Performance Work Statement
Criminal Investigation
Development of Exploitation Techniques Against Cryptowallets

March 2021

PERFORMANCE WORK STATEMENT
INTERNAL REVENUE SERVICE (IRS), CRIMINAL INVESTIGATION (CI)
Development of Exploitation Techniques
Against Cryptowallets

1 INTRODUCTION/BACKGROUND

Internal Revenue Service – Criminal Investigation (CI) is the law enforcement arm of the Internal Revenue Service. CI is charged with the enforcement of the federal income tax statutes. CI's top priority is the investigation of violations of the federal income tax law. Additionally, CI special agents lend their financial investigative expertise to money laundering and narcotics investigations conducted in conjunction with other law enforcement agencies at the local, state and federal levels.

The emergence and rapid adoption of cryptographic currencies over the last decade has created a gap in digital forensic capabilities. The decentralization and anonymity provided by cryptocurrencies has fostered an environment for the storage and exchange of something of value, outside of the traditional purview of law enforcement and regulatory organizations. While research exists on the analysis and tracking of blockchain transactions, there is a portion of this cryptographic puzzle that continues to elude organizations – millions, perhaps even billions of dollars, exist within cryptowallets, but the value cannot be realized because of the challenging cryptographic problem. A cryptocurrency wallet (also known as crypowallet) provides a means of storing the public and private cryptographic keys to track ownership of cryptocurrencies. These cryptowallets contain the clues to access and extract the value represented by the blockchain transactions of a given cryptocurrency. The individual or organization who controls the public and private keys controls the cryptocurrency tied to that ‘wallet’. To secure the value of cryptocurrencies, secure embedded hardware devices have emerged in recent years to hold the public and private keys securely, offline from an internet connected computer. The rationale for this new technology is that the cryptocurrency is safer on a purpose built, secure electronic device rather than an internet connected computer or phone which may be compromised. In the routine course of their law enforcement activities, law enforcement organizations may receive hardware cryptowallets as evidence related to a case. If a subject fails to comply or is unavailable to aid, agencies may not be able to access the hardware cryptowallet. This may limit the options to investigate the movement of currencies across cryptographic currencies as well as prevent the forfeiture and recovery of these assets in line with established federal guidelines.

A body of research has begun to emerge on the cybersecurity of hardware cryptographic wallets. The research is frequently showcased at cybersecurity conferences for the purpose of increasing the security of cryptowallets as well as reporting exploits to the manufacturers of these devices. Despite best cyber security efforts, even secure embedded hardware devices may possess vulnerabilities in hardware, software and firmware that allow for the unintentional disclosure of information. Since hardware cryptographic wallets contain digital data – public and

private cryptographic keys – these small hardware computing devices may provide crucial data in investigations.

Digital forensics is a branch of forensic science focused on the recovery and investigation of data that exists on computer and other electronic devices. Digital forensics relies on the consistent, repeatable scientific processes that can ensure the integrity of the data for investigative and judicial processes. If the acquisition of data is possible from cryptographic wallets, the technique should be able to be defined in a consistent, repeatable process that will be:

- defensible in court,
- trainable to digital forensic examiners, and
- reliable for the recovery of digital data artifacts from cryptocurrency wallets.

2. OBJECTIVE

The Digital Forensics Unit of IRS-CI provides forensic support for task forces agents, computer investigative specialists, and cyber investigators throughout the country in conducting numerous activities. Digital Forensics routinely encounters cryptowallets subject to seizure and forfeiture. Though a few known cyber penetration testers have published vulnerabilities on specific devices, the process of decrypting the hardware devices to gain access to the wallets has been challenging. In support of IRS-CI, further forensic research is needed to mature the process and obtain reliable results.

The objective of this proposal is to

- Validate cybersecurity research in cryptographic wallets exploitation,
- Identify new methods to gain access to cryptographic wallets,
- Identify successful cryptographic models exploits can be accomplished,
- Document the processes, hardware, and skillsets needed for reproduction in an advance digital forensic laboratory, and
- Create hands-on training for the identified techniques in supporting of IRS-CI Digital Forensics Laboratory.

3. SCOPE

The contractor shall combine the leading-edge cybersecurity research available on the topics of embedded hardware exploitation with the disciplined, established science of digital forensics. The explicit outcome of this contract is to tame the cybersecurity research into measured, repeatable, consistent digital forensics processes that can be trained and followed in a digital forensics' laboratory.

Established exploitation, reverse engineering and digital forensic techniques shall be used to accomplish these tasks including software and firmware analysis, hardware reverse engineering, integrated circuit identification and research, removal of integrated circuit packages and components, deconstruction of printed circuit boards and

integrated circuit packages for the express purpose of identifying consistent, repeatable exploitation techniques against a given device.

The following contract seeks, through phased tasks specified in Section 4, to:

- Validate existing cybersecurity research on the topic of accessing cryptographic wallets through advanced exploitation techniques.
- Employ additional digital forensic and cybersecurity exploitation techniques to identify new methods to compromise the cryptographic wallets.
- Identify manufactures, models, and device versions the techniques can be successfully accomplished on.
- Document the process, the hardware, and the skillset sufficient to reproduce the capability in an advanced digital forensic laboratory.
- Create training on process and hands-on technique to reproduce the results.

Tangential Goals:

- Develop a body of research and expertise on this topic within the IRS-CI through a trusted third-party contractor.
- Identify new acquisition techniques against new device models and previously untested devices.

4. TASK ORDER OBJECTIVES

The Contractor shall produce Work Products/Deliverables that conform to, and integrate with, existing IRS standards and guidelines. The Contractor shall conform to all IRS Security and Disclosure policies. The Contractor shall provide support and services in the following general areas.

Task 1 Orientation Briefing
Task 2 CryptoWallet Exploitation and Training Development
    Task 2.1 Single Exploit, Single Device Topic
    Task 2.2 Multiple Exploits, Multiple Device Topics
Task 3 Advanced Exploratory Digital Forensic Research on Exploiting Emerging Devices
Task 4 Transition Support & Plan

TASK 1 - ORIENTATION BRIEFING (CLIN 0001)

The contractor shall schedule, facilitate, and conduct a kickoff/orientation briefing for the Government within ten (10) business days after award. The government does not require an elaborate orientation briefing, nor does it expect the contractor to expend significant resources in preparation for this briefing.

Rather, the intent of the briefing is to initiate the communication expectations and process between the government and contractor by introducing key contract participants, explaining their roles, reviewing communication ground rules and assuring a common understanding of the requirements outlined in the objectives and scope.

The orientation briefing shall be held via a conference call or at the Government's facility on a mutually agreed upon date and time. The contractor's Key Personnel shall present the materials. The contractor shall develop a cooperative/partnership working relationship with the CI program office stakeholders to ensure operations and performance is aligned with business goals and objectives

The completion of this briefing shall result in the following:

a) The contractor and Government personnel who will perform work under this task order will be introduced.
b) The Government shall disclose the non-evidentiary exemplar device of interest for Task 2.1.
c) Any issues concerning the contractor clearances for contractor personnel will be discussed.
d) The government and contractor shall agree to file repository and encryption requirements for deliverables.
e) The contractor shall demonstrate confirmation of their understanding of the work to be accomplished under this PWS.
f) The contractor shall provide the accounting period end dates to be used for the term of this task order.

DESIRED OUTCOME/DELIVERABLE: Final orientation briefing and minutes, agreed upon changes in writing to any tasks or deliverables.

Task 1: Orientation Briefing - FFP				
Deliverable ID	**Deliverable**	**Frequency**	**Due Date**	**Electronic Delivery Address:**
Task 1	• Orientation briefing • Document communication process • List of task participants • Document Roles and Responsibilities • Document ground rules • Document outcome and understanding • Document information sharing requirements	Once	Within 10 business days after Task Order Award	Will be provided once contract awarded

TASK 2 – CryptoWallet Exploitation and Training Development (CLIN 0002)

The tasks will be broken into the following schedule and options. The applicable contractor shall be responsible for procuring any exemplar devices, hardware, tools, equipment, and training to perform any of the tasks below. All tasks will be completed at the contractor's facility. Contractor's team leads are expected to attend monthly status meetings which detail current task progress, issues encountered, and the number and type of activities performed.

Subtask 2.1 Single Exploit, Single Device Topic

To validate the premise, all available exploit types will be aimed against a single device type (a specific model from a manufacturer identified by the government).

The contractor shall provide the “Proof-of-Concept” that cybersecurity exploits can be used to compromise the integrity of the cryptocurrency wallet protections for seizure. The goal will be to transition the exploit into consistent and repeatable processes through scientific testing, documentation, and process creation. All testing and process definition will be conducted on non-evidentiary exemplar devices of like manufacturer and model from evidentiary devices.

The contractor shall review of all available exploits identified for the Manufacturer Model cryptocurrency wallet. The contractor shall analyze all exploitation avenues for a successful consistent and repeatable attack, such as but not limited to:

- publicly available exploits,
- RF (if applicable),
- USB (if applicable),
- Software and firmware review (if available from OEM or can be retrieved from the device),
- Circuit board exploit (UART, SWD, SPI, JTAG, etc.),
- Microcontroller exploit in-site (still attached to the circuit board; glitching, chip-read, bootloader interference, etc.),
- Microcontroller exploit removed (chip-off and binary dump; glitching, chip-read, bootloader interference, etc.),
- Any other available flash integrated circuits on the board,
- Targeted at the specific Manufacturer Model cryptocurrency wallet,
- Targeted at the microcontroller architecture utilized in the device (STMicroelectronics STM32F microcontroller or whichever model is used in the device).

At the conclusion of this task the contractor shall deliver a device-specific acquisition/exploitation process, guide, and training to utilize against the same model devices in a digital forensics laboratory.

The contractor shall provide exploitation confirmation of evidentiary device under the supervision of government at contractor’s forensic laboratory at the government’s discretion.

Subtask 2.2 Multiple Exploits, Multiple Device Topics

Build on the successful Proof-of-Concept in Task 1 by extending to multiple cryptowallets

- Identify the leading cybersecurity research in the world aimed at cryptographic wallets
- Validates the published techniques against the variety of wallets.
- Extend the Proof-of-Concept listed in Task 2.1 against all the current known exploits for each of the device models available.
- Identify trends in the exploitation techniques, the microcontrollers vulnerable to exploitation, and the other variables that are consistent across the variety of devices.
- Expand exploitation capability to a proactive response, allowing the trends to emerge across the existing research.

At the conclusion of this task the contractor shall deliver device-specific acquisition/exploitation processes, guide, and training for each device topic for utilization in a digital forensics laboratory.

The contractor shall provide exploitation confirmation of evidentiary devices matching government sampling from exemplars under the supervision of government at contractor's forensic laboratory at the government's discretion.

DESIRED OUTCOME/DELIVERABLE:
All identified, hardware cryptowallets receive a complete (1) Report, (2) Process Documentation, and (3) integration into the Cryptowallet Exploitation training for each of the interrogated devices. All identified hardware cryptowallets receive a report. Successful, repeatable processes will be followed with Process Documentation and Training integration. A matrix of exploits per device will be crafted with intention to move this to a webpage and/or mobile platform during Task 3.

1. Comprehensive Exploitation Report.
   Thorough and exhaustive report analyzing all characteristics about each device topic. Analysis of exploitation techniques possible with the device. Interrogation of the board and chips included on the board. Identification of firmware and OS that can be identified from the device.
   - Teardown
   - Integrated circuit package identification
   - Firmware and OS identification
   - Exploitation
   - Decapsulation of custom ASICs.
   - Circuit board layer disassembly and mapping.
   - Index of publicly available articles and resources related to the hardware, components, exploitation, and cybersecurity risks.

2. Process Documentation
   Process Documentation Summarized, repeatable digital forensics step process to acquiring data and exploiting data from each device topic.

3. Training
   Integration into the Cryptowallet Exploitation training for each of the interrogated devices.

4. Matrix of exploits per device
   Matrix of exploits per device will be crafted in Task 2.2 with intention to move this to a webpage and/or mobile platform during Task 3.

Task 2: CryptoWallet Exploitation and Training Development (CLIN 0002)				
Deliverable ID	**Deliverable**	**Frequency**	**Due Date**	**Electronic Delivery Address:**
2.1	Monthly Status Report	Monthly	Due dates will be established by Project Schedule	Will be provided once contract awarded

2.1	Comprehensive Exploitation Report	Within 15 days of period of performance end date.	Within 3 calendar months after Task Order Award	Will be provided once contract awarded
2.1	Guide with Process Documentation for device-specific acquisition/exploitation process of Task 2.1 Device	Within 15 days of period of performance end date.	Within 3 calendar months after Task Order Award	Will be provided once contract awarded
2.1	Cryptowallet Exploitation Training on Task 2.1 Device	Within 15 days of period of performance end date.	Within 3 calendar months after Task Order Award	Will be provided once contract awarded
2.2	Monthly Status Report	Monthly	Due dates will be established by Project Schedule	Will be provided once contract awarded
2.2	Comprehensive Exploitation Report for all identified, hardware cryptowallets	Within 15 days of period of performance end date.	Within 12 calendar months after Task Order Award	Will be provided once contract awarded
2.2	Guide with Process Documentation for device-specific acquisition/exploitation for all identified, hardware cryptowallets	Within 15 days of period of performance end date.	Within 12 calendar months after Task Order Award	Will be provided once contract awarded
2.2	Cryptowallet Exploitation Training on for all identified, hardware cryptowallets	Within 15 days of period of performance end date.	Within 12 calendar months after Task Order Award	Will be provided once contract awarded
2.2	Matrix of exploits per device for all identified, hardware cryptowallets	Within 15 days of period of performance end date	Within 12 calendar months after Task Order Award	Will be provided once contract awarded
2.2	Period of Performance Summary Report.	Within 15 days of period of performance end date.	Within 12 calendar months after Task Order Award by Project Schedule	Will be provided once contract awarded

TASK 3 - Advanced Exploratory Digital Forensic Research on Exploiting Emerging Devices (Optional) (CLIN 1001)

The clear transition of advanced cybersecurity research into repeatable, consistent digital forensic processes is evident from the successes of Task 2. In Task 3, the contractor expands the analysis of Task 2 from the Exploitation Matrix to identify forward risks on new technologies.

The current state of cybersecurity research by this task highlights vulnerabilities within specific microcontrollers as well as a variety of ways to exploit these systems. Exploitation can range from an interrogation of the integrated circuit package (IC package) directly to in-situ interrogation by interrupting the normal operation of the IC package. Glitching introduces an intentional fault through a variety of means to interfere with the normal operation (and normal security features) of the IC package that is targeted.

Through mastery of the identification of vulnerable components on embedded devices as well as a complete toolbox of exploitation techniques, advanced exploratory research can be conducted against new device types as they emerge. The variety of these techniques can be crafted from a digital forensic perspective from the beginning instead of the adaptation of cybersecurity techniques into consistent, repeatable digital forensic topics.

The contractor shall develop a comprehensive digital forensics hardware exploitation lab shopping list and setup guide; thorough documentation on the various exploitation techniques utilized throughout Task Two and Three; as well measured, defined exploitation targets throughout lifecycle of Stage Three. Successful exploitation candidates will receive comprehensive exploitation reports, process documentation and integration into the defined training.

Create and deliver Online reference platform including exploitation matrix, how-to guidance and exploitation reports per device with Task Three deliverables. Any data for online platform must be stored in an open source format (e.g. sqlite, json).

Task 3: Advanced Exploratory Digital Forensic Research on Exploiting Emerging Devices (Optional) (CLIN 1001)				
Deliverable ID	**Deliverable**	**Frequency**	**Due Date**	**Electronic Delivery Address:**
Task 3	Monthly Status Report	Monthly	Due dates will be established by Project Schedule	Will be provided once contract awarded
Task 3	Comprehensive Exploitation Report for all identified, successful exploitation candidates	Within 15 days of period of performance end date.	Due dates will be established	Will be provided once contract awarded

			by Project Schedule	
Task 3	Guide with Process Documentation for device-specific acquisition/exploitation for all identified, successful exploitation candidates	Within 15 days of period of performance end date.	Due dates will be established by Project Schedule	Will be provided once contract awarded
Task 3	Cryptowallet Exploitation Training on for all identified, successful exploitation candidates	Within 15 days of period of performance end date.	Due dates will be established by Project Schedule	Will be provided once contract awarded
Task 3	Online reference platform including exploitation matrix, how-to guidance and exploitation reports per device	Within 15 days of period of performance end date.	Due dates will be established by Project Schedule	Will be provided once contract awarded

TASK 4 - TRANSITION SUPPORT AND PLAN (Optional) (CLIN 1002)

At the end of the contract, the Contractor shall provide transition-out services. The Contractor shall facilitate the transition of contracted activities and services to CI, Cybersecurity Program personnel and/or to a follow-on Contractor in accordance with the Government Approved Transition-Out Plan (TOP). The Contractor shall identify transition activities, schedules, and milestones for the turnover of work (e.g., operations, maintenance, engineering, training, asset management, and logistics functions) and identify how it will coordinate with the incoming Contractor(s) and CI personnel to transfer knowledge. The transition period shall commence no later than 120 calendar days before the contract expiration. During the transition period, the Contractor shall implement all activities necessary to establish a stable environment, through the creation of a Transition Readiness Review (TRR), in which specific readiness criteria and status are presented.

- The TRR shall include:
  - All technical support activities and documentation that should be transferred to enable Government personnel, and/or incoming Contractor staff to effectively continue any DME and O&M Support
  - Status report and project schedule
  - Planned activities
  - Issues encountered - Issues Log
  - Risks Identified – Risk Log
  - Updates to action items assigned – Action Items Log

The Contractor shall:

- Minimize transition impact to the end-user community, ensuring a transparent and seamless transition with no breaks in the application and existing support service

functionality.

- Maintain system and meet delivery milestones of ongoing project tasks.
- Ensure that the IT security posture during transition is maintained at current levels without creating gaps and/or vulnerabilities.
- Provide all required personnel, management oversight, tools, processes, and other necessary resources to fully support these transition tasks.
- Transition of technical skills and lessons learned to the CI staff and/or Government designee upon completion of deliverables and work products.
- Transfer of complete documentation for all delivered functionality. Deliverables shall be in softcopy and hardcopy format and shall be the sole property of the Federal Government. The format of deliverables will be provided in a format which will allow the Government the ability to update if necessary. A complete set of documentation will also be stored in the projects' PAL.
- Transfer of all Source Codes to the Government. These source codes are the sole property of the Government.
- Transition is to involve the incumbent Contractor staff working with the incoming Contractor staff. This activity includes the review of key components with the project. The Contractor's key representatives shall attend weekly stakeholder meetings to discuss the status of the transition. This includes, but is not limited to the following:
    - Support team members and IRS / contracting staff working on the assignment in a collaboration.
    - The sharing of information and considerations necessary for the decision-making process.
    - Mentoring of the assigned key staff personnel in development of the skills needed to perform this scope of work.
    - Maintaining all documentation of standards and procedures for ongoing maintenance of the programs.

The Contractor shall provide to IRS-CI the tools and technical knowledge necessary to maintain the performance of IRS-CI's processes and functions after the engagement has been completed. 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). Prior to the transfer of knowledge, the Contractor shall develop a draft Transition-Out Plan (TOP) and present it to the Government within the first 15 business days after award. The Transition-Out Plan shall identify the Contractor resources 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. The project schedule shall identify tasks, dependencies, deliverables, and milestones. The project schedule shall be at a sufficient level of detail to track progress on a bi-weekly basis, (i.e., all tasks will be detailed to a level such that no task has duration of more than ten workdays).

The Government shall have 15 business days to review the draft TOP and provide comments to the Contractor. Government and Contractor representatives will then meet to discuss the comments, after which the Contractor shall incorporate the

agreed-upon changes and deliver a final TOP within 5 business days of the government's feedback. Full and complete knowledge transfer should occur no later than ninety (90) days after award.

Task 4: Transition Support and Plan - (Optional) (CLIN 1002)				
Deliverable ID	**Deliverable**	**Frequency**	**Due Date**	**Electronic Delivery address**
Task 4	Knowledge transfer of technical skills and lessons learned to IRS staff upon completion of deliverables and work products	Within 15 days of period of performance end date	Due dates will be established by Project Schedule	Will be provided once contract awarded
Task 4	Transfer of complete documentation for all delivered functionality	Within 15 days of period of performance end date	Due dates will be established by Project Schedule	Will be provided once contract awarded
Task 4	Knowledge transfer of all configurable data, including usernames and passwords, and shall include application settings, integrations, and interfaces	Within 15 days of period of performance end date	Due dates will be established by Project Schedule	Will be provided once contract awarded
Task 4	Provide Transition Plan for services defined in contract award/PWS	TBD once contract awarded	Within 15 days after contract award	Will be provided once contract awarded

SECTION E

INSPECTION, ACCEPTANCE AND SUBMISSION OF WORK

INSPECTION
Inspection will be at the same place as performance and delivery, unless otherwise specified.

GENERAL ACCEPTANCE CRITERIA

The general quality measures as set forth below will be applied to each work product/deliverable received from the contractor under this contract and any resulting task orders awarded. All Deliverables, Documents, and Services shall satisfy program and project requirements, and comply with IRS CMMI standards, existing IRS standards and guidelines, and integrate with IRS, security requirements, and Section 508.

1. Contractor shall provide clear documentation for all projects they are engaged on and listed above that (where appropriate).

2. Accuracy - work products/deliverables shall be accurate in presentation, technical content, and shall adhere to accepted elements of style, operational content and consistent within itself and with other documentation.

3. Clarity - work products shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand and relevant to the supporting narrative. Reports and documentation produced under this Task Order must be clearly written and understood by the COR and EAO staff, prior to acceptance of the Work Product/Deliverable.

4. Specification Validity – Work Products/Deliverables must satisfy the technical and/or functional requirements of the Government, as specified in this PWS, to produce the Desired Outcomes stated in Section 4.

5. File Editing – All text and any diagrammatic files shall be editable by the Government.

6. Format - work products shall be submitted in hard copy (where applicable) and in media defined in the PWS/SOW. The work product format may be different in each task order. Hard copy formats shall follow Department of the Treasury and IRS Directives and shall be consistent with other similar efforts. All text and diagrammatic files shall be editable by the Government.

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

8. Operability – Software and other Work Products/Deliverables created for this Task Order must operate without faults, to produce the Desired Outcomes, prior to their acceptance by the Government.

9. Functionality – Software and other Work Products/Deliverables created under this Task Order must function in such a way as to produce the stated Desired Outcomes for each activity.

10. Compliance – Work Products/Deliverables shall be in conformance with all standards and regulations noted in this PWS.

11. Accuracy and Validity – Data produced by software and procedures developed under this Task Order, as well as all reports and documentation, must be accurate and valid prior to acceptance.

12. Completeness – Work Products/Deliverables must be submitted as fully completed end products and demonstrates sufficient level of detail to show

understanding of the requirements, technology and design, customers, and operating environment.

13. Feasibility – Work Products/Deliverables shall define information, which is formatted properly, contains valid information in support of each task and provides a deliverable within time constraints.

14. Practicality - The document provides information and guidance that is practical for implementation within the IRS environment and appropriate given the subject organization's level of maturity.

REVIEW OF DELIVERABLES

The IRS will inspect Work Products/Deliverables for conformance as specified in this Section of the Task Order. Upon receipt of any Work Products/Deliverables, the IRS will have ten (10) federal business days to review, comment, and accept or reject Work Products/Deliverables. Any rejection will state the basis for the rejection; include a specific reference to the Task Order paragraph or Section with which the Work Product/Deliverable does not conform and identify the corrective action or rework that is required.
All acceptance or rejection of Work Products/Deliverables will be documented by the Government.

Any rework required due to rejection will be at no cost to the Government.

Rework required shall be completed within three (3) federal business days after notification from CI. When the Contractor returns the reworked Work Product/Deliverable, CI will re-inspect the Work Product/Deliverable within five (5) federal business days of receipt for verification that written deficiencies have been addressed and incorporated, as necessary.

Work Products/Deliverables are provided to demonstrate sufficient progress toward a required product, service, or Work Products/Deliverables. All Work Products/Deliverables will be made available in accordance with the due date(s) specified in the Delivery Schedule. The Government may provide comments to the Contractor within five (5) federal business days after receipt of Work Products.

The Contractor shall notify the CO and COR when content required to complete the work has not been provided.

The Contractor shall produce final documents without typographic and grammatical errors and shall be formatted according to standards provided by the Government. The Contractor shall send all electronic deliverables to the designated COR.

SECTION F

DELIVERIES OR PERFORMANCE

DELIVERABLES

The contractor shall complete and deliver the deliverables listed in Section 4 of this PWS, to the Contracting Officer's Representative (COR) by the dates or within the timeframes indicated.

For most required services, the Contractor provided deliverables shall meet three key requirements: (1) Proposed Timeline, (2) Draft and Final Products, and (3) Complete Official Record. Details and guidelines for the preparation of these will be discussed and finalized with the COR.

All deliverables will be rated on the timeliness and quality of the product. IRS will be given a 10-day review period to critique all Deliverables. The Contractor will have 5 days to update the Deliverable once comments are provided by IRS.

All deliverables shall be provided in either MS Word, PowerPoint, Excel or other compatible format designated by the COR or CO. Deliverables/work products could require continuous updates

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 in electronic format to the CI Technical Point of Contact and Project/Program Manager for the work product/deliverable and to the COR.

All deliverables will be rated on the timeliness and quality of the product. IRS will be given a 10-day review period to critique all Deliverables. The Contractor will have 5 days to update the Deliverable once comments are provided by IRS.

Work and work products, including email communications, shall only be accomplished on CI issued laptop computers.

DELIVERY SCHEDULE

Work Products/Deliverables are required to be delivered in accordance with the deliverable tables in Section 4 of this PWS. Due dates will be negotiated during the transition phase and re-baselined with the approval of the IRS Project Manager and COR. The deliverable table will be modified to include each due date.

PERIOD OF PERFORMANCE

The period of performance for the anticipated task order will be two years (base plus one 12-month option year) to include a 6-month extension period if needed.

The anticipated Period of Performance for the base period will be September 30,2021 through September 29, 2022 with the option year as follows:

Option Year 1: 09/30/2022-09/29/2023

If requirement is awarded prior to 09/30/2021, Digital Forensics has a critical need to start the contract as soon as possible.

RAMP UP PERIOD

Work under this PWS may require a ramp-up period at the initial contract award date prior to the contract period of performance for the Contractor to recruit and hire personnel specifically for this PWS. If needed, the ramp-up period specifics shall be identified in the Contractor's proposal.

HOURS and PLACE OF PERFORMANCE

The work hours for this Task Order shall be M-F 8:30am – 5:00pm EST. Schedule changes that meet mission need may be approved by the Contracting Officer and the IRS Program Manager.

Work is performed remotely, only at contractor's US facility.

Government personnel will be available to work with Contractor to provide access to relevant data to facilitate timely completion of deliverables.

The Government will provide list of non-evidentiary exemplar devices. Contractor is responsible for procuring model matching exemplar devices at contractor's sole cost.

Tasks are firm fixed price with no overages authorized.

PERFORMANCE REQUIREMENTS, STANDARDS AND SURVEILLANCE

The Government believes there is value in incorporating Performance-Based Service Acquisition (PBSA) methodology with an outcomes-based focus for this work. The Matrix below defines the Government's Desired Outcomes, Required Services, Performance Standards, Acceptable Quality Levels and Monitoring Methods for each Sub-task included in this Task Order.

Task 1: Orientation Briefing - FFP				
Deliverable ID	**Deliverable**	**Acceptable Quality Level (AQL)**	**Surveillance Method**	**Incentives and/or Adverse Actions**
Task 1	• Orientation briefing • Document communication process • List of task participants • Document Roles and Responsibilities • Document ground rules	AQL: 95% of all recent information	100 Percent Inspection	Past Performance

	• Document outcome and understanding • Document information sharing requirements			
Task 2: CryptoWallet Exploitation and Training Development (CLIN 0002)				
Deliverable ID	**Deliverable**	**Acceptable Quality Level (AQL)**	**Surveillance Method**	**Incentives and/or Adverse Actions**
2.1	Monthly Status Report	AQL: 95% of all recent information	100 Percent Inspection	Past Performance
2.1	Comprehensive Exploitation Report	AQL: 100% of all recent information	100 Percent Inspection	Past Performance
2.1	Guide with Process Documentation for device-specific acquisition/exploitation process of Task 2.1 Device	AQL: 100% of all recent information	100 Percent Inspection	Past Performance
2.1	Cryptowallet Exploitation Training on Task 2.1 Device	AQL: 100% of all recent information	100 Percent Inspection	Past Performance
2.2	Monthly Status Report	AQL: 95% of all recent information	100 Percent Inspection	Past Performance
2.2	Comprehensive Exploitation Report for all identified, hardware cryptowallets	AQL: 100% of all recent information	100 Percent Inspection	Past Performance
2.2	Guide with Process Documentation for device-specific acquisition/exploitation for all identified, hardware cryptowallets	AQL: 100% of all recent information	100 Percent Inspection	Past Performance
2.2	Cryptowallet Exploitation Training on for all identified, hardware cryptowallets	AQL: 100% of all recent information	100 Percent Inspection	Past Performance
2.2	Matrix of exploits per device for all identified, hardware cryptowallets	AQL: 100% of all recent information	100 Percent Inspection	Past Performance
2.2	Period of Performance Summar Report.	AQL: 95% of all recent information	100 Percent Inspection	Past Performance
Task 3: Advanced Exploratory Digital Forensic Research on Exploiting Emerging Devices (Optional) (CLIN 1001)				
Deliverable ID	**Deliverable**	**Acceptable Quality Level (AQL)**	**Surveillance Method**	**Incentives and/or Adverse Actions**
Task 3	Monthly Status Report	AQL: 95% of all recent information	100 Percent Inspection	Past Performance

Task 3	Comprehensive Exploitation Report for all identified, successful exploitation candidates	AQL: 100% of all recent information	100 Percent Inspection	Past Performance
Task 3	Guide with Process Documentation for device-specific acquisition/exploitation for all identified, successful exploitation candidates	AQL: 100% of all recent information	100 Percent Inspection	Past Performance
Task 3	Cryptowallet Exploitation Training on for all identified, successful exploitation candidates	AQL: 100% of all recent information	100 Percent Inspection	Past Performance
Task 3	Online reference platform including exploitation matrix, how-to guidance and exploitation reports per device	AQL: 100% of all recent information	100 Percent Inspection	Past Performance
Task 4: Transition Support (Optional) (CLIN 1002)				
Deliverable ID	**Deliverable**	**Acceptable Quality Level (AQL)**	**Surveillance Method**	**Incentives and/or Adverse Actions**
Task 4	Knowledge transfer of technical skills and lessons learned to IRS staff upon completion of deliverables and work products	AQL: 95% of all recent information	100 Percent Inspection	Past Performance
Task 4	Transfer of complete documentation for all delivered functionality	AQL: 95% of all recent information	100 Percent Inspection	Past Performance
Task 4	Knowledge transfer of all configurable data, including usernames and passwords, and shall include application settings, integrations, and interfaces	AQL: 95% of all recent information	100 Percent Inspection	Past Performance
Task 4	Provide Transition Plan for services defined in contract award/PWS	AQL: 95% of all recent information	100 Percent Inspection	Past Performance

SECTION G
CONTRACT ADMINISTRATION DATA

IDENTIFICATION OF GOVERNMENT TASK ORDER PERSONNEL

The COR designation will be identified by the CO's written designation memo. The CO will identify the (COR/LCOR) via e-mail to the Contractor.

PAYMENT TERMS AND CONDITIONS

The contractor shall submit invoices for Contract Line Items (CLINs) in equal monthly payments.

SECTION H, SPECIAL TASK ORDER REQUIREMENTS

STAFFING AND KEY PERSONNEL/Facility REQUIREMENTS

Treasury Directive 71-10, that all contractors working on a Treasury (or IRS) contract must be U.S. citizens or permanent residents. Contractor shall not utilize any employee on PWS who does not meet these criteria. All work performed on PWS must be performed in Contractor's forensic laboratory with appropriate security controls.

GOVERNMENT FURNISHED EQUIPMENT, INFORMATION AND SERVICES

No government property to be provided to contractor.

GOVERNMENT FURNISHED INFORMATION (GFI)

GFI (to include manuals, notes, memos, instruction ©materials, and other information) will be provided in the performance of this Task Order. The following GFI will be provided to the Contractor upon Task Order award.

INFORMATION ITEMS
Manuals, directives, instructions and other printed/electronic media required for the performance of duties including IRM and other official use only publications

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

RIGHTS TO DATA AND DISCLOSURE

Due to the nature of the IRS mission, all data, work products and deliverables used in its mission is the property of the IRS.

Contractor shall not utilize or disclose any information pertaining to this Task Order without the prior written consent of IRS Contracting Officer (CO).

TRAVEL REQUIREMENTS

No travel is reimbursable or authorized for this PWS.

INVOICING

Invoices shall be submitted monthly (by the 10th).

Invoices must be submitted via the invoice processing platform at www.IPP.GOV.

CONTRACTOR RESPONSIBILITY FOR ASSIGNED SPACE, EQUIPMENT AND SUPPLIES

No Government space, equipment, or supplies provided per PWS.

APPLICABLE LAWS & DIRECTIVES

The contractor shall comply with Government-wide and Bureau-specific policies, including but not limited to the following:

Treasury Directive (TD) 15.71
Internal Revenue Manual (IRM) 10.23.2
Homeland Security Presidential Directive (HSPD) 12
TOIS Service Level Agreement
IRS Service Level Agreement

The IRS, upon request, will make available these documents. The contractor shall comply with all new versions, amendments, and modifications made to the above-mentioned documents/standards, when they become applicable in the future.

In addition, there are specific laws and regulations that bind our IT investments to ensure compliance is established government-wide in addition to internal IRS laws, regulations and policies. Some of those include:

- Federal Acquisition Regulations (FAR)
- Competition in Contracting Act 1984 (CICA)
- Federal Information Security Management Act of 2002 (FISMA)
- The E-Government Act of 2002
- Clinger-Cohen Act of 1996
- American Recovery and Reinvestment Act of 2009
- Section 508 of the Rehabilitation Act of 1983, per the 1998 Amendments
- IRS Enterprise Architecture
- Enterprise Life Cycle
- IRS Security Standards
- IRS Contractor Security and Contractor Mandatory Training
- Federal Travel Regulations/the Joint Travel Regulations

INFORMATION SECURITY / FEDERAL INFORMATION SECURITY MODERNIZATION ACT (FISMA) (IT Systems / Applications or Services) Revised April 2020

Pursuant to the Federal Information Security Modernization Act (FISMA), Title III of the

E-Government Act of 2014 (Pub. L. 113–283), the contractor shall provide minimum security controls required to protect Federal information and information systems in accordance with NIST Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations. The contractor shall provide a risk-based process for selecting the security controls necessary to satisfy the minimum-security requirements in accordance with Federal Information Processing Standard (FIPS) 199. The term information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentially, integrity and availability. An information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Information resources include information and related resources, such as personnel, equipment, funds, and information technology.

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

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

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

FedRAMP security requirements shall apply to all IRS cloud services and products and shall be implemented and complied with as part of FedRAMP.

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

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

The contractor shall follow Information Security guidance established by the National Institute of Standards and Technology (NIST). The contractor shall establish the minimum- security controls identified in NIST Special Publication 800-53 Rev. 4, Security and Privacy Controls for Federal Information Systems and Organizations for FISMA compliance. The contractor shall follow the best practices and guidance established by NIST special publication 800 Series and Federal Information Processing Standards (FIPS) for computer security. The IRS may determine such applicable Information Technology (IT) Security standards and policies.

SECTION 508
COR will insert clauses once IRAP approval received

POINTS OF CONTACT

TBD

ATTACHMENT 1

Quality Assurance Surveillance Plan (QASP)

PROGRAM CONTROL AND PROCESS MANAGEMENT SUPPORT

1.0 INTRODUCTION

This performance-based Quality Assurance Surveillance Plan (QASP) sets forth the procedures and guidance that the IRS will use to evaluate and reward the performance of the Contractor in accordance with the terms and conditions of this Task Order. Whereas the IRS-CI and the Contractor have entered into a partnership with shared objectives to achieve the Outcomes indicated in Section 3 to the Task Order, the QASP consolidates two historically separate documents into one: The Contractor Quality Control Plan (QCP), and the QASP (historically a Government-only document), . Accordingly, this document shall be contractually binding.

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. Information generated from the IRS CI Project Management Office (CI-PMO) surveillance activities will directly feed into the CI-PMO performance discussions with the Contractor.

The QASP can be changed/updated, etc. It is intended to be a “living” document that should 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.

1.1 Purpose of the QASP

The QASP provides the IRS CI Project Manager (PM), the COR, the Contracting Officer the ability to conduct surveillance activities of Contractor performance during the life of this Task Order. The QASP details how and when the IRS-CI PMO will monitor, evaluate, and document Contractor performance with regards to the Performance Work Statement (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 will be assessed;
3) Describe the rating elements and the evaluation method that will be employed by the Government in assessing the Contractor’s performance.
4) Provide copies of the performance assessment form(s) that the Government will use in documenting and evaluating the Contractor’s performance.

5) Describe the process of performance assessment documentation.

1.2 Roles and Responsibilities of Government Officials
The QASP is a guide to be used by IRS CI personnel to conduct surveillance activities of the Contractor after Task Order award. The IRS-CI-PMO will review technical documents and products generated by the Contractor. IRS CI contract managers (e.g., Contracting Officers (CO) and Contract Specialists) will also conduct review of contract specific Reports of Works such as invoices, monthly status reports, and work plans. The PM and the CO will use the QASP as a tool to evaluate if the Contractor-provided service meets the performance standards in the contract and will be the basis for determining incentives involving additional work earned for the Contractor.

The Contracting Officer's Representative (COR) is responsible for technical administration. Although principally responsible for administration of this surveillance plan, the COR relies upon the Project Manager and his/her assigned Technical Points of Contact to perform and document many of the detailed surveillance activities required by the plan.

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 Contracting Officer for action.

The Contracting Officer (CO), Lead COR, and/or the CO's representative, will have overall responsibility for overseeing the Contractor's performance. The CO will also be responsible for the day-to-day monitoring of the Contractor's performance in the area of contract compliance, contract administration, cost control; reviewing the PM or COR assessment of the Contractor's performance; and resolving all differences between the Government and the Contractor. The CO may call upon the technical expertise of other Government officials as required.

1.3 Key Deliverables for Assessment
IRS CI and the Contractor have entered into a partnership with shared objectives to achieve the Outcomes indicated in Section 2 in the PWS. Each Outcome is to successfully complete the tasks. To successfully complete each task the deliverables listed in Section 2 must be produced by the Contractor as indicated in the PWS.

2.0 Rating Elements and Standards of Performance for Key Deliverables
The Contractor's performance shall be evaluated using the following two Performance Standards: Schedule and Quality. These Performance Standards are weighted for each Outcome. Acceptable Quality Levels (AQLs) for each Performance Standard are summarized in Section F.

3.0 Surveillance Methodology
Surveillance methodology is included in Section F (i.e., Monitoring Method).

4.0 Process of Quality Assurance Assessment

A determination of the Contractor's overall performance will be on an annual basis. The IRS CI will provide annual customer feedback to the Contractor by summarizing the past year's surveillance activities under the Contractor Performance Assessment Reporting System (CPARS) administered by the Naval Sea Systems Command (NAVSEA) . In addition, IRS will provide immediate and annual performance customer feedback from Government personnel involved in the use or management of the project. As soon as a discrepancy is identified with a deliverable associated with this Task Order, the PM and/or CO will notify the Contractor.

The Government will score each document and/or deliverable received from 1 to 100 points based on completeness, feasibility, understandability, accuracy, and practicality. The minimum acceptable score for each document and/or deliverable is 90. Scores of 89 and below will require the Contractor to revise each document and/or deliverable at no additional cost to the Government.

5.0 Performance Requirements Summary

The development of a Performance Requirements Summary, presents the tasks under surveillance; presents the deliverables to be monitored; gives the surveillance methodology for each task, provides the acceptable performance rating for each task; gives the frequency of each deliverable being monitored; and, describes the type of monitoring to be performed by Internal Revenue Service personnel.

6.0 Surveillance Documentation

A Development Performance Standards Checklist will be used by IRS CI personnel conducting the monitoring of the Contractor's performance on this Task Order. Performance evaluations associated with the performance categories of cost; schedule and quality for the contract will be documented. The Performance Standards Checklist will be submitted by the PM and/or COR to the CO for appropriate action. Also, the Contractor Performance Evaluation Form will be used to document findings for the past year's surveillance activities regarding the Contractor's performance under this Task Order and will be the basis for an annual performance discussion between IRS personnel and the Contractor representative under the CPS.

7.0 Information Required from the Contractor

7.1 Quality Control Plan

In this section, the Contractor that is awarded the Task Order shall establish and maintain a complete Quality Control Plan (QCP) to ensure that the requirements of the Task Order are provided as specified. The QCP shall describe the methods for identifying and preventing problems before the level of performance becomes unacceptable.