Performance Work Statement

IRS CYBERSECURTY FRAUD ANALYTICS AND MONITORING

3.0 DESCRIPTION OF SERVICES/SCOPE OF WORK

3.1 INTRODUCTION AND BACKGROUND

The Internal Revenue Service (IRS), Information Technology (IT) Cybersecurity organization implemented critical Fraud Analytics and Monitoring capabilities to mitigate serious risks to the IRS. Taxpayer and Tax professional interactions with IRS online applications continue to grow significantly each year, and the IRS continues to expand its portfolio of digital services to its customers. Along with this continued growth, fraudsters continuously to probe and develop new schemes to use stolen identity information to access taxpayer Personally Identifiable Information (PII) and file fraudulent tax returns. Recent trends in cyber related fraud and the misuse of government systems have presented an increasing threat to taxpayer information safeguarded by IRS systems, applications, and databases. The IRS requires continued investment in technology and human capital to process the ever-growing transaction volumes and mitigate the evolving fraud risks.

3.1.1 FRAUD ANALYTICS AND MONITORING BACKGROUND

Theft of personal data from sources outside the IRS to perpetrate tax refund fraud exploded from 2010 to 2012. Since then, the IRS has made steady progress protecting against fraudulent refund claims and prosecuting those who engage in this crime. Although the IRS has been effective at stopping individuals perpetrating these crimes, the IRS faces threats posed by organized crime syndicates leveraging increasing amounts of personal data obtained from data breaches outside the IRS. This proliferation of non-IRS identity theft related data breaches creates increasing challenges for the IRS to protect the taxpayers we serve.

At the same time, over the last several years, the IRS has been working to meet taxpayers' increasing demand for self-service and electronic service options by providing them with more web-based tools. As part of that effort, the IRS launched the Get Transcript online application in January 2014. Get Transcript allows taxpayers to view and print a copy of their prior years' tax information, also known as a transcript, in a matter of minutes. Prior to the introduction of this online tool, taxpayers had to wait five to seven days to receive a paper transcript by mail.

During the 2015 filing season, taxpayers used the Get Transcript application to obtain 23 million copies of their recently filed tax information. In May 2015, the IRS cybersecurity team noticed unusual activity on the Get Transcript application thought initially to be a "denial of service" attack. The IRS ultimately uncovered questionable attempts to access the Get Transcript application and on May 21, 2015, the application was disabled. In April 2016, the IRS re-launched the Get Transcript Application with a more rigorous authentication process and increased security monitoring.

As criminals obtain more personal information, fraud detection and prevention techniques must become more sophisticated while continuing to permit legitimate

DRAFT

taxpayers to access their data and use IRS services online. To this end, the IRS IT Cybersecurity organization has created the Cybersecurity Fraud Analytics and Monitoring Team with a focused mission of using advanced analytic techniques to prevent and detect fraudulent activity in IRS's variety of online applications. This team uses highly complex data analysis techniques to prevent and detect fraud. These techniques shall be modeled after the defense and intelligence communities which have demonstrated success with application layer fraud detection. It is expected that this team shall develop metrics, indicators, dashboards, and real-time models to alert the IRS to potentially suspicious activity. The initial focus of these advanced analytic deployment efforts was to support the IRS eAuthentication (AKA eAuth) platform and its protected applications, such as Get Transcript and IP PIN.

Since 2021. the IRS has transitioned from eAuth to the new Secure Access Digital Identity (SADI) framework to meet NIST SP 800-63-3 standards. Beginning May 17, 2023, eAuth shut down to taxpayer traffic, users accessing IRS online services shall no longer have the option to sign in with their exiting IRS username and must register with the current Credential Service Provider (CSP). eAuth successfully completed the full decommissioning of eAuth on 9/30/2023. The new SADI ecosystem includes the following three major components:

- The third-party Credential Service Providers (CSPs) for identity verification.
- The IRS SADI platform for authentication and authorization.
- The wide range of IRS online applications that SADI is designed to protect, including both the frontend and backend of these applications.

The IRS persistently enhances its array of digital offerings for its clientele, leading to a substantial uptick in online engagement among taxpayers and tax professionals alike. In addition, IRS digital services evolution continually introduces key identity management initiatives and new applications that require monitoring and analysis for suspicious activity with aggressive timelines. Along with this evolutionary growth, fraudsters are continuously evolving their capabilities and developing new schemes to steal identities, access taxpayer PII, and file fraudulent tax returns. Maintaining a robust fraud detection posture requires cybersecurity Fraud Analytics and Monitoring (CFAM) to develop a sound strategy and initiate and manage several high visibility initiatives simultaneously to advance its analytics and meet the demands of IRS's digital services initiatives.

3.2 TASK ORDER OBJECTIVES

The IRS has implemented significant enhancements to its Cybersecurity Fraud Analyticsand Monitoring (CFAM) program. This contract shall continue those programmatic successes and ensure the protection of IRS's online applications, taxpayers' data, and the tax revenue.

3.2.1 CYBERSECURITY FRAUD ANALYTICS AND MONITORING (CFAM)OBJECTIVES

As the IRS continues to develop and enhance the capabilities of the Cybersecurity Fraud Analytics and Monitoring Team, it is imperative that this

DRAFT

capability is provided by leveraging this contract and delivery of the tasks identified below. Specifically, the Fraud Analytics support is expected to ensure that the IRS has a team of forensic analysts and data scientists that are organized, trained, and equipped to do the following:

- Maintain and continuously improve the near-real-time monitoring posture to detect and treat evolving cyber threats.
- Quick responses, near immediate acknowledgement and initial observations expected to be reported within one week, to tips, incidents, and suspicious activities. Such responses include identification of the threats' nature, root-cause analysis, and recommendation for immediate action and future mitigation.
- Conduct complex analytics on large transactional data sets to identify anomalouspatterns in users' activity and build and refine predictive models to classify anomalous transactions.
- Conduct deep forensics analysis of incidents and anomalies with log data to identify new use case patterns of behavior and potential attack vectors as input into the predictive analytics, as well as deep analysis of potential anomalous activity isolated by the predictive analysis.
- Review and support the data architecture and data elements design, improvement, analysis, and extract-transform-load (ETL) operation of the entire SADI/CSPs/Applications ecosystem.

Due to the increasing ease with which complex cyber-attacks are being launched, a single clearinghouse of information and centralized pool of highly specialized analysts (See Section 5.0) is necessary to provide a very cost-effective means of ensuring comprehensive analysis of log data for fraudulent activity within IRS online applications. In addition to the importance of a centralized analytics capability to a successful Fraud Analytics Team, equally vital is distributed control and coordination with IRS Business Units, Applications Development (AD) organization, CSPs and system administrators who play key roles in the prevention and detection of fraud in IRS online applications.

The contractor must have broad and deep experience in fraud analytics and demonstrated successes in implementing and supporting this capability within a Cybersecurity organization that supports over 100 million taxpayers, tens of millions of SADI users and analyze the IRS's petabytes of log data in the cybersecurity data lake. The contractor shall be able to process the ever-growing transaction volumes and mitigate the evolving fraud risks. The contractor must provide cybersecurity and fraud analytics visionary talents to assist the Fraud Analytics Team in pursuit of a forward-thinking approach to move its programs to the next level, aligning with Team goals and objectives. Also, the contractor shall recommend and implement technologies, techniques, processes, and procedures that increase program efficiency and effectiveness by incorporating best practices from the industry in fraud analytics.

DRAFT

The contractor shall meet or exceed the objectives of the Fraud Analytics Team major operational functions. The contractor shall be able to handle effectively and timely ad-hoc requests for comments, recommendations, whitepapers, presentations, and project reports from various levels of leadership. Finally, the contractor shall be able to have close operational collaboration with internal and external stakeholders to share information on suspicious user activity, refer specific activity for treatment, and discuss vulnerability findings and risk assessments, and recommend remediations.

The Fraud Analytics Team's operational functions are comprised of several critical processes to prevent, detect, and support the response to fraud incidents. This Fraud Analytics contract support shall provide the following basic services:

- Monitor – Maintain a near-real-time 24x7x365 monitoring posture, with continuously improved indicators/models, and standardized incidence response workflow and procedures.
- Prevention – Provide monthly recommendation reports to communicate their suggested improvements to IRS's applications, processes, and policies to defendagainst and defeat future fraudulent activities.
- Detection – Provide analysis reports by monitoring and analysis of transaction logdata to uncover suspicious and fraudulent activities and trends. Stay ahead of emerging threats by creating and maintaining various data pipelines, fraud indicators, dashboards, risk models, web-based pattern discovery system and scalable normalized automation processes and quick-response analytical capabilities to discover new threat patterns and signatures. Provided reports must delivered timely (within 24 hours of identified suspicious activities).
- Response – Provide forensic analysis reports resulting from impact assessments of detected fraudulent activities. Develop countermeasures against emerging threats, and work with stakeholders for their implementation. At a minimum, reports must include notification methods, stakeholder contacts, IRS incident response process used, mitigation steps taken to prevent further immediate fraudulent actions and recommendationsto prevent additional fraudulent activities.

3.3 SCOPE OF WORK AND TASK DESCRIPTION

- The scope of work performed by the contractor, as reflected in this PWS, is designed to monitor, prevent/deter, detect and support in response to fraud incidents targeting the IRS's data, applications, processes, and tax revenue. This PWS shall result in a FFP and T&M Task Order awarded under GSA Multiple Award Schedule (MAS) IT Professional Services 54151S.
- General Tasks:
    - All projects shall follow IRS Enterprise Life Cycle (ELC) and Investment Decision Management (IDM) processes.
    - The contractor shall produce Work Products/Deliverables that conform to, and

DRAFT

integrate with, existing IRS standards and guidelines.

- The contractor shall conform to all IRS Security and Disclosure policies.
- The contractor shall support IRS initiatives to counter evolving fraud trends, mitigate emerging threats, and enhance the overall security posture of online applications.

- Specific Tasks:
  - Provide comprehensive program and project management support.
  - Develop, enhance and maintain a 24x7x365 fraud monitoring posture.
  - Support SADI Applications and CSP Integration.
  - Fraud analytics product development and enhancement.
  - Fraud Investigation tool development and manual investigation process automation.
  - Perform deep forensics analysis of log data.
  - Perform predictive analytics.
  - Develop and maintain policies, governance, and standard operation procedures (SOPs).
  - Provide support for analytics platform cloud transition and SEIM (Splunk) development and enhancements.
  - Provide support for IRS' analytics ecosystems.
  - Provide support/augmentation for IRS' Watch Operations Teams.
  - Produce and submit monthly and quarterly project management reports.
  - Produce white papers, briefings, and presentations to leadership upon ad-hoc requests with tight deadlines.
  - Address inquiries from TIGTA, GAO, Congress, and law enforcement agencies.

3.3.1 TASK 1: FRAUD ANALYTICS AND MONITORING COMMON PROJECT TASKS (Firm Fixed Price and Optional Labor Hour Tasks)

This FFP and Labor Hour Sub-task list provides the management oversight and subject matter expertise to ensure that all contractor resources are effectively contributing to the desired programmatic outcomes. This task leverages the designated resources identified, bylabor category and skillset requirements, in Section 5.0 to compile the deliverables listed below and provide overall support for the delivery of the Fraud Analytics and monitoring program.

3.3.1.1 SUB-TASK: ORIENTATION BRIEFING (FFP)

Description: Within five (5) days of task order award, the contractor shall conduct an orientation briefing for the government.

The government does not desire an elaborate orientation briefing nor does it

DRAFT

expect the contractor to expend significant resources in preparation for this briefing. Rather, the intent of the briefing is to initiate the communication process between the government and 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 orientation briefing shall be held at the government's facility and both parties shall mutually agree upon the date and time.

Desired Outcome: The completion of this briefing shall result in the following:

- The contractor and government personnel who shall perform work under thistask order shall be introduced.
- The government shall show the applicable facilities to the contractor if the contractor shall be performing work on the government's site. The government may provide any GFP to the contractor at this time.
- Identify issues concerning the contractor's request for clearances for itspersonnel shall be discussed to plan for resolution.
- The contractor shall present its plan to accomplish the work under this PWS.
- The contractor shall provide the accounting period end dates to be used for the term of this task order.

3.3.1.2 OPTIONAL SUB-TASK: RAMP-UP KNOWLEDGE TRANSFER (LH)

Description: Ramp-Up Knowledge Transfer is defined as the contractor acquiring anunderstanding, the necessary documentation, information, and processes related to any work in progress. **This task applies ONLY if a transition to a new vendor occurs.**

This task includes meeting with the IRS Subject Matter Experts frequently to gather any tacit knowledge related to the Core Systems, Compliance Document Matching and Solutions Engineering/Enterprise Services tasks or programs in development.The government estimates this task shall take approximately four to six months to complete after the Task Order is awarded.

The contractor shall appoint a knowledge transfer manager to oversee the transfer of knowledge and ensure all areas are accounted for. If desired, this can be the Project Manager (PM) or Project Scheduler. Prior to the transfer of knowledge, thecontractor shall develop a draft Knowledge Transfer Plan (KTP) and present it to the government within the first 15 business days after award (See 3.4.1 REVIEW OF DELIVERABLES).

The government shall have ten (10) business days to review the draft KTP plan and provide comments to the contractor. Government and contractor representatives shall then meet to discuss the comments after which the contractor shall incorporatethe agreed-upon changes and deliver a final KTP within five working days of the government's feedback.

The contractor shall meet with the IRS bi-weekly (twice a month) to discuss

DRAFT

the progress of the knowledge transfer. The contractor shall present an updated MS Project Schedule and discuss any risks or concerns at this time.

Desired Outcome: The contractor provides a Knowledge Transfer Plan that is accepted by the government and successfully completes knowledge transfer in accordance with the plan.

3.3.1.3 SUB-TASK: PERIOD OF PERFORMANCE SUMMARY REPORT (FFP)

Description: Provide a summary of work performed, including a list of deliverables, at the end of each Base and Option 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 CO. This ad hoc report, if desired, shall be requested at least once during the life of the task order and is in addition to the regularly scheduled Period of Performance Summary report.

Desired Outcome: The contractor shall provide the Period of Performance Summary Report.

3.3.1.4 SUB-TASK: TRANSITION TO SUPPORT (LH)

Description: The purpose of this section is to ensure a seamless transition of work products and knowledge without regard to whether this is a new Contractor or an incumbent to and from the Contractor, preserving the continuity and quality of the services, as well as the integrity, accessibility, and operability of the data and systems involved.

The transition to support process shall include, but not be limited, to the following:

- Transition In:
  - The Contractor shall, ensure a smooth transition of the services from any incumbent contractor or in-house team to the Contractor.
  - The Contractor shall collaborate with any incumbent contractor or in-house team to understand and document the current state of the services, processes, and systems.
  - The Contractor shall be responsible for obtaining, all tools, source code, validation evidence, repeatability proofs, source control repositories, standard operating procedures, and other computational, mathematical, data analytic, or forensic artifacts relevant to the services.
- Transition Out:
  - Upon the expiration, termination, or conclusion of this Contract, or upon the Agency's request, the Contractor shall facilitate a seamless transition of the services to the Agency, a succeeding contractor, or back to an in-house team without the aide of the in-house team.
  - The Contractor shall provide the Agency with:
    - Data models and analytics tools and frameworks.
    - All source code developed under this contract, with comprehensive

DRAFT

documentation.

- Process descriptions and flowcharts.
- Evidence of validation for all computational models, algorithms, and processes.
- Proof of repeatability for all tasks and processes.
- Access to and documentation for source control repositories.
- Standard operating procedures.
- Broad knowledge transfer, including training sessions and workshops, of processes and code.
- All other computational, mathematical, data analytic, or forensic artifacts generated during the term of the Contract.
- Configurable data including usernames, passwords, application settings and scripts.

- The Contractor shall ensure that all transitions are done in compliance with relevant FAR (Federal Acquisition Regulation) clauses, specifically FAR 52.237-3 "Continuity of Services".
- The Contractor shall provide support and assistance for a period of 180 days post-transition to address any queries, issues, or challenges faced by the Agency or the succeeding contractor.
- Warranties and Representations: The Contractor represents and warrants that all information, code, and artifacts provided during the transition phases are complete, accurate, and free from any encumbrances, and that the Agency shall have full rights to use, modify, and distribute them as it sees fit.
    - Confidentiality: The Contractor shall maintain the confidentiality of all information acquired during the Contract's term and shall not disclose or use such information for any purpose other than to fulfill its obligations under this Contract, unless expressly authorized in writing by the Agency
    - Indemnification: The Contractor agrees to indemnify and hold the Agency harmless from any claims, damages, or losses arising out of the Contractor's failure to properly transition the services, data, or any other obligations under this section.

Desired Outcome: The contractor shall transition support to the government prior to the completion of the contract.

3.3.1.5 SUB-TASK: PROJECT & PROGRAM MANAGEMENT

This shall be achieved by providing direct subject matter expertise, guidance, and oversight as reflected in the following descriptions of work efforts.

Description: The contractor shall be able to adopt a comprehensive program management approach to address both strategic and highly tactical developments.

The contractor shall be able to utilize program and project management methodologies to

DRAFT

operate and stay ahead of the evolving cyber-threat landscape. The contractor shall provide program management with the requested deliverables and services, collaborate across the IRS, and participate in the development of analytic strategies to achieve identified objectives.

The contractor shall coordinate with IRS Cyber Operations personnel to ensure that the Fraud Analytics and Monitoring program objectives are aligned with the direction of this task order by routinely reporting progress against established project schedules and performance requirements. The contractor shall enhance data agility to reduce time-to-insight from data & analytics and accelerate investigations.

In addition, the contractor shall prepare and submit project artifacts and provide project schedule and status update as requested by IRS Cybersecurity IT Modernization and the Inflation Reduction Act (IRA) programs. The contractor shall also need to respond timely to leadership's ad-hoc requests for statistics, briefings, whitepapers, operations review, and executive summaries.

Desired Outcome: The contractor develops analytic strategies to support the Fraud Analytics mission and consistently provide assurance to designated IRS personnel that task objectives and performance requirements are being achieved and schedules are being met.

The contractor establishes and implements clear program performance objectives, milestones, and metrics tailored towards our advanced fraud analytics' goals and operational needs.

The contractor develops, prioritizes, and aligns strategies to meet performance objectives, demonstrating sound decision-making and considering key influences on organizational and operational performance.

The contractor effectively works with the IT – Integrated Master Schedule (IT IMS) representatives to create project schedule Work Breakdown Structure (WBS).

The contractor leverages available resources (human, financial, computational, etc.) to maximize efficiency and produce high quality results.

The contractor ensures effective internal/management controls and has taken appropriate action to strengthen controls and correctly identified weaknesses, to provide timely response to IG audit requests and attention to information security.

3.3.2 TASK 2: FRAUD ANALYTICS AND MONITORING HIGHLY SPECIALIZED TASKS (FFP)

3.3.2.1 This Firm-Fixed Price (FFP) task provides the specialized, technical expertise to implement near real- time fraud and predictive analytics and monitoring on the government's on-premises and cloud-based big data platforms, with structured and unstructured data sets to produce analytic views of correlated activities. This includes development of fraud indicators, predicting previously undetected anomalous or malicious activity, while implementing and maintaining a 24x7x365 fraud monitoring capability that staffed by at least two analysts per shift. The vendor is required to provide their own staffing plan but at a minimum it shall

DRAFT

include 2 contractors per shift equates to 9 of the 22 FTE devoted to executing the 24x7x365 support and presumes the remainder of the 13 FTE would be to address the remaining skillsets required to execute the highly specialized fraud analytics program activities (e.g., data scientists, data developers, and senior forensics analysis). The following represent tasks, with the understanding that the contractor is responsible for the outcome of the fraud detection or lack of fraud detection during the contract and as such shall implement the requisite analytic methods to detect anomalous and/or potentially fraudulent activity with timely alerts provided to IRS management.

3.3.2.2 SUB-TASK: CURRENT STATE OPERATIONS AND MAINTENANCE (FFP)

Description: The contractor shall perform predictive analytics and deep forensics activities associated with the IRS's SADI/CSPs ecosystem and online applications. In support of this task, the contractor shall conduct analytics and forensics functions, provide 24x7x365 monitoring coverage, recommend actions, treatments, and mitigations, and coordinate with stakeholders on all findings and implementations. This includes changes the user interface, the business logic, the user flow and processes, improvement in logging, data elements, and data transfer processes; sub-activities associated with this task include:

- Development and customization of analytical algorithms for detection of anomalous, malicious, and fraudulent activity. Provide subject matter expertisein interpreting analytical results to guide business processes.
- Responsible for managing a highly skilled team to analyze real-time event data,detect and respond to potential security incidents, and coordinate mitigation efforts through closure with internal business units and external third parties.
- Lead and train a team of analysts in a high stress 24x7x365 Operations and Response environment to perform real-time analysis of events, produce qualityoutput, and execute notifications and escalations within 60 minutes of event occurrence to confidently brief senior government leadership.
- Automate interactive and batch investigation tasks.

Work with data services team to manage the collection of log data to ensure timely delivery, completeness, integrity, and availability. Work with application developers to understand the workflow and business logic.

- Leverage the use of advanced data analytics with the use of Machine Learning/AI paradigms. Assist in the collection and documentation of new data sources when necessary.
- Create and maintain data dictionary and data catalog, manage reference and master data in RDBMS or NoSQL database.

DRAFT

- Develop data extraction, transformation, and loading (ETL) processes and utilities.
- Development of signatures (i.e., a combination of indicators) that shall help identify fraud activity and differentiate them from benign activity.
- Developing and maintaining a historical list of identifiable fraud activity whereby new efforts to defraud the IRS system may be easily identified from past activity.
- Development of new fraud indicators and models based on predictive and forensics analytics findings.
- Development of monthly reports on Fraud Analytics findings.
- Development of automated reports for data monitoring.
- Development of web applications as needed to help fraud investigations.
- Provide Forensics and Incident Management support in response to anomalous, malicious, and fraudulent activity.
- Respond to fraud incidents, notify required parties, and support remediationactivities.
- Support the implementation and testing of changes to data ingestion andanalytics processes to accommodate modifications in data sources.
- Perform open-source research and integrate other threat intelligence asneeded.
- Provide off-hour forensic analytics coverage: 5pm – 9am; weekends, andholidays.
- Work with CSPs for timely data and intelligence sharing, root-cause analyses, user process improvements, and incidence responses.
- Work with SADI for the integration of new CSPs: data elements specification and testing, user-flow analysis (including NIST compliance), data acquisition and ETL.

Desired Outcome: The contractor shall maintain current predictive and forensic analytics capability and provide off-hour forensic analytic coverage for the IRS applications monitored by the Cybersecurity Fraud Analytics and Monitoring (CFAM) team.

The contractor improves operational efficiency and effectiveness, removes workflow bottlenecks, replaces time-consuming, labor-intensive, and error-prone manual investigation tasks and repetitive investigation processes, standardizes the workflow, reduces complexity and operating costs, and increases team's performance and transparency,

Knowledge gained shall be clearly documented and communicated to the team and IRS stakeholders timely.

Communicate effectively with IRS leadership and internal teams by

DRAFT

delivering detailed documentation and presentations of incident handling and analysis, proactively anticipating leadership questions, and offering mitigation strategies based on historic knowledge and operational requirements. The documents and presentations shall be of high quality, free of errors, logical and consistent, and easy-to-understand for non-technical audiences.

3.3.2.3 SUB-TASK:CONTINUOUS ENHANCEMENTS AND EXPANSION OF ANALYSIS (FFP)

Description: The contractor shall expand its fraud analytics operational support to encompass all the applications monitored by CFAM, while continuously enhancingexisting capabilities. This shall include application of predictive analytics and deep forensics to transactions associated with all current online applications. In supportof this task, the contractor shall conduct analytics and forensics functions, and coordinate with other IRS business units, on all findings; sub-activities associatedwith this task include:

- Log analysis, parsing, data transformation and data analysis of new front and back-end transactions and Fraud Channel Intake (FCI) transactions from CSPs.
    - It is critical for our organization to continually review and analyze all attempts made in relation to the Fraud Intake Channel. This not only helps in identifying possible breaches but also in fine-tuning our security measures and improving our response to potential threats.
    - Historical Precedence: A case in point underscoring the significance of reviewing attempts is the situation faced with the "Get Transcript" application in May of 2015. The vigilance in monitoring attempts provided key insights into questionable activities that might have otherwise gone unnoticed. Such a proactive approach led to the identification of vulnerabilities and, consequently, a timely intervention to thwart further malicious actions.
    - In light of historical incidents and the continuous evolution of digital threats, it remains of paramount importance to give due diligence to reviewing attempts, especially in channels that are directly or indirectly related to fraud detection and prevention.
- Incorporation of new techniques to analyze existing data sets.
- Development and customization of analytical algorithms for detection offraudulent activity.
- Provide subject matter expertise in interpreting analytical results to guidebusiness processes.
- Development of fraud indicators for both offline analytics and near real time monitoring.
- Development of machine learning models based on predictive and forensics analytics findings.

DRAFT

- Enhancement of data ingestion and analytics visibility to include near real time streaming (<1 hour) analytics.
- Development of monthly reports on CFAM findings.
- Provide Forensics and Incident Management support in response to fraudulent activity.
- Respond to incidents, notify required parties, and support remediationactivities.
- Support the implementation and testing of data ingestion and data analyticssystem changes to accommodate modifications in data sources.
- Perform open-source research and integrate other threat intelligence asneeded.
- Support analytics architectural definition, including Cyber IT architecting.

Desired Outcome*:* The contractor shall develop and expand predictive and forensic analytics capabilities for applications whose log data are currently available to CFAM, to support more reliable identification and monitoring of anomalous, malicious, and fraudulent activities associated with these applications.

The contractor develops modern fraud analytics products using AI and ML and other cutting-edge technologies, to incorporate diverse sources of information, intelligence, and team's insights. These products shall enhance and expand CFAM's fraud-fighting capabilities, streamline the operation, facilitate end-users' adoption and increase cost efficiency for the CFAM program.

The contractor communicates effectively with IRS leadership and internal teams by delivering detailed documentation and presentations of incident handling and analysis, proactively anticipating leadership questions, and offering mitigation strategies based on historic knowledge and operational requirements. The documents and presentations shall be of high quality, free of errors, logical and consistent, and easy-to-understand for non-technical audiences.

3.3.2.4 SUB-TASK: SUPPORT NEW APPLICATIONS AND NEW CREDENTIAL SERVICE PROVIDERS (FFP)

Description: The contractor shall support the launch and protection of new IRS online applications. This shall include discovery to understand each new application's process design, business logic, user behaviors, and work with the application's owner to acquire the data, examine the data quality, recommend improvement if needed, and develop analytics and monitoring coverage. In addition, the contractor shall support the integration of new CSPs with SADI.

In support of this task, the contractor shall:

- Interface with application owners and CSPs and IRS's Information Technology resources(applications, systems, databases, and log data), as well as business representatives to understand the application's and/or CSP's user behavior and transaction data

DRAFT

structure.

- Log analysis of applicable data sources to develop data ingestion models. Provide recommendations to application owners and/or CSPs to improve data dictionary and data logging if necessary.
- Implementation and testing of ingestion engines, and development of analytical data sets.
- Analysis of analytical data sets to reconstruct and understand user behavior.
- Development of fraud indicators for both offline analytics and near real time monitoring.
- Development and customization of analytical algorithms for detection of fraudulent activity.
- Development of models, including machine learning models based on predictive and forensics analytics findings.
- Development of monthly reports on CFAM findings.
- Provide Forensics and Incident Management support in response to fraudulent activity.
- Respond timely to fraud incidents, determine the nature of the threats, and recommend actions.

Desired Outcomes: The contractor shall develop a predictive and forensic analytics capability to prevent, detect, and mitigate anomalous, malicious, and fraudulent activity.

The contractor maintains a robust fraud detection posture and advances CFAM's analytics and meets the demands of IRS's digital services initiatives.

The contractor communicates effectively with IRS leadership and internal teams by delivering detailed documentation and presentations of progresses, issues, and findings. The documents and presentations shall be of high quality, free of errors, logical and consistent, and easy-to-understand for non-technical audiences.

3.3.2.5 SUB-TASK: SECURITY THREAT COLLABORATION WITH STAKEHOLDERS (FFP)

Description: The contractor shall coordinate with internal and external entities, including the tax preparation industry, the financial services sector, and intelligence community to identify and address new and emerging techniques used by adversaries to commit fraud, data theft, social engineering, phishing campaigns, intelligence gathering, or other schemes. The contractor shall operationally collaborate with several key stakeholders to share information on suspicious user activity, refer specific activity for treatment, and discuss vulnerability findings and risk

DRAFT

assessments, and recommend remediations. These stakeholders include both IT organizations such as Cybersecurity, Applications Development (AD), WebApps, and Integrated Enterprise Portal (IEP), and non-IT organizations such as Return Integrity and Compliance Services (RICS), Identity Assurance (IA), Identity and Access Management (IAM), Privacy Governmental Liaison and Disclosure (PGLD), Office of Fraud Enforcement (OFE), Treasury Inspector General for Tax Administration (TIGTA), Criminal Investigation (CI), and Research, Applied Analytics and Statistics (RAAS), as well as external non-IRS entities such as Credential Service Providers (CSPs).

Sub-activities associated with this task shall include:

- Engage in collaborative sessions with key stakeholders, including IRS Subject Matter experts, Executives, Branch and Line managers exuding professionalism and competence.
- Present to IRS leaders and provide expert opinion on findings and or assessments.
- Regularly schedule meetings with key customers to facilitate collaboration and feedback on CFAM referrals.
- Collaborate with key internal and external stakeholders to improve our fraud detection capabilities to achieve business results.
- Collaborate with CI, TIGTA and OFE to support ongoing investigations on suspicious activity.
- Hold regularly collaborative information exchange sessions with CSPs to improve each party's fraud detection capabilities and discuss potential CSP product vulnerabilities and recommended remediations.
- Hold information exchange sessions with RAAS to better inform each other of their respective findings for identification of fraud schemes.

Desired Outcomes: The contractor integrates new and existing capabilities and resolves resource and visibility gaps to support prompt identification and mitigationof new threats and adversary techniques.

3.3.2.6 SUB-TASK: NEAR REAL-TIME FRAUD ANALYTICS AND MONITORING (FFP)

Description: The contractor shall provide 24x7x365 fraud analytics and monitoring to examine designated dashboards, events, and logs to identify and escalate potential indicators of fraud. The contractor shall execute a near real-time analyticsstrategy based on identified and correlated events of interest and apply analyticaltechniques to increase efficiency and effectiveness. The contractor shall recommend and execute coverage schedules to provide 24x7 monitoring based effectively and efficiently on identified patterns of activity and load and support additional event investigation as required and follow the ticketing and event escalation procedures. Events of interest shall be immediately

DRAFT

reported to an identified incident coordinator. The contractor shall work with the government to keep the Standard Operation Procedures (SOPs) updated.

Desired Outcomes: The contractor provides near real-time detection and notification of potential fraudulent use of IRS systems or applications.

3.3.2.7 SUB-TASK: ENTERPRISE IT EVENT MANAGEMENT AND COORDINATION

Description: The contractor shall provide 24x7x365 coverage to coordinate the IRS-wide response to significant cybersecurity and data disclosure incidents. The contractor shall act as a facilitator or a main point of contact for bringing various organizations together and serve as the main distribution point for disseminating the resulting response or mitigation strategies to the rest of the constituency. The contractor shall coordinate the incident handlers' activities, gather information from the handlers, provide incident updates to other groups, and ensure that the team's needs are met. The coordination work may involve collecting contact information, notifying organizations of their potential involvement, collecting statistics about the numberof assets involved, and facilitating information exchange and analysis. Part of the coordination work may involve notification and collaboration with IRS Counsel, TIGTA, Criminal Investigations, PGLD, other Information Technology organizations, vendors, CSPs, and other IRS business units. This service does not involve direct, on-site incident response.

Desired Outcomes: The contractor coordinates significant incidents to mitigate malicious activity, manage significant situations, and supports recovery efforts.

3.3.2.8 SUB-TASK: CLOUD MIGRATION AND PLATFORM ADVISORY SERVICES (FFP)

Description: The Internal Revenue Service (IRS) Cyber division is migrating their Cyber Security Data Warehouse (CSDW) analytics tools from on-premises into the Treasury Workplace Community Cloud FedRAMP High (WC2-H) platform. The migration approach will be Hybrid Lift and Shift with similarities to the current on-premises system, but with a desire to leverage cloud native capabilities such as AWS' Elastic MapReduce (EMR), S3 object storage services, and Elasticsearch and other analytics tools.

The overall solution will migrate the IRS CSDW suite to the WC2-H environment for Platform as a Service (PaaS) leveraging AWS for Infrastructure as a Service (IaaS). The WC2-H environment offers a viable solution for IRS CSDW with a design that incorporates FedRAMP guiding principles and offers FedRAMP-approved tools and services to support IRS CSDW's requirements. CSDW cloud is expected to be fully operational by 12/31/2023. IRS Cybersecurity plans to integrate data feeds fully by the end of March 2024, and initiate the migration of CFAM operations over to the CSDW cloud in 2024.

DRAFT

The contractor shall support fraud analytics platform migration from on premises servers to the cloud by working with cybersecurity data services team. Tasks include but not limited to rebuilding automated processes to align with the new environment and advising on cloud specific capabilities and implementing performance improvement measures.

The contractor shall provide advisory guidance for integration, platform administration, programming, data source management, schema, and normalization functions for all identified applications monitored from the IEP.

Desired Outcomes: The contractor shall fully transition CFAM's operations from on premises to a cloud platform to improve accessibility to vast cybersecurity data collection, accelerate CFAM's fraud-detection research and development, facilitate large-scale cases investigations, and reduce response time to court orders and inquiries from Congress and law-enforcement agencies.

The contractor provides supporting fraud analytics operations cloud migration and platform advisory services. Here are some desired outcomes:

- Ensure a smooth and successful migration of the fraud analytics operations, including data, tools, and pipelines, to the cloud environment.
- Guarantee the security and integrity of sensitive data throughout the migration process and within the cloud environment, adhering to relevant compliance standards and regulations.
- Improve the performance and scalability of fraud analytics operations in the cloud, allowing for faster data processing and analysis.
- Optimize cloud resources to control costs while maintaining or improving the quality and capabilities of the fraud analytics operations.
- Minimize disruptions to fraud analytics processes to ensure seamless operations.
- Leverage cloud-native features and technologies to enhance fraud detection and analysis capabilities.
- Establish a robust monitoring and alerting system to proactively detect and respond to issues in the cloud-based fraud analytics environment.
- Transfer cloud-related knowledge and skills to the IRS's IT and analytics teams to enable self-sufficiency and long-term management.
- Maintain comprehensive documentation of the cloud architecture, configurations, and operational procedures to support ongoing management.
- Identify and address potential risks associated with the fraud analytics operations in the cloud, ensuring the continuity of critical functions.

DRAFT

- Ensure that the cloud migration and platform advisory services align with the organization's fraud prevention and detection objectives.
- Meet or exceed agreed-upon SLAs for fraud detection accuracy, response times, and system availability.
- Continuously evaluate and optimize the cloud-based fraud analytics environment to adapt to evolving fraud patterns and emerging technologies.
- Enable advanced data analytics and reporting capabilities to provide insights into fraud trends and patterns.
- Design the cloud analytics platform to be scalable and flexible, accommodating growth in data volume and analytics demands.

To provide a clear guideline for contractors in handling and responding to congressional inquiries, particularly concerning accounts that have been treated for fraud potentially based on a false positive.

Scope: This section applies to all contractors involved in fraud detection, management, and response mechanisms concerning legislative matters.

Congressional Inquiries – Importance and Implications: Congressional inquiries, stemming from the representative duty of Congress to the American populace, bear significant weight. Their nature requires an immediate, accurate, and transparent response, ensuring that the legislative branch receives a comprehensive understanding of any matter in question.

Contractor Responsibilities:

- Acknowledgment: Upon receipt of any congressional inquiry, contractors must immediately acknowledge its receipt per FAR 52.233-1 (Disputes), affirming the commitment to resolve any concerns.
- Detailed Investigation: A comprehensive review of the account or situation in question is imperative. This investigation shall determine the validity of fraud allegations, mechanisms employed in detection, and any potential oversights leading to false positives.
- Communication and Reporting: Using guidelines from FAR 52.215-2 (Audit and Records—Negotiation), contractors must ensure that all communications are well-documented, clear, and unbiased. Transparency is key, and all findings – especially in cases of false positives – shall be communicated unequivocally to the inquiring legislative body.
- Corrective Actions: In events of false positives, contractors are responsible for:
    - Pinpointing and detailing the factors leading to the oversight.

DRAFT

- Implementing immediate corrective measures to rectify the error.
- Setting forth strategies to minimize the likelihood of future occurrences.

Documentation and Record Keeping: As mandated by FAR 4.703 (Policy), contractors must ensure proper documentation of all activities related to the congressional inquiry. This includes investigative reports, communication records, and any corrective action plans.

Training: Consistent with FAR 52.203-13 (Contractor Code of Business Ethics and Conduct), contractors must ensure their teams are regularly trained on: The legislative landscape and protocols related to congressional inquiries. Technicalities of fraud detection systems to competently address any false positive concerns. Effective and transparent communication strategies.

Conclusion: By adhering to the above guidelines and the stipulations set forth in the relevant FAR clauses, contractors ensure not only compliance but also foster trust and transparency with both the legislative branch and the public at large.

3.3.3 OPTIONAL TASK 3: SURGE SUPPORT FRAUD ANALYTICS (LH)

This labor task provides the specialized, technical expertise required to effectively respond to unforeseen increases in Fraud Analytics requirements driven by IRS application modifications and/or significant expansion in the scope of the monitoring platform. Such surges may arise from changes of Tax Season deadlines, new Congressional mandates, expedited launch of new initiatives, new fraud trends, large-scale 3rd-party data breaches with potential impact on IRS, new tips from partners, etc. These surge resources would be leveraged to augment contractor staffing supporting Task 2, “Fraud Analytics Highly Specialized Tasks” and would provide similarly scoped tasks that shall have resulted from additional IRS fraud analytics requirements throughout the course of this contract. This shall be a labor hour task, that includes a condition not to exceed a specified amount of funding for surge support.

3.3.4 OPTIONAL TASK 4: SUPPORT STAKEHOLDERS AND CSPs BY DEVELOPING REQUIREMENTS AND IMPLMENTATION CAPABILITIES RELATED TO FRAUD AND IDENTITY THEFT (LH)

This labor hour task requires specialized fraud analytics expertise to support IRS stakeholders with their tasks which would benefit from the unique skills and information obtained through extensive fraud analytics experience. The following tasks currently include but are not limited to:

- Specify log data requirements for new stakeholders for fraud detection and compliance purposes.
- Work with engineers to understand stakeholder data exchange

mechanisms and log formats and develop prototype pipelines.

- Testing and quality assurance of stakeholder data elements and its data dictionary.
- Work closely with CSPs and other stakeholders on log data delivery design and shared data access.
- Identify gaps and issues in stakeholders design and ensure compliance with NIST identity management guidance.
- Establish procedures for collaboration with stakeholders for case tracking, investigations, and intelligence sharing.
- Conduct fraud risk assessment of stakeholder's identity-proofing and authentication workflow design and security controls.
- Conduct desktop exercises with IRS stakeholders and CSPs on incidence responses.
- Identify security weaknesses and vulnerabilities in CSPs, facilitate their remediation to enhance anti-fraud capabilities.
- Prepare documents and responses in case of TIGTA inquiries and audits.

3.3.5 SKILLS REQUIREMENTS

The skill sets provided for all the tasks identified in this PWS must be commensuratewith the labor categories listed in the table in section 5.0. The contractor shall provide experienced program management, project management, personnel withdemonstrated success managing an analytics team that required integration and collaboration across a large, complex organization of similar scope to the IRS. Specialized program management and integration experience shall also include expertise in such areas as advanced fraud detection techniques. The contractor shall have proven experience with detection, and monitoring in a large and diverse operational environment,expertise in Open-Source Intelligence (OSINT) techniques, development of intelligence products, data mining, predictive and prescriptive analytics, link analysis,network analytics, text mining (structured and unstructured), and data visualization techniques.

This experience, at a minimum, shall reflect the following. The contractor shallprovide personnel with the following qualifications that have demonstrated:

- Ability to innovatively apply the latest fraud analyticstechniques, technologies, industry standards, processes, procedures, and best practices to existing operations.
- Success in implementing and supporting this capability within the Government Agencies, Financial Services Industry or US Intelligence Community.

DRAFT

- Success in implementing Fraud Analytics governance processes; specifically, the discipline to organize reporting, analytics and manipulate data to support analytical models and filters.
- Ability to develop software applications and provide software domain expertise tosolve computer science cyber issues and associated forensics.
- Expertise in Data Extraction, specifically the ability to obtain data from variant sources and manipulate the data to support many analytical models and filters.
- Ability to articulate as well as support a visionary approach that shall position the IRS to successfully deter, detect, and mitigate near and long-term cyber threats from a fraud landscape perspective.
- Success in performing innovative deep data analysis by senior level Subject MatterExperts (SME), such as Data Scientists and Law Enforcement among others, across a wide range of IT systems such as mainframes, servers, databases, and network devices, including applications, to identify anomalous activity by privilegedand nonprivileged users on IT systems**.**
- Ability to perform machine learning, natural language, and statistical analysis methods, such as classification, collaborative filtering, association rules, topic modeling, time-series analysis, regression, statistical inference, and validation methods.
- Capability to analyze big data using sophisticated analytical and algorithmictechniques.
- Contribution to data mining architectures, modeling standards, reporting and dataanalysis methodologies.
- Collaboration with stakeholders to integrate data mining results with existing systems and monitor data mining systems performance and implement efficiencyimprovements.
- Ability in working cohesively and productively with various levels of management to include technicians that reflects a mature understanding of operations and organizational dynamics.
- Ability to communicate the correlation of vast stores of log data creatively and cogently into succinct presentation models for informed and decisive management action to deter, detect, and mitigate fraud risks.
- Ability to create high-quality, error-free, logical and consistent technical and non-technical documents and presentations.
- Ability and discipline in following IRS change control processes and industry best practices in source code control and documentation management.
- Experience in program management, project management, personnel

DRAFT

with demonstrated success managing an analytics team that required integration and collaboration across a large, complex organization of similar scope to the IRS.

Further, the contractor shall provide the required skillsets as identified inSection 5.0 below that possess the following qualifications:

Quantitative and Qualitative methods, techniques and theories drawn from many fieldswithin the broad areas of mathematics, statistics, operations research, information science, and computer science, including signal processing, probability models,machine learning, statistical learning, data mining, database, data engineering, pattern recognition and learning, visualization, predictive analytics, uncertainty modeling, data warehousing, data compression, computer programming, artificial intelligence, and high performance computing. The incumbent shall bring analytical rigor and statistical methods to apply on data in all its forms including structured and unstructured data to form, develop and provide advice and analytical support to all levels of management.

Major duties for the contractor personnel include but are not limited to:

- Analyze and model data in all its forms (both structured and unstructured) using advanced statistical methods and implement algorithms and software needed to perform analyses.
- Cluster large amount of user-generated content and process data in large-scale environments using platforms and services like Amazon EC2,EMR, SageMaker , Glue, RedShift, Kafka, Lambda, RDS, Hadoop, Spark etc. Perform explanatory data analyses, generate and test working hypotheses, prepare and analyze historical data and identify patterns and correlations.
- Research and develop methods for applications in diverse domains such as cybersecurity, fraud analytics, service development, marketing research, public policy, optimization, and risk management. Research new algorithms and methods for optimizing service quality, business growth and new ways for modeling end-user behavior through quantitative analysis.
- Perform machine learning, natural language, and statistical analysis methods, such as classification, collaborative filtering, association rules, topic modeling, time-series analysis, regression, statistical inference, and validation methods.
- Lead client engagements focused on Big Data and Advanced Business Analytics,in diverse domains such as cyber security, fraud analytics, service development, public policy, optimization, risk management; Communicate results and educate others through reports and presentations.
- Design experiments and analysis to answer targeted questions diverse

DRAFT

subject domains within IRS such as cyber security, fraud analytics, and risk management.

- Lead investigations into data quality and develop methods and techniques to improve the quality of tax and other enterprise data. Develop and plan required analytic projects in response to data science and analysis and clean, massage andanalyze big data using sophisticated analytical and algorithmic techniques.
- Contribute to data mining architectures, modeling standards, reporting and data analysis methodologies.
- Collaborate with stakeholders to integrate data mining results with existing systems and monitor data mining systems performance and implement efficiencyimprovements.
- Adopt an agile mindset and methodology in the development and enhancement of fraud analytics products for fast actions and response time against ongoing fraud threats
- Adopt DevOps/MLOps to increase the speed, efficiency, and quality of software and AI/ML product delivery. Evaluate each project and implement process changes to align with DevOps/MLOps approaches and strategies.
- Demonstrated proficiency in understanding industry best practices and the capability to effectively apply them in relevant scenarios for optimal results.

Specific tools and technologies include, but are not limited to, the following:

- **Methodologies:** Agile, Scrum, SAFe, Six Sigma, Kanban, CRISP-DM, SDLC
- **Web Technologies**: Java, API, SOAP, REST, HTML, Web Services, SOA, Microservices, Flask, JavaScript, JQuery, CSS, REACT
- **Databases & NoSQL**: PostgreSQL, Splunk, Elasticsearch, Redshift
- **Data Analytics**: Python, Scala, SQL, SAS, R, Tableau, Power BI, Kibana, Hadoop, ETL/ELT – Spark, Kafka, EDA, Feature Engineering, AI, ML, NLP, Deep Learning, Active Learning, Predictive Analytics, Data Mining, Linked Analysis, Text Analytics, Simulation, Optimization, Graphic-based Analytics, Data Visualizations
- **Data Management**: Data Governance, Data Architecture, Data Modeling and Design, Data Security, Data Privacy, Data Integration, Business Intelligence (BI), Data Warehousing, Data Lake, Master and Metadata Management, Data Quality, Big Data
- **Cloud Computing**: SaaS, PaaS, IaaS, Microsoft Azure, AWS (EC2, ELB, EBS, S3, VPC, IAM, EMR, Redshift, Glue, RDS, API Gateway, Lambda, CloudWatch, CloudTrail, CloudFront, CloudFormation, Amazon Kinesis, SageMaker, Athena), Hybrid Cloud, Infrastructure-as-Code (IaC), Hybrid Cloud
- **Security & Privacy**: GDPR, FedRAMP, FISAM, Governance, Risk, and

DRAFT

Compliance (GRC), SIEM, Splunk, IAM, Digital Forensics, Auditing, Incident Response, Threat Intelligence, Cloud Security, Zero Trust

- **DevOps & MLOps**: Kubernetes, DBT, GitLab, GitLab CI, Airflow, Linux Shell Scripting

Desired but not required certifications:

- Project Management Professional (PMP)
- Certified Information System Security practitioner (CISSP)
- Any Applicable Data Science/Analytics/AWS Certifications

3.3 DELIVERY

The contractor shall deliver all products concurrently to the IRS Government Technical Monitor (GTM) and the Contracting Officer's Representative (COR). The COR shall notifythe contractor whether the formal deliverable has been accepted or provide written comments within ten (10) government workdays of receipt. Contractor shall then resubmit the final deliverable within ten (10) government workdays to the IRS GTM andthe COR, if necessary. All documents shall be provided in electronic format to the IRS using Microsoft Word, Excel, PowerPoint and/or Visio using the IRS' standard document templates.

Documents shall be submitted electronically whenever possible. Hardcopies shall be provided upon request. Section 3.16 below, outlines the report/delivery schedule for support.

3.3.4 QUALITY ASSURANCE FOR DELIVERABLE SUBMISSION

All deliverables shall meet requirements as described under the tasks in clear, concise,well- written language, and in accordance with this Performance Work Statement. Accordingly, the quality measures (acceptance criteria) as set forth below shall be applied to each work product or deliverable received from the contractor under this Performance Work Statement.

- Completeness - Initial requirements (as identified) are satisfied in all sections. Each deliverable must encapsulate all the algorithms, methodologies, datasets, equations, and topics as dictated by the specified tasks. Any missing components, data, or explanations shall necessitate revision or might lead to rejection.
- Accuracy - Documents shall be accurate in presentation, technical content, and adherence to accepted elements of style. Algorithms, equations, and statistical methods presented in the deliverables must be technically sound and valid. Data utilized or provided shall be cleaned, validated, and free from inconsistencies or errors. Erroneous or misinterpreted data shall mandate immediate rectification.
- Clarity - Documents shall be clear and concise; project management and terms shallbe used, as appropriate. All diagrams shall be easy to

DRAFT

understand and be relevantto the supporting narrative. Complex concepts, algorithms, and methodologies shall be elucidated with utmost clarity, ensuring comprehensibility even to those not deeply versed in the topic.

- Rigor – Mathematical notations and conventions must remain consistent throughout. Proper citations for borrowed or adapted methodologies or algorithms shall be provided.
- Specification Validity - All deliverables must satisfy the requirements of the U.S. government as specified herein. Deliverables shall correlate seamlessly with the project's technical and analytical specifications mentioned in the performance work statement. Software or code shall adhere to industry standards, be well-commented, and maintainable.
- File Editing - All documents shall be provided in electronic format to the IRS using Microsoft Word, Excel, PowerPoint, Vizio, or other mutually agreeable method. Deliverables, especially code and datasets, shall be in formats that facilitate easy editing and replication of results. This includes but isn't limited to providing Jupyter notebooks, Python scripts, or other relevant formats with associated data files.
- Format - Documents shall be submitted electronically whenever possible. Hardcopies shall be provided upon request. The documents format may change from Subtask to Subtask.
- Timeliness - Deliverables shall be submitted on or before the due date specified inthe Deliverables Section, 3.15, of this PWS or submitted in accordance with a laterscheduled date determined solely by the government. All computational results, analyses, documents, and other deliverables must be proffered within the designated timeframe as outlined in the performance work statement. Delays beyond stipulated deadlines might be penalized as delineated in the contract. The contractor acknowledges the imperative nature of these quality measures and acceptance criteria, especially in the nuanced fields of computer science, statistics, and data science. Non-conformity to these standards may lead to deliverable rejection, mandating the contractor to provide revisions at their own expense until the stipulated criteria are met.

3.3.4 REVIEW OF DELIVERABLES

The government shall perform an initial review of deliverables detailed in section 3.16.If problems are encountered during the deliverable review, the contractor must correctthem. If necessary, a meeting may be convened to resolve any differences. The contractor shall make all required changes to achieve an acceptable deliverable. The government shall perform its review within approximately 15 calendar days from receiptof the deliverable or as otherwise specified in each task order.

- When the review of a deliverable results in necessary modifications, the government shall, in accordance with the approved task order schedule, provide thenecessary documentation to correct the deliverable. It shall then

DRAFT

be the responsibilityof the contractor to properly and consistently incorporate the comments in the finalproduct.

- The contractor shall develop and provide monthly reports on Fraud Analytics findings.
- The contractor shall provide a draft Knowledge Transfer Plan (KTP) to the government within the first 15 business days after award to identify the contractorresources and roles involved in the transfer process, provide a list of risks and mitigation strategies for the transfer, and contain a detailed resource balanced project schedule developed with Microsoft Project. The project schedule (Integrated Master Schedule) shall identify tasks, dependencies, deliverables, andmilestones. The project schedule shall be at a sufficient level of detail to track progress on a bi-weekly basis, (i.e., all tasks shall be detailed to a level such that no task has duration of more than ten workdays).
- These procedures shall not be construed to constitute a waiver on the part of the government of its rights under FAR Subpart 49.4, entitled "Termination for Default,"nor of any other rights or remedies provided by law or under this contract.

3.4 PLACE OF PERFORMANCE

The work location is at the discretion of the government lead. The primary work location is on-site, and the lead may approve the option to work from the contractor's site and other remote locations.

X **Government's site (Primary Location)**

X **Contractor's site**, with reasonable access to government site *(contractor personnel can travel to government site for meetings within two hours' notice and at reasonabletravel costs.*)

The government site is located at: New Carrollton Federal Building, 5000 Ellin Road, Lanham, MD 20706.

3.5 PERIOD OF PERFORMANCE, CONTRACT TYPE, AND KEY PERSONNEL

3.5.4 PERIOD OF PERFORMANCE

The period of performance for this Task Order is 12 months from the effective date ofthe Task Order award with four (4) 12-month option periods. (See Section 3.19 for the High-Level Project Schedule).

12-month base year period and four 12-month option periods:

- Base Year (12-months) October 31, 2024 – October 30, 2025
- Option Period 1 (12-months) October 31, 2025 – October 30, 2026
- Option Period 2 (12-months) October 31, 2026 – October 30, 2027
- Option Period 3 (12 months) October 31, 2027 – October 30, 2028
- Option Period 4 (12 months) October 31, 2028 – October 30, 2029
- ❖ The dates listed above are for estimation to identify the length of time. The start date can be adjusted to fit the government's transition need after discussion with the (apparent successful) contractor.

DRAFT

3.5.4 CONTRACT TYPE

This is a Hybrid contract type consisting of Firm Fixed Price (FFP) and Labor Hour CLINs. This contract includes Option Years and a Support CLIN.

3.5.4 PERSONNEL REQUIREMENT FOR KNOWLEDGE/EXPERIENCE

The skill sets provided for in this PWS must be commensurate with the labor categories listed in the table in Section 5.0. In addition, due to the highly complex and significant risk profile to the IRS, it is required that key personnel must demonstrate that they have experience of similar scope and scale to the IRS fraud analytics program and 75% of the resources required to support Tasks 1 and 2 must be staffed from the vendors current employees. This eliminates the risk associated with a contractor staffing this high-impact Cybersecurity program with newly recruited personnel that have not been evaluated for a minimum of one-year by the contractor. Failure to acknowledge this requirement would result in a failure to comply with the intent and requirement of this PWS to obtain experienced, highly skilled personnel with demonstrated experience in fraud analytics.

The offeror shall identify, (in their quote based on information provided in the table below), certain positions or roles and associated labor categories considered to be Key Positions based on their proposed solution. The contractor shall submit the name and resume of the contractor employee proposed in each Key Position.

Contractor employees identified as Key Personnel shall be dedicated to this project. If any changes in proposed key personnel become necessary during actual performance, the contractor shall provide written notification 60 days in advance. In the event of a sudden change in key personnel (death, incapacitation, immediate termination, etc.), the contractor shall provide written notice to the CO within 3 calendar days of the event. For any substitution, the contractor shall submit a justification with a proposed substitute whose qualifications are equal to or greater than the person being replaced, along with a 1 to 2-page introductory summary, in sufficient detail to permit evaluation within 10 calendar days of notification of a substitution.

3.5.8.1 KEY PERSONNEL

The government has identified certain roles in the below table as Key personnel. The contractor shall submit the resumes (certified by their respective manger) of thecontractor employee(s) that shall fill the position(s) identified in the following table. Resumes shall demonstrate that proposed key personnel possess skill and experience as described at PWS Section 3.3.10, “Skill Requirements.”

DRAFT

Role	Labor Category
Manager	Managers, All Other (11-9199)
Technical Lead/Watch Commander	Computer & Information Research Scientists (15-1111)
Technical Lead/Lead Data Scientist	Computer & Information Research Scientists (15-1111)

3.6 PERFORMANCE REQUIREMENTS, STANDARDS AND SURVEILLANCE

The government has determined there is value in incorporating Performance-BasedService Acquisition (PBSA) methodology with an outcomes-based focus for this work. Section 3.19 defines the High-Level Project Schedule. Deliverables are listed in the tablesunder section 3.16. Exhibit 1 of the QASP defines the government's Desired PerformanceStandards, Acceptable Quality Levels and Monitoring Methods for each sub-task and deliverable included in this Task Order.

3.6.4 FRAUD ANALYTICS AND MONITORING PERFORMANCE REQUIREMENTS

Performance requirements include in Exhibit 2 QASP are: Performance RequirementSummary, Standards/AQLs, and Incentive/Remedy which are defined by the government. Exhibit 1 of the QASP defines the desired outcomes as successfully completing specified Sub-tasks including all deliverables, work products and support.This aligns the contractor's objectives with the government objectives, which are to successfully complete the Sub-tasks and deliver value-added products and services to the end users.

3.6.4 FRAUD ANALYTICS AND MONITORING PERFORMANCE STANDARDS

Performance Standards have been identified in Exhibit 2 of the QASP for each of theSub-tasks.

3.6.4 FRAUD ANALYTICS AND MONITORING SURVEILLANCE

The surveillance process has two interrelated parts: The Quality Assurance Surveillance Plan (QASP) included as Section 4.1. The contractor shall establish andmaintain a complete Quality Control Plan (QCP) in accordance with Section 7 of the QASP. This links the government and contractor's quality assurance efforts into an integrated package with shared objectives.

3.7 GOVERNMENT-FURNISHED PROPERTY (GFP)

The government may provide any GFP to the contractor during the orientation briefing. GFP *(to include material, equipment, and/or information)* may be provided in the performance of this task order:

DRAFT

ITEMS	QUANTITY
Contractor Identification Badge	1 Per
Contractor Building Access/Proximity Card	1 Per
Desktop/Laptop Computer with Local Area Network Access	1 Per
Microsoft Office	1 Per
Office Space (Desk, Chair, Standard Office Equipment)	TBD
Desktop telephone device with VMS	TBD

3.8 GOVERNMENT-FURNISHED INFORMATION

GFI *(to include manuals, notes, memos, instruction materials and other information)* maybe provided in the performance of this task order. The following GFI shall be provided to the contractor upon task order award.

INFORMATION ITEMS
Power Points that provide background knowledge on the development of the effort.
Dashboards that are used by 24x7 team to monitor data in near-real time
Access to the team SharePoint Site

At the end of this task order, disposition of GFI shall be in accordance with FAR 52.245.5.

3.9 TRAVEL

For any trip to be authorized, the COR must approve such travel in writing and in advance.Tasks contemplating travel shall have a specific CLIN. Travel and per diem shall be reimbursed at actual cost in accordance with the limitations set forth in FAR 31.205-46 and the General Services Administration's Federal Travel Regulations. Profit shall not beapplied to the travel costs. Local travel may be required for on-site meetings, etc.

The contractor shall provide a travel voucher statement for all travel. The voucher shall ensure verification of costs incurred for travel under the contract is both allowable and reasonable and in accordance with the regulation FAR 31.205.46. The contractor shall attach the voucher and receipts to the monthly invoice.

3.10 OPERATING HOURS, GOVERNMENT CLOSURES

Unless specified elsewhere in this PWS, at a minimum, the contractor shall provide coverage between the hours of 8:30 AM to 5:00 PM, Monday thru Friday (less Federal holidays). The IRS reserves the right to increase/decrease these hours as workload fluctuates.

Holidays: Unless required under the terms of the contract or authorized by the CO, thecontractor shall not work at any government facility, nor shall any deliveries under this contract be made to any government facility, on any of the

DRAFT

following holidays:

- New Year's Day January 1
- Martin Luther King's Birthday 3rd Monday in January
- Washington's Birthday 3rd Monday in February
- Memorial Day last Monday in May
- Juneteenth National Independence Day June 19
- Independence Day July 4
- Labor Day 1st Monday in September
- Columbus Day 2nd Monday in October
- Veterans' Day November 11
- Thanksgiving Day 4th Thursday in November
- Christmas Day December 25
- Any other day designated by Federal Statute, Executive Order or aPresidential proclamation.

When a holiday falls on a Sunday, the following Monday shall be observed as a legal holiday. When a holiday falls on a Saturday, the preceding Friday is observed as a holidayby U. S. government agencies.

The amounts in schedule of the contract include an allowance for holidays to be observed.The government shall not be billed for such holidays, except when services are required by the government and are performed on a holiday.

When the government grants administrative leave to government employees, or is closedbecause of inclement weather, potentially hazardous conditions, or other special circumstances, contractor personnel working at the specific facility/location grantedadministrative leave shall also be dismissed.

3.11 CONTRACTOR REPORTS

Reports shall be at the following level *(check only one)*:

☐ Task Order (least detailed)

☒ Sub-Task (more detailed)

For specific reports provided as scheduled deliverable(s) refer to Section 4.2 for specificdescriptions, performance requirements, and standards.

3.12 ACCESS TO GOVERNMENT PROPERTY AND FACILITIES

The contractor shall be allowed limited access to the government's property and facilities,as detailed in the sections below.

3.12.4 SECURITY

The U.S. Federal Government shall conduct background checks and verify informationsubmitted by the employees, conduct fingerprint checks, and conduct other appropriate investigations. Investigations shall include, but are not limited to, criminal record, credit worthiness, and prior work performance history. The contactor shall coordinate with the assigned COR to process background investigations for contractorstaff supporting this effort and

DRAFT

complete annual UNAX training and certification, and other annual contractor training required by the government.

The contractor shall comply with all information technology system security policies and procedures that apply to IRS. All personnel providing services under the resultantTask Orders must meet all requirements to successfully complete the screening process. All contractor personnel providing support must achieve the basic screeningprocess in order to work on-site.

All contractor employees, providing support under the task order, shall complete Unauthorized Access (UNAX) and IT Security Training annually. In addition, each individual contractor employee shall sign a non-disclosure form. The contractor shall conduct Disclosure Awareness training prior to giving officers and employees accessto the SBU data and annually thereafter if the order is renewed or extended. Each participant must sign and date the training roster. The contractor shall provide written certification to the COR that this training was held.

Due to the requirement for continuous availability of the system, contractor resourcesassigned to the Task Order shall have approved Moderate Background Investigations(MBIs).

Under FISMA, government employees and contractors are subject to Federal information security laws, regulations and policies, including annual security awareness training. This training requirement is satisfied by the IRS mandatory Information Protection briefing, which covers computer security, disclosure, privacy, and UNAX

A. DISCLOSURE AWARENESS TRAINING
IRS conducts a series of security awareness training; in particularly the UnauthorizedAccess (UNAX) training and Computer Security Awareness training, which is conducted annually and mandatory for all IRS employees and contractors. To reduceinformation security risks, FISMA requires continuous security awareness training onagency guidance, policies and procedures for personnel, including contractors, otherusers, and individuals with significant IT Security responsibilities that support the operations and assets of the agency.

The contractor shall comply with IRS mandatory annual Computer Security Awareness and UNAX briefing requirements and receive an initial orientation before being allowed access to IRS Information Systems. All contractors and contractor employees who are involved with the management, use, programming or maintenance of IRS information systems must complete the IRS mandatory ComputerSecurity briefing. All contractors and contractor employees who could have access toreturn information must complete the mandatory UNAX briefing. Contractors shall certify the completion of training by their employees annually. The certification shall be submitted to the contracting officer, with a copy to the COR.

B. NON-DISCLOSURE AGREEMENT
The contractor shall comply with Department of Treasury Directive TD P 85-01, Treasury Security Manual TDP 71-10, and Internal Revenue Manual

10.8.1 Information Technology Security Policy and Guidance. The contractor shall comply with IRS Internal Revenue Manuals (IRM) and Law Enforcement Manuals (LEM) whendeveloping or administering IRS information and information systems.

The contractor shall be required to sign the “Non-Disclosure Agreement Form,” TDP 71-10, prior to rendering services. The contractor shall submit the signed form to the COR.

3.13 CONTRACT ADMINISTRATION DATA

- **The CO for this requirement is:**
  Name:
  Address:
  Email:
  Voice:

- **The COR for this requirement is:**
  Name:
  Address:
  Email:
  Voice:

- **Fraud Analytics Government Program Manager (PM) Points of Contact:**
  Name: John Dunnivan
  E-mail: john.r.dunnivan@irs.gov
  Telephone:

3.14 SHIP TO

Unless otherwise specified, all deliverables/work products shall be provided to the COR no later than 4:00 p.m. local time on the date(s) specified in the task order.

3.15 DELIVERABLES

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 contractor shall adhere to Section 508 of the Rehabilitation Act of 1973, which requires access to the Federal Government electronic and information technology.

The law applies to all Federal agencies when they develop, procure, maintain, or use electronic and information technology. Federal agencies must ensure that this technologyis accessible to employees and members of the public with disabilities. http://www.section508.gov/.

Each Electronic and Information technology product or service furnished under this contract shall comply with the Electronic and Information Technology (EIT)

DRAFT

Accessibility Standards (29 U.S.C. *&794(d)) this includes all task/delivery orders and product supportservices furnished in the performance of this contract.

For every EIT product or service accepted under this contract by the government that does not comply with (29 U.S.C. *&794(d)), the contractor shall at the discretion of the government, make every effort to replace or upgrade it with a compliant equivalent product or service, if commercially available and cost neutral, on either the planned refresh cycle of the product or service, or on the order renewal date, whichever shall occurfirst."

The contractor shall refer to tables 3.16.1 and 3.16.2 for due dates of the reports referenced in section 3.16 Delivery Schedule. Unless otherwise requested in writing by the COR, work products shall be produced using Microsoft Office Professional products, as applicable, and all work products shall be submitted via electronic delivery unlessotherwise instructed.

3.15.4 TASK 1: FRAUD ANALYTICS AND MONITORING COMMON PROJECT TASKS (FFP)

Number	Name	Frequency	Quantity
3.16.1.1	Orientation Briefing: A PowerPoint presentation that defines what, how, and when the contractor proposes to fulfill the PWS requirements.	5 days following award	1
3.16.1.2	Program Management Skills Requirement Validation Report: Demonstrate, through a skills requirement validation report, that necessary Program Management, Security Threat Collaboration, and IEP Integration expertise has been satisfactorily aligned to the government's requirement contained in this PWS.	30 days following award	1
3.16.1.3	Baseline Financial Forecast and Budget Tracking Report: Baseline expenditures plan aligned to all sub-tasks within this PWS and subsequent contract modifications shall be monitored monthly in deliverable 3.16.2.1.5 below.	30 days following award	1

DRAFT

3.16.1.4	QCP: Provide written proposed QCP to ensure that the PWS requirements are provided as specified. The QCP shall describe methods for identifying and preventing problems before performance levels become unacceptable. The QCP shall be discussed at the Orientation Briefing (see Section 3.19).	45 days following award	1
3.16.1.5	Monthly Financial Forecast: Tracking of expenditures against actuals and budget projections by Sub-Task.	1st Tue of every month	1

3.15.4 TASK 2: FRAUD ANALYTICS AND MONITORING HIGHLY SPECIALIZED TASKS (T&M)

3.15.7.1 SECURITY THREAT COLLABORATION AND APPLICATION INTEGRATION

Number	Name	Frequency	Quantity

DRAFT

3.16.2.1.1	Baseline Threat Collaboration with CSP/SADI/Portal/Backend applications.: Baseline strategy for integrating new and existing capabilities to identify and mitigate new threats, and establish processes to routinely communicate and collaborate with stakeholders.	30 days following award	1
3.16.2.1.2	: Monthly reporting of enhancements to cybersecurity leadership and/or stakeholders to include, but not be limited to, new and emerging techniques to address fraud detection/remediation capabilities a. Ensure that all delivered capabilities strictly adhere to the Enterprise Life Cycle (ELC) standards and best practices, ensuring alignment with the Agency's objectives and operational requirements. b. Furnish the Agency with the complete source code for all software components developed, modified, or otherwise used in the delivered capabilities. The Contractor is bound by FAR 52.227-14 – "Rights in Data – General," to ensure that the Government has rights to use, reproduce, and disclose the source code as deemed necessary. c. Provide comprehensive and clear documentation that covers all aspects of the delivered capabilities. This documentation shall include but is not limited to system architecture, user manuals, installation guides, and troubleshooting references. Adherence to FAR 52.212-4 – "Contract Terms and Conditions—Commercial Items," especially the subparagraph on 'Technical Data', is imperative to ensure proper transfer of knowledge and information. d. Shall there be any updates, modifications, or expansions of the capabilities, the Contractor must promptly provide updated source code and relevant documentation. e. The execution of this clause is subject to quality assurance procedures and reviews, as outlined in FAR Part 46 – "Quality	1st Tue of every month	1

DRAFT

	Assurance," to ensure compliance with ELC standards and documentation requirements.		

3.15.7.2 NEAR REAL-TIME FRAUD ANALYTICS AND MONITORING

Number	Name	Frequency	Quantity
3.16.2.2.1	Weekly Near Real-Time Fraud Analytics Monitoring Report: Status Report to include a task order deliverable summary, work accomplished during reporting period, issues, and work planned for next period	2nd Tuesday following contract award; Every Tuesday thereafter	1
3.16.2.2.2	Near Real-Time Fraud Analytics Monitoring Skills Requirement Validation Report: Demonstrate, through a skills requirement validation report, that necessary Near Real-Time Fraud Analytics Monitoring expertise has been satisfactorily aligned to the government's requirement contained in this PWS.	30 days following contract award	1

3.15.7.3 ENTERPRISE IT EVENT MANAGEMENT AND COORDINATION

Number	Name	Frequency	Quantity
3.16.2.3.1	Weekly Enterprise IT Event Management and Coordination Report: Status Report to include a task order deliverable summary, work accomplished during reporting period, issues, and work planned for next period	2nd Tuesday following contract award; Every Tuesday thereafter	1

DRAFT

3.16.2.3.2	Enterprise IT Event Management and Coordination Skills Requirement Validation Report	30 days following contract award	1
3.16.2.3.3	Weekly status report of development of analytics products including data models and analytic tools and frameworks	2nd Tuesday following contract award; Every Tuesday thereafter	1

3.15.7.4 CLOUD MIGRATION AND PLATFORM ADVISORY SERVICES

Number	Name	Frequency	Quantity
3.16.2.4.1	Cloud Services Report shall be requested: Status Report to include a task order deliverable summary, work accomplished during reporting period, issues, and work planned for next period Weekly Platform Advisory Services Report: Status Report to include a task order deliverable summary, work accomplished during reporting period, issues, and work planned for next period	2nd Tuesday following contract award; Every Tuesday thereafter	1
3.16.2.4.2	Platform Advisory Services Skills Requirement Validation Report: Demonstrate, through a skills requirement validation report, that the following technology skillsets are provided, ETL, big-data programming/analytics, and data integration lead expertise have been satisfactorily aligned to the government's requirement contained in this PWS.	30 days following contract award	1

3.15.7.5 OPTIONAL TASK SURGE SUPPORT FRAUD ANALYTICS (LH)

DRAFT

3.16.2.5.1	If this optional CLIN is executed a weekly Surge Support Services Report shall be requested: Status Report to include a task order deliverable summary, work accomplished during reporting period, issues, and work planned for next period.	2nd Tuesday following contract award; Every Tuesday thereafter	1

3.15.7.6 SUPPORT STAKEHOLDERS IN THE DEVELOPMENT OF CREDENTIAL SERVICE PROVIDER REQUIREMENTS RELATED TO FRAUD AND IDENTITY THEFT (LH)

3.15.2.7.1	If this optional CLIN is executed a Bi-weekly Stakeholder CSP Services Report shall be requested: Status Report to include a task order deliverable summary, work accomplished during reporting period, issues, and work planned for next period. In addition, deliver documents to CSPs and IRS stakeholders on-demand regarding data requirements, risk assessment, fraud mitigation strategy recommendations, table-top exercises assessments, and TIGTA inquiries/audits. The documents shall be clear, free of errors, logical, consistent and easy to understand for non-technical audiences. The Contractor shall not merely provide a theoretical or paper-based representation of the product. Instead, they are required to deliver a functional product that has been thoroughly tested, validated, and meets the operational needs as specified in this contract. In ensuring these objectives: a. The Contractor must adhere to FAR 46.5 – "Acceptance," whereby products shall undergo inspection and tests required to ensure conformance with contract specifications. b. The delivered product must demonstrate practical usability and shall be accompanied by live demonstrations, validations, or tests,	2nd Tuesday following contract award; Every Tuesday thereafter	1

DRAFT

	as appropriate. Evidence of these sessions, which shall be witnessed by representatives of the Agency, must be maintained and made available upon request. c. The Contractor is bound by FAR 52.246-2 – "Inspection of Supplies—Fixed-Price" to ensure the furnished final product conforms to contract requirements and to remedy any discrepancies in accordance with the clause. d. The product shall be bolstered by tangible results, including user feedback, performance benchmarks, and other metrics that confirm its efficacy and functionality in real-world scenarios. e. In the event of performance issues or discrepancies, the Contractor is responsible, at their own expense, for prompt rectifications in accordance with FAR 52.246-8 – "Inspection of Research and Development—Fixed-Price." f. The Contractor must provide comprehensive training, documentation, and knowledge transfer sessions, ensuring that the Agency personnel are equipped to deploy, use, and maintain the product effectively. g. All deliverables and the execution of this clause are subject to the quality assurance and inspection terms set forth in FAR Part 46 – "Quality Assurance."		

3.16 DELIVERY SCHEDULE

The work products and deliverables are listed in Section 3.15 of this PWS. The high-level project schedule is listed in Section 3.18.

3.17 RAMP-UP PERIOD

The contractor's Orientation Briefing shall include a Staffing Plan to demonstrate how they shall ramp up staffing to immediately begin supporting the work described in the PWSat Task Order award and how they shall accomplish the process to ensure all proposed staff achieves Final Staff-Like Access approval within no more than 45 days of award. The IRS clearance process is expected to require 30-45 days from the accurate submission of the required background investigation documents and completion of other requirements (e.g., timely fingerprinting) by the contractor. Due to this process, partial billing of FFP work efforts described above, shall occur for any contractor personnel not cleared by the IRS to work on the contract as required by IRS policy.

DRAFT

The COR designation shall be identified by the CO's written designation memo. The CO shall identify the COR via e-mail to the contractor.

3.18 HIGH LEVEL PROJECT SCHEDULE

The schedule, in the table below, represents estimated dates that shall be used for planningpurposes. The key to award shall be successful completion of the sub-task deliverables.All deliverables listed in Section 3.15 of this PWS, "Deliverables" shall be incorporated into this high- level project scheduled based on the weekly, monthly, or otherwise scheduled timeframe.

ID#	Service	Standard
1	Orientation Briefing	5 days after award
2	Program Management Skills Requirement Validation Report	30 days after award
3	Baseline Financial Forecast andBudget Tracking Report	30 days after award
4	Quality Control Plan	45 days after award
5	Monthly Financial Forecast and Budget Tracking Report	Monthly
6	Baseline Threat Collaboration and IEP Integration Strategy	30 days after award
7	Monthly Threat Collaboration and IEP Integration Enhancement Reporting	1st Tue of every month

4.0. DELIVERY AND PERFORMANCE INFORMATION

4.1. Quality Assurance Surveillance Plan (QASP)

Support Services for Fraud Analytics and Monitoring Capabilities

This QASP is pursuant to the requirements listed in the performance work statement (PWS) entitled Support Services Fraud Analytics and monitoring Capabilities. This plan sets forth the procedures and guidelines IRS Cybersecurity shall use in ensuring the required performance standards or services levels are achieved by the contractor.

The QASP shall be used as a government document to enforce the inspection and acceptance of the Task Order. The QASP describes the mechanism for documenting noteworthy accomplishments or discrepancies for work performed by the contractor.

DRAFT

Information generated from the IRS Project Management Office (PMO) surveillance activities shall directly feed into the PMO performance discussions with the contractor.

The QASP can be changed/updated, etc. It is intended to be a “living” document that shall be revised or modified as circumstances warrant. Either the contractor or the government may initiate changes to the QASP. Bilateral changes may be made to the plan at any time during contract performance. Such changes shall not entitle the contractor to any equitable adjustments or to any other compensation for performance in a prior period. The contractor is responsible and shall manage and ensure that quality controls meet the terms of the Task Order.

4.1.1. Purpose

4.1.1.1. The purpose of the QASP is to describe the systematic methods used to monitor performance and to identify the required documentation and the resources to be employed. The QASP provides a means for evaluating whether the contractor is meeting the performance standards/quality levels identified in the PWS and the contractor’s QCP, and to ensure that the government pays only for the level of services received.

4.1.1.2 This QASP defines the roles and responsibilities of all members of the integrated project team (IPT), identifies the performance objectives, defines the methodologies used to monitor and evaluate the contractor’s performance, describes quality assurance documentation requirements, and describes the analysis of quality assurance monitoring results. The QASP details how and when the IRS PMO shall monitor, evaluate and document contractor performance with regards to the PWS.

The QASP is intended to accomplish the following:

1) Define the role and responsibilities of participating government officials.
2) Define the key deliverables that shall be assessed.
3) Describe the rating elements and the evaluation method that shall be employedby the government in assessing the contractor’s performance.
4) Provide copies of the performance assessment form(s) that the government shall use in documenting and evaluating the contractor’s performance.
5) Describe the process of performance assessment documentation.

4.1.2 Performance Management Approach

4.1.2.1 The PWS structures the acquisition around “what” service or quality level is required, as opposed to “how” the contractor shall perform the work (i.e., results, not compliance). This QASP shall define the performance management approach taken by IRS Cybersecurity Fraud Analyticsto monitor and manage the contractor’s performance to ensure the expected outcomes or performance objectives communicated in the PWS are achieved. Performance management rests on developing a capability to review and analyzeinformation generated through performance assessment. The ability to make decisions based on the analysis of performance data is the cornerstone of

DRAFT

performance management; this analysis yields information that indicates whether expected outcomes for the project are being achieved by the contractor.

4.1.2.2 Performance management represents a significant shift from the more traditional quality assurance (QA) concepts in several ways. Performance management focuses on assessing whether outcomes are being achieved and to what extent. This approach migrates away from scrutiny of compliance with the processes and practices used to achieve the outcome. A performance-based approach enables the contractor to play a large role in how the work is performed, as long as the proposed processes are within the stated constraints. The only exceptions to process reviews are those required by law (federal, state, and local) and compelling business situations, such as safety and health. A “results” focus provides the contractor flexibility to continuously improve and innovate over the course of the contract as long as the critical outcomes expected are being achieved and/or the desired performance levels are being met.

4.1.3 Performance Management Strategy

4.1.3.1 The contractor is responsible for the quality of all work performed. The contractor measures that quality through the contractor’s own quality control (QC) program. QC is work output, not workers, and therefore includes all work performed under this contract regardless of whether the work is performed by contractor employees or by subcontractors. The contractor’s QCP shall set forth thestaffing and procedures for self-inspecting the quality, timeliness, responsiveness,customer satisfaction, and other performance requirements in the PWS. The contractor shall develop and implement a performance management system with processes to assess and report its performance to the designated government representative. The contractor’s QCP shall set forth the staffing and procedures forself-inspecting the quality, timeliness, responsiveness, customer satisfaction, andother performance requirements in the PWS. This QASP enables the governmentto take advantage of the contractor’s QC program.

4.1.3.2 The government representative(s) shall monitor performance and review performance reports furnished by the contractor to determine how the contractor is performing against communicated performance objectives. The government shallmake determination regarding incentives based on performance measurement metric data and notify the contractor of those decisions. The contractor shall be responsible for making required changes in processes and practices to ensure performance is managed effectively.

4.1.4 Roles and Responsibilities

4.1.4.1 The Contracting Officer

The Contracting Officer (CO) is responsible for monitoring contract compliance, contract administration, and cost control and for resolving any differences between the observations documented by the Contracting Officer’s Representative (COR) or Program Manager (PM) and the contractor. The CO shall designate one full-

DRAFT

timeCOR as the government authority for performance management. The number of additional representatives serving as technical inspectors depends on the complexity of the services measured, as well as the contractor's performance, andmust be identified and designated by the CO.

4.1.4.2 The Contracting Officer's Representative

In accordance with DTAR clause 1052.201-70, the COR is designated in writing by the CO to act as his or her authorized representative to assist in administering a contract. COR limitations are contained in the written appointment letter. The COR is responsible for administration of the project and ensures proper government surveillance of the contractor's performance. The COR is not empowered to make any contractual commitments or to authorize any contractual changes on the government's behalf. Any changes that the contractor deems may affect contract price, terms, or conditions shall be referred to the CO for action. The COR shall have the responsibility for completing QA monitoring forms used to document the inspection and evaluation of the contractor's work performance. Government surveillance may occur under the inspection of services clause for any service relating to the contract.

4.1.5. Identification Of Required Performance Standards/Quality Levels

The required performance standards and/or quality levels are included in Exhibit 1 of this QASP. If the contractor meets the required service or performance level, it shall bepaid the monthly amount agreed on in the contract. Failure to meet the required service or performance level shall result in a deduction from the monthly amount.

4.1.6. Methodologies To Monitor Performance

4.1.6.1 Surveillance Techniques

To minimize the performance management burden, simplified surveillance methods shall be used by the government to evaluate contractor performance when appropriate. The primary methods of surveillance are:

- Random monitoring, which shall be performed by the COR designated inspector.
- 100% Inspection – Each month, the COR, shall review the generated documentation and enter summary results into the Surveillance Activity Checklist.
- Periodic Inspection – COR typically performs the periodic inspection monthly.

4.1.6.2 Customer Feedback

The contractor is expected to establish and maintain professional communication between its employees and customers. The primary objective of this communication is customer satisfaction. Customer satisfaction is the most significant external indicator of the success and effectiveness of all services provided and can be measured through customer complaints.

DRAFT

Performance management drives the contractor to be customer focused through initially and internally addressing customer complaints and investigating the issues and/or problems but the customer always has the option to communicate complaints to the COR, as opposed to the contractor.

Customer complaints, to be considered valid, must set forth clearly and in writing the detailed nature of the complaint, must be signed, and must be forwarded to the COR. The COR shall accept those customer complaints and investigate using the Quality Assurance Monitoring Form – Customer Complaint Investigation, identifiedin Exhibit 2 of this QASP.

Customer feedback may also be obtained either from the results of formal customer satisfaction surveys or from random customer complaints.

4.1.6.3 Acceptable Quality Levels

The acceptable quality levels (AQLs) for contractor performance are structured to allow the contractor to manage how the work is performed while providing negative incentives for performance shortfalls. For certain critical activities, the desired performance level is established at 100 percent. Other levels of performance are keyed to the relative importance of the task to the overall mission performance, as defined by the Program Manager.

4.1.7. Quality Assurance Documentation

4.1.7.1 The Performance Management Feedback Loop

The performance management feedback loop begins with the communication of expected outcomes. Performance standards are expressed in Exhibit 1 to this QASP.

4.1.7.2 Monitoring Forms

The government's QA surveillance, accomplished by the COR or PM, shall be reportedusing the monitoring forms in Exhibit 2 of this QASP. The forms, when completed, shalldocument the government's assessment of the contractor's performance under the contract to ensure that the required results are being achieved. The COR shall retain a copy of all completed QA surveillance forms.

4.1.8. Analysis of Quality Assurance Assessment

4.1.8.1 Determining Performance

4.1.8.2 Government shall use the monitoring methods cited to determine whether the performance standards/service levels/AQLs have been met. If the contractor has not met the minimum requirements, it may be asked to develop a corrective action plan to show how and by what date it intends to bring performance up to the required levels.

4.1.8.2 Reporting

DRAFT

At the end of each month, the COR shall prepare a written report for the PM summarizing the overall results of the quality assurance surveillance of the contractor's performance. This written report, which includes the contractor's submitted monthly report and the completed quality assurance monitoring forms (Exhibit 2 of this QASP), shall become part of the QA documentation. It shall enable thegovernment to demonstrate whether the contractor is meeting the stated objectives and/or performance standards, including cost/technical/scheduling objectives.

4.1.8.3 Reviews and Resolution

4.1.8.3.1 The COR may require the contractor's project manager, or a designated alternate, to meet with the PM and other government personnel as deemed necessary to discuss performance evaluation. The COR shall define a frequency ofin-depth reviews with the contractor, including appropriate self-assessments by thecontractor; however, if the need arises, the contractor shall meet with the PM as often as required or per the contractor's request. The agenda of the reviews may include:

4.1.8.3.2

- Monthly performance assessment data and trend analysis
- Issues and concerns of both parties
- Projected outlook for upcoming months and progress against expected trends,including a corrective action plan analysis
- Recommendations for improved efficiency and/or effectiveness

4.1.8.3.3 The QAR must coordinate and communicate with the contractor to resolve issues and concerns regarding marginal or unacceptable performance.

4.1.8.3.4 The COR, PM and contractor shall jointly formulate tactical and long-term courses of action. Decisions regarding changes to metrics, thresholds, or service levels shall be clearly documented. Changes to service levels, procedures, and metrics shall be incorporated as a contract modification at the convenience of the PCO/ACO.

5.0. LABOR CATEGORIES AND DESCRIPTIONS

As a hybrid FFP/T&M contract, this section specifies the government's required hours by labor category along with the expected experience/skills to effectively perform the task listed below. These labor categories and skillset requirements are applicable to both FFP and T&M tasks. The labor categories and skillsets follow the Office of Management and Budget's (OMB) Standard Occupational Classification (SOC) for which the Bureau of Labor Statistics (BLS) maintains compensation data. Labor categories are further defined as Junior, Journeyman, and Senior based on years of experience, education, and duties/responsibilities as follows:

- JUNIOR: A Junior labor category has up to 3 years of experience and a BA/BS degree. A Junior labor category is responsible for assisting more senior positions and/or

DRAFT

performing functional duties under the oversight of more senior positions.

- JOURNEYMAN: A Journeyman labor category has 3 to 10 years of experience and a BA/BS or MA/MS degree. A Journeyman labor category typically performs all functional duties independently.
- SENIOR: A Senior labor category has over 10 years of experience and a MA/MS degree. A Senior labor category typically works on high-visibility or mission critical aspects of a given program and performs all functional duties independently. A Senior labor category may oversee the efforts of less senior staff and/or be responsible for the efforts of all staff assigned to a specific job.
- SUBJECT MATTER EXPERT (SME): A Subject Matter Expert is an individual whose qualifications and/or particular expertise are exceptional and/or highly unique. Subject Matter Experts do not have specific experience/education qualifications but are typically identified as recognized Industry leaders for a given area of expertise. Subject Matter Experts typically perform the following kinds of functions: Initiates, supervises, and/or develops requirements from a project's inception to conclusion for complex to extremely complex programs; Provides strategic advice, technical guidance and expertise to program and project staff; Provides detailed analysis, evaluation and recommendations for improvements, optimization development, and/or maintenance efforts for client-specific or mission critical challenges/issues; Consults with client to define need or problem supervises studies and leads surveys to collect and analyze data to provide advice and recommend solutions.

5.1 REQUIRED LABOR CATEGORIES, SKILLS, AND HOURS

The IRS requests the following labor categories and skill levels based on previous labor considerations.

Task 1 (FFP/LH): Fraud Analytics and Monitoring Labor Categories and Hours			
CLIN 0001: Fraud Analytics and Monitoring Common Project Tasks (FFP/LH)			
Occupation (SOC Code)	**Skill Level**	**FTE**	**Hours**
Computer and Information Systems Managers (11-3021)	SME	0.5	956
Computer and Information Systems Managers (11-3021)	Senior	1.0	1,912
Editors (27-3041)	Journeyman	.5	956
Sub-Total CLIN 0001: Fraud Analytics and Monitoring (FFP/LH)		**2**	**3824**

Task 2 (FFP): Fraud Analytics and Monitoring Labor Categories and Hours

DRAFT

CLIN 0002: Fraud Analytics and Monitoring Highly Specialized Tasks (FFP)			
Occupation (SOC Code)	**Skill Level**	**FTE**	**Hours**
Computer and Information Research Scientists (15-1111)	SME/WL4	1.0	1912
Operations Research Analyst (15-2031)	Principal II	1.0	1912
Operations Research Analyst (15-2031)	Journeyman	1.0	1912
Statistician (15-2041)	Lead	2.0	3,824
Engineers, All Other (17-2199)	Principal	1.0	1912
Engineers, All Other (17-2199)	Lead	2.0	3,824
Management Analysts (13-1111)	Senior	1.0	1,912
Business Operations Specialists, All Other (13-1199)	Principal	1.0	1,912
Business Operations Specialists, All Other (13-1199)	Senior Staff	4.0	7,648
Business Operations Specialists, All Other (13-1199)	Staff	2.0	3824
Sub-Total CLIN 0002: Fraud Analytics and Monitoring (FFP)		**17**	**32,504**

*Projected FTE count does not include Optional Tasks execution at inception.

Optional Task 3 – Surge Support Fraud Analytics and Monitoring Labor Categories and Hours			
Optional CLIN 0003: Fraud Analytics and Monitoring- Senior/Journeyman (LH)			
Occupation (SOC Code)	**E&Q Level**	**FTE**	**Hours**
Engineers, All Other (17-2199)	All LCATs	*5.0*	*9,560*
Operations Research Analyst (15-2031)	All LCATs	*5.0*	*9,560*
Sub-Total OPTIONAL CLIN 0003: Fraud Analytics and Monitoring Surge Support(LH)		***10.0***	***19,120***

Optional Task 4 – Fraud Analytics Stakeholder Support (LH)			
Optional CLIN 0004: Fraud Analytics and Monitoring- Senior (LH)			
Occupation (SOC Code)	**E&Q Level**	**FTE**	**Hours**
Operations Research Analyst (15-2031)	All LCATs	*2.0*	*3824*
Engineers, All Other (17-2199)	All LCATs	*2.0*	*3824*
Business Operations Specialists, All Other (13-1199)	All LCATs	*2.0*	*3824*
Sub-Total OPTIONAL CLIN 0004: Fraud Analytics and Monitoring Stakeholder Support(LH)		***6.0***	***11,472***