Tax Information section of IRM 10.5.1 and current requirements in IRM 10.5.1.2.4.
- Proposed cloud solution must comply with security guidance for Internal Revenue Manual (IRM) 10.8.24, Information Technology (IT) Security, and Cloud Computing Security Policy.
- Provide project management, cybersecurity management, configuration management, incident management, risk management, and schedule management support
- Prepare reports and briefings, and present the project at meetings
- Milestone planning recommendations and analysis (WBS)
- Create all supporting ELC documents and User Support Documentation, and provide training to IRS Business users
- Develop recommended feedback mechanisms and assessment of feedback results
- Address User Acceptance Testing (UAT) and Cybersecurity Testing requirements
- Provide planning, preparation, briefings, meetings, working groups and teams. Support should include conference facilitation, creation and delivery of graphics, briefing material, and tracking of action items and associated documentation.
- Provide Palantir training to IRS Business Users

3.2. **TASK 2, Training**

- The Contractor shall provide training for users, to include training materials.
- The Contractor shall provide initial training by in-person training sessions, Lunch & Learns sessions, and training videos.
- The Contractor shall provide end users User Documentation, computer-based training modules, and User Aids for a quick resource and guidance on common tasks, updated as system is updated
- The Contractor shall provide face-to-face training for each W&I-RICS & CI field offices, for the initial system introduction and training on using the system and performing manual research functionality.
- The Contractor shall provide train-the-trainer and SME training to identified system experts.
- All training will follow IRS guidelines for computer-based training and the use of live data.

* IRS specific training modules, once completed, will be the property of the Government.

Training modules will be accessible to any user on the IRS DS network who requests access to the application and will be the source used for on-going training.

3.3. **TASKS 3, Period of Performance Summary Work**

Provide a summary of work performed and accepted by the Government, to include a list of deliverables and their acceptance date for each Period of Performance.

The Government also reserves the right to request this report at any point during the performance of the order at the discretion of the Contracting Officer. This ad hoc report, if desired, will only be requested once during the period of performance and is in addition to the regularly scheduled Period of Performance Summary report.

DESIRED OUTCOME- Accurate, up to date description of work performed, list of deliverables, and the date accepted.

3.4. **TASKS 4, Software as a Service (SaaS) Managed Service**

3.4.1.1. ***Architecture***

Following are general IRS IT standards and guidelines that shall be taken into consideration for Discoverer replacement as managed service implementation.

- The Contractor shall produce and maintain a roadmap for platform enhancements, manage the innovation process, and validate that the overall design and implementation of Discoverer replacement solution continues to adhere to the original design and design goals.
- The Contractor shall perform Capacity Planning up to and including: a) Developing and creating long-term plans for the platform, based on growth targets, capacity projections b) Interpreting the demands on the Service and future for workload growth (or shrinkage) c) Influencing demand for computing resources d) Monitoring existing capacity levels.
- The IRS will provide yearly requirements for future capacity management needs (future capacity projections are listed in Sec 3.1.6), and the Contractor shall ensure that there is sufficient capacity all times including peak filing season to meet the agreed service levels.
- The Contractor shall provide the annual Capacity Management Report which encompasses the above listed information as well as capacity allocation information. The annual Capacity Management Report can also be covered in the vendors' Federal Cloud Service System Security Plan if so desired.
- The Contractor shall support Operations and Management **(**O&M**)** functions during new requirements and design activities in accordance with the Contractor's standard O&M terms.
- The contractor shall use out of the box (OOTB) product configurations to meet business needs and minimize development/customization. This should reduce time to deliver and reduce maintenance complexity and cost
- The contractor shall use industry-leading and standard-based architectural and

design patterns to provide a standard way for solution components to interact with the IRS technical environment and supporting tools when calling and conducting services to streamline integration and enable a loosely coupled solution, providing solution durability, compatibility, maintainability and scalability and promoting consistent user experience across the solution.

- The contractor shall deliver a solution that adheres to various regulatory, legal, and security-related policies and guidance, and provide the capability to support IRS availability and redundancy requirements, leveraging high-availability, disaster recovery, and alternate-site processing configurations and technologies as needed to meet IRS requirements.
- Establish a framework, develop processes and perform functions to integrate external components and data, including access control, with the IRS infrastructure, applications, data, and security systems and platforms.

3.4.1.2. *Helpdesk & System Maintenance Support*

The Contractor shall provide maintenance for all components of the Discoverer replacement solution to ensure no system down-time or user interruption is experienced. Users will have 24/7/365 access to IRS Incident Management (KISAM) and can submit support tickets for troubleshooting, administrator, or system issues.

DESIRED OUTCOME:

- Operate and maintain the Discoverer replacement solution to ensure critical revenue protection objective is not interrupted
- Refresh data sets on an ongoing, scheduled basis as determined by data availability.
- Provide Help Desk management and technical support via the KISAM or equivalent Incident Management system
- The Contractor shall manage emergency KISAM tickets during extended hours (06am-04am next day EST), excluding Federal holidays.
- The Contractor shall manage standard helpdesk tickets during business hours (8:00 AM – 8:00 PM), excluding Federal holidays.
- The Contractor shall be available to proactively receive, respond and remediate issues per response times that are determined by business.
- The Contractor shall manage a Frequently Asked Questions forum and provide regular updates, as necessary
- The Contractor shall provide technical support, responses and resolution of user issues and questions. The Contractor shall also provide the IRS project management team with a report of issues received Contractor response time, Contractor mitigation, status and request for closure no later than noon daily during filing season and weekly outside of filing season.
- Fixes and modifications to operational solutions, such as immediate changes to fix critical problems via emergency maintenance or non-critical changes accumulated and implemented as Planned Maintenance.

3.5. **TASK5, PROGRAM MANAGEMENT AND INTEGRATION**

Deliver Program Management and Integration Services across all principal work areas and ensure that overarching security and privacy, Section 508, and program level requirements are met for all current and future task orders.

3.5.1. *Program Management and Control*

The Contractor shall manage following O&M ongoing services for Discoverer replacement solution.

- The Contractor shall manage the program measurement in the Quality Assurance Surveillance Plan (QASP), including a process for developing, implementing, and monitoring a set of performance measures to validate that program activities efficiently and effectively support both business and IT strategies. This includes implementing program-wide measures, quantifiable outcomes, and providing an approach for monitoring actual-versus-expected performance.
- The Contractor shall implement the Program Management Plan that clearly delineates their program and project management approach including, at a minimum, the Project Management Institute's *the Standard for Program Management, Third Edition* (**ISBN-**13: 9781935589686).
- The Contractor shall ensure that all requirements are met in this Task Order and will oversee and govern contractual obligations and risks associated with this contract.
- The Contractor shall control and manage contracts deliverables and work products in conjunction with the IRS.
- The Contractor shall manage the IRS coordinated review cycle of all work products and deliverables.
- The Contractor shall perform quality assurance of work products and deliverables.
- The Contractor shall manage staffing.
- The Contractor shall manage subcontractors, procurement activities, and vendor contractual obligations.
- The Contractor shall be responsible for Discoverer replacement solution O&M Asset Management and will manage a) Hardware maintenance agreement with vendors. b) Software subscription renewals and license entitlement compliance. c) The delivery of quarterly asset management findings will be reflected in the quarterly Composition Report.
- The Contractor shall perform contracts change control.
- The Contractor shall manage new work requests from IRS.
- The Contractor shall provide quality control and oversight over the Discoverer replacement solution O&M SLO reporting to the IRS.
- The Contractor shall coordinate a quarterly Customer Satisfaction Review process based on a template and stakeholder list provided by the IRS PPMO. The Customer Satisfaction

Review process will be coordinated in conjunction with the IRS PPMO. Findings shall be discussed with the IRS PPMO for potential inclusion in the Palantir Innovation Plan.

3.5.2. *508 Testing Support*

The Government is committed to complying with Section 508 of 36 CFR 1194, providing accessibility to employees and members of the public who may have disabilities. The Contractor shall comply with Section 508 compliance requirements as follows:

- Where information technology resources being provided by the Contractor are required to conform to Section 508, such requirements will be included in the requirements document developed in consultation with and approved by the IRS.
- The Contractor shall use assisted testing (JAWS 11 and above, latest version of Google Chrome, Zoom Text version 9 and above, Dragon Naturally Speaking version 10 and above) in their test plans for solution components accessed by Government employees and/or the public. The Contractor shall use screen readers, screen magnifiers, and speech recognition software that are supported by Windows 8 (and higher operating systems for PCs) and Mac OS version 10.1 (and higher operating systems for Apple computers) in their test plans for Section 508 solution components and compliance.
- The IRS will determine whether the Contractor's deliverables are in conformance to Section 508 requirements. Upon successful completion of the agreed upon tests, the Contractor's obligations regarding Section 508 compliancy shall be deemed to have been fully satisfied, subject to the applicable Contract warranty, if any.
- The Contractor shall have the right to rely upon assurances by third parties of compliance with 36 CFR 1194 standards of equipment or software provided by such third parties.
- Section 508 testing shall be conducted by the Contractor as part of ongoing resolution of open issues as defined by the IRS and Section 508.
- The Contractor shall not be responsible for the compliance of Government Furnished Property (GFP) or Government Furnished Information (GFI) with the Section 508 Standards. The Contractor shall not be responsible for non-compliance with Standards to the extent it results from or about the combination of Contractor-provided technology and any other technology of the Government's or its other contractors and/or vendors.
- The Government's designated COR technical representative will have the authority to, and will, resolve any conflicts identified by the Contractor in the interpretation of requirements within the 36 CFR 1194 standards, and will, prior to implementation, provide direction to the Contractor as to the appropriate interpretation (or direct the Contractor to proceed at its discretion).

3.5.3. *Security and Privacy*

The Contractor shall comply with the security, privacy, assurance, and disclosure requirements dictated by the IRS and associated Federal laws and mandates, as shown in following Figure

NIST Risk Management Framework

3.5.4. ***Security Risk Management Framework***

- The Contractor shall operate the security program in accordance with the Risk Management Framework processes outlined in NIST 800-37 current version as shown in Figure NIST Risk Management Framework
- The Contractor shall implement all steps of the NIST Risk Management Framework, except for the authorization, which is an IRS responsibility.
- The Contractor shall manage security risks to minimize potential impact to IRS systems and data.
- The Contractor shall actively manage security risks and promote ongoing information system authorization via a formal risk management process.
- The Contractor shall operate an integrated risk management process across the Palantir environment.
- The Contractor shall prioritize the management of risks based on severity.
- The Contractor shall integrate the security controls into the Palantir architecture and all phases of the System Development Life Cycle (SDLC).

16

- The Contractor shall review information on new or emerging threats as evidenced by threat activities present in monitoring results, threat modeling and other trusted sources.

3.5.5. ***Third Party Assessment***

- On an annual basis, the Contractor shall retain an independent third-party auditor to assess the Contractor's security controls against NIST SP 800-53 and contractual requirements. The third-party auditor shall determine the extent to which security controls are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting security requirements per the SSP, Security Configuration and Change Management Plan, Security Audit Plan, Incident Handling Monitoring and Response Plan, Security Patch Management Plan, Continuous Monitoring Plan, and security operations requirements in this PWS.
- The third-party auditor shall conduct the assessment in accordance with Generally Accepted Government Auditing Standards (GAGAS) and Federal Information System Controls Audit Manual (FISCAM) shall be experienced at conducting security audits of managed security service contracts.
- Each annual assessment shall cover critical and volatile security controls as agreed to in the test planning activities.
- The Contractor shall arrange for the third-party assessment to occur each contract year with the results of the first assessment due to the IRS in contract year two (2).
- The Contractor shall schedule the assessment and provide the third-party auditor access to

facilities, systems, personnel, reports and requested documents necessary to perform the testing.

- Prior to starting the assessment, the Contractor shall meet with the PPMO to ensure that any requirements dictated by the IRM that are above and beyond the FedRAMP moderate baseline are included in the scope of the assessment. In the event that a requirement in the IRM cannot be included in the third-party assessment, the contractor will provide evidence of compliance directly to the IRS.
- The third-party auditor shall develop and provide the Palantir Third Party Security Audit Report as a deliverable to the IRS.
- The Contractor shall obtain a penetration test from a third-party company annually. The third-party tester shall provide the Palantir Third Party Security Audit Report containing the results of the penetration test to the IRS.
- The Contractor shall mitigate the security deficiencies found during third party control assessments, penetration tests and third-party audit during the second and third award year.

3.5.6. *Security Operations*

- The Contractor shall maintain situational awareness of Discoverer replacement solution environment. The Contractor shall correlate security data produced by tools and processes across the environment to detect and respond to security risks. The Contractor shall avoid treating each security tool output as a silo.
- The Contractor shall implement and manage security operations to analyze, monitor and respond to security risks on a day-to-day basis with visibility and responsibility over all Palantir systems and data.
- The Contractor shall monitor security events and potential suspicious activity on a 24/7 basis and respond rapidly to prevent and contain risks.
- The Contractor's security staff shall work in unison with the operations staff to help prevent outages, damage to systems and breaches of taxpayer data.
- The Contractor shall ensure security-monitoring tools are functioning always with visibility across all systems and devices in the environment.
- The Contractor shall operate security configuration and change management processes and procedures in accordance with the Security Configuration and Change Management Plan for Discoverer replacement solution.
- The Contractor shall implement a Security Impact Assessment (SIA) process that is traceable throughout the entire change process and includes post implementation validation.
- The Contractor shall operate security audit processes and procedures in accordance with the Security Audit Plan for Discoverer replacement solution
- The Contractor shall operate procedures to prevent, detect and mitigate advanced persistent threat attacks. The Contractor shall audit critical system components such as the domain controller and VPN activity for indicators of advanced persistent threats.
- The Contractor shall operate incident monitoring, handling and response processes and procedures in accordance with the Incident Handling, Monitoring and Response Plan.
- The Contractor shall conduct forensic activities to investigate potential incidents and suspicious activity. The Contractor shall provide log data and other forensic system information requested to support investigations conducted by the government or law enforcement agencies.
- The Contractor shall operate security patch and vulnerability management processes and procedures in accordance with the Security Patch Management Plan for Discoverer replacement solution.
- The Contractor shall perform ongoing external vulnerability scanning and use the results as inputs to the vulnerability management process.
- The Contractor shall operate using a Separation of Duties Matrix that delineates responsibilities at a granular level.
- The Contractor shall monitor outbound connections and activity to identify and contain potential exfiltration of sensitive data from attackers.

3.5.7. *Protection Taxpayer Data*

- Taxpayer data is a highly sensitive form of Personally Identifiable information (PII). IRS policies prohibit unauthorized inspection or disclosure of taxpayer data.

- The Contractor shall comply with OMB M-07-16, NIST 800-53 Privacy Control Catalog and IRS policies, procedures or guidance to protect taxpayer data.
- The Contractor shall operate privacy controls to prevent, detect and report breaches of taxpayer data. These requirements also apply to subcontractors.

18

3.5.8. ***Continuous Monitoring***

- The Contractor shall operate Continuous Monitoring processes in accordance with NIST 800-137 current version, the Palantir Continuous Monitoring Plan and related Palantir security plans.
- The Contractor shall use the criteria from NIST 800-137 Establishing Monitoring and Assessment Frequencies Section to determine assessment frequencies for security controls.
- The Contractor shall correct control deficiencies using a Plan of Action and Milestones (POA&M) and will assist with reporting on POA&Ms using Trusted Agent FISMA (TAF) security recording website. This requirement is contingent upon Contractor access to TAF. The IRS will provide Read-Only access for the Contractor to allow usage of FISMA Trusted Agent.
- The Contractor shall obtain IRS approval of POA&M completion dates before the POA&Ms are recorded in TAF and Palantir's POA&M Tracker spreadsheet. The Contractor shall submit testing evidence to demonstrate remediation of all POA&Ms. The Contractor shall obtain IRS approval prior to setting the status of POA&Ms as completed in Contractor's POA&M Tracker spreadsheet.
- The Contractor shall provide reports that support IRS FISMA Compliance requirements such as inventory, inventory change log, and security configuration compliance reports.
- The Contractor shall perform continuous monitoring of subcontractor systems as defined in the Palantir O&M continuous monitoring plan.
- The Contractor shall test the ISCP at least annually.
- The Contractor shall participate in an IRS scheduled and coordinated annual ISCP Tabletop Training and Exercise (TTE) and a Functional ISCP test.
- The Contractor shall support the IRS Security Control Assessment (SCA) process including pre-SCA activities, coordinating for resources to support SCA plan development and test case execution.
- The Contractor shall assist the IRS Cyber Security test team in executing annual NIST SP 800-53 current version control test, providing access to facilities, systems, personnel, reports and requested documents to support the IRS Enterprise Continuous Monitoring (eCM) process.
- The Contractor shall test the Incident Handling, Monitoring and Response Plan using a simulated incident at least once annually for a moderate system or every six months for a high system and provide a copy of the Incident Response Test Report, including lessons learned. The simulated incidents should test the security controls implemented to mitigate attacks from the specific threat actors in the Contractor's threat model.

3.5.9. ***Security Reporting***

1. The Contractor shall report Palantir security status using metrics that measure operational security processes and convey the security posture of the systems.
2. The Contractor shall report situational awareness of all Palantir systems and describe threats, vulnerabilities, risks and mitigations.

3. The Contractor shall include information such as the impact on IRS, likelihood of occurrence and severity when reporting risks and mitigations.
4. The Contractor shall provide a Monthly Security Status and a bi-monthly set of slides for the Security PMR.
5. The Contractor shall prioritize the highest severity risks first in all status reports.
6. The Contractor shall avoid reporting raw, uncorrelated data.
7. The Contractor shall provide data in the Monthly Security Status report that supports the SLO metrics.
8. The Contractor shall summarize in the Monthly Security Status report how they followed up on potential incidents and suspicious activity to mitigate risks and prevent breaches. The Contractor shall submit detailed evidence along with the report that shows the steps they performed to follow-up with each potential incident and suspicious activity. This evidence includes the details of all analysis performed to close SIEM tickets, even if those tickets were not communicated to CSIRC.
9. The Vulnerability Assessment (Analysis) shall contain the status of vulnerabilities and Contractor's effort to remediate them through patches or secure configurations.
10. The Security Incident Report contains the detailed investigation documentation for all material potential/suspected incidents detected and investigated by the Contractor's security operations team that affect or may affect the IRS. This includes the details of the analysis performed to close each SIEM ticket escalated.
11. Contractor does report through FedRAMP on OMB Max, IRS request a monthly report of this information.

3.5.10. ***Security Document***

1. The Contractor shall update security plans when changes occur or at least on an annual basis. Examples of scenarios that would prompt updates to security plans include security control assessments, changes in policy or procedure, changes in requirements, process or technology improvements and changes in laws or NIST guidance.
2. The Contractor shall obtain approval from IRS for changes to security plans.

3.6 SNAP Data Alerting LBC

- The contractor will maintain enhanced alerting emails for IT/RRP/RRP-LC and business user consumption to provide early notification of upstream data issues and to provide insight to business users on which tables are impacted by any late data in the morning SNAP refresh.
    - Contractor will implement an RRP cutoff email alert to provide early warning of late missing data. This interim report will:

        - capture which files missed their SLA to get to SNAP
        - Include timestamp of when the file was received by SNAP for processing
    - Contractor will implement a 0700 email alert for business users to notify them of SNAP status. This email will capture:
        - which user-facing tables are late and have not yet updated in order to provide transparency into SNAP table status.
        - Which raw table whose absence/late arrival caused a table to build late

3.7 SNAP FEDRAMP HIGH

- The contractor will maintain system maintain the system requirements for FEDRAMP High

3.8 SNAP NTIN FLAG AUDIT LOG FEATURE

- The contractor will maintain NTIN audit log feature for SNAP Contour query events so that audit logs will contain an NTIN flag and redacted NTINs from a user's query results.
- The contractor will implement additional services that run a parallel query to a user's query that returns results without redacting NTINs. This query will be invisible to users.
- The user's query results and the parallel query results will be compared to validate the difference between the results of each query. If there is a difference between the query results, the audit logs will include the redacted TIN fields in the audit log events and the NTIN flag.
- Contractor will send the audit logs for usage in IRS's audit log tool.

Assumptions:

- Users cannot commit NTIN violations in SNAP because user NTIN lists are redacted from their query results.
- Thus, the NTIN flag features in the audit logs do not mean that a user committed an NTIN violation (i.e. viewed one of their NTINs); rather, they indicate that a user's query would have surfaced one of their NTINs in the results if SNAP did not prefilter out user NTIN lists from search results.

3.9 Office of Fraud Enforcement Pilot user onboarding

- The contactor will support continued use of 15 Office of Fraud Enforcement (OFE) pilot users under this PWS.
- The contractor will provide OFE access to Contour in SNAP. OFE data access in SNAP will be inherited from their BEARS permissions. There will be no additional data integration or workflow configuration as part of the OFE pilot usage.
- IRS will maintain the option to onboard additional OFE users in a non-pilot capacity.

4. PLACE OF PERFORMANCE

The Contractor shall have the option to work at the Government's site if so desired. The Contractor shall be allowed to work at the contractor facility with advanced notification and approval.

-

-

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.

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).

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

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).