Start: SOW

1. Enter the PR Number if known.

*@User: Explanation* *Provide the PR number that is assigned in FSMS when the funds are/were committed.*

*@LLM: Example Answer –PR257667F001*

*@Optional*

1. Is this requirement IT related?

*@User:* *Explanation If IT related services or supplies are included in the requirement, an ITAR review is required. A yes answer triggers incorporation of the TSA Enterprise Architecture and Cybersecurity language required by CIO.*

*@LLM: Example Answer - Yes*

*@Required*

1. What is the Name of the program?

*@User:* *Explanation: The name of the program should match the name of the PR. Some examples are Focused Operations Services, Microsoft License Renewal, Personnel, Payroll and Benefits (PPBE)*

*@LLM: Example Answer – Focused Operations Services*

*@Required*

1. What is the requiring activity?

*@User: (i.e. Program Office,* *should start with TSA, then Office, Division, Branch if applicable)*

*@LLM: Example Answer - Transportation Security Administration (TSA)/Information Technology (IT)/Information Assurance Division (IAD) Focused Operations (FO) Branch*

*@Required*

1. What is the background information relative to this requirement?

*@User: Provide relevant background information that will be useful to contractors in understanding the need for the services and to assist the contractors in understanding how TSA past practices or current policies could impact future efforts. Address any previous contract activities for similar work.*

*@LLM: Example Answer -* *The TSA was created to meet the nation’s need for transportation security, including all modes of domestic transportation and international aviation. The Homeland Security Act (HSA) transferred the TSA to the Department of Homeland Security (DHS**). Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency.*

*Congress granted TSA wide latitude in acquiring and managing the Information Technology (IT infrastructure necessary to support accomplishment of the TSA mission. TSA IT’s mission is to ensure the security and productivity of TSA and its employees through IT. The TSA IT organization provides the administration’s response to meeting the practical and statutory security requirements associated with the use of IT solutions to support administration assets. They provide centralized management and leadership of TSA's information technology needs. The TSA IT organization is committed to using best practices, streamlining business processes, improving performance, and striving for excellence in support of TSA’s mission. The TSA IT vision is to provide secure information anytime, anywhere.*

*The TSA Chief Information Security Officer (CISO) is responsible for the IT security activities necessary to protect the TSA IT Infrastructure. IAD, within TSA IT, is the IT security oversight arm for TSA. IAD provides focused and efficient management of the IT security activities necessary to protect the TSA IT infrastructure. IAD manages the IT security activities necessary to protect the TSA IT Infrastructure and is the central office responsible for delivering information security services to TSA, to include risk and policy management. IAD delivers the IT security services mandated by federal security laws.*

*The FO Branch within IAD works to achieve TSA compliance with federal, DHS, and TSA cybersecurity requirements. TSA/IT/IAD FO is responsible for maintaining an operational capability that combines multiple disciplines of advanced cyber analytics. It is a tactical group composed of highly skilled IT security experts specializing in fields of cyber intrusion expertise designed to discover, investigate and mitigate stealthy cyber intrusion identification and detection, threat emulation, cyber intelligence, digital media analysis and litigation support through e-Discovery and forensics. The FO team processes threat indicators on a daily basis to prevent network exploitation and the exfiltration of sensitive TSA data. FO conducts cyber investigations within TSA. FO maintains its own network that supports the various cyber investigations it conducts.*

*FO Requires contractor support services to carry out its mission objectives.*

*@ Required*

1. Why is this needed?

*@User: Explanation Describe the mission or statutory requirement the effort is supporting*

*@LLM: Example Answer Title III of the E-Government Act, entitled the Federal Information Security Management Act (FISMA) requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and information systems that support the operations and assets of the agency. FO Requires contractor support services in order to carry out its mission objectives*

*@Optional*

1. What is the problem it is fixing?

*@User:* *Explanation Address the root issue, what has happened that requires this supply/service. For example, the checkpoint is too far away from the potable water supply, therefore, bottled water is needed for the TSOs at the checkpoint.*

*@LLM: Example Answer – This support will help protect the TSA Infrastructure from cyber intrusion and prevent network exploitation and the exfiltration of sensitive TSA data.*

*@Optional*

1. Who needs the requirement?

*@User: Explanation* *is it support for TSA HQ operations for overall mission support or direct field support at an airport?*

*@LLM: Example Answer FO Requires contractor support services to carry out its mission objectives*

*@Optional*

1. What is the purpose of the requirement?

*@User: Provide a concise statement that describes the purpose you are trying to achieve. Provide a short scope to present an idea of the size and range. Provide specific result.*

*@LLM: Example Answer - The purpose of this requirement is the procurement and delivery of professional services to support the Transportation Security Administration (TSA)/Information Technology (IT)/Information Assurance Division (IAD) Focused Operations (FO) Branch to maintain an operational capability that combines multiple disciplines of advanced cyber analytics.*

*FO is seeking contractor support to assist them in the accomplishment of their mission and provide highly adaptive, highly advanced cybersecurity support services that:*

1. *Expand TSA’s capacity to test their high-priority IT systems;*
2. *Rapidly address potential vulnerabilities; and*
3. *Stop adversaries before they impact TSA’s networks*

*@Required*

1. Is there a general scope or required range that would be helpful to

prospective vendors?

*@User:* *A general scope will provide clarity into the requirement and assist prospective vendors in preparing their proposal to meet the government’s needs. The scope focuses on how the objectives of the action will be accomplished.*

*@LLM: Example Answer The Operations and Maintenance (O&M) coverage will be applied to identified TSA A/V and VTC configurations throughout the nation. These locations mainly consist of airports and the National Capitol Region (NCR). TSA also supports A/V and VTC configurations at smaller office sites. Throughout the nation, there are currently two hundred and twenty-nine (229) A/V and VTC systems, as well as one hundred and fifteen (115) at*

*TSA Headquarters (HQ).*

*@Optional*

1. What is the desired outcome?

*@User: Explanation* *The outcome can be expressed as objectives to be met, successful results, or delivery of a product.*

*@LLM: Example Answer The* ***intent of this task order is to assist FO in accomplishing the following objectives:***

*Successful collaboration and coordination of activities with all FO stakeholders (as needed) including the TSA SOC. Success is defined as accomplishing the mission while ensuring stakeholder relations remain cordial and without friction.*

*Successful cyber investigative digital forensic examinations.*

*Successful cyber threat emulation operations on TSA systems.*

*Successful malware analysis, cyber threat intelligence and digital forensics and cyber threat hunt operations.*

*Successful completion of all* ***forensic lab management*** *activities to include case intake/outtake, monthly inventory of FO Branch assets, cleaning and other activities that ensure the security of the Forensic lab property. All assets, actors, licenses will be accounted for and protected per TSA security policy. Asset loss must be avoided without failure. Asset accountability must be maintained at all times.*

*Successful completion of malware analysis, cyber threat intelligence and digital forensics, cyber threat hunt operations on TSA systems on a* ***24x7*** *(24 hours, 7 days a week) as needed basis.*

*Successful installation, deployment and implementation of our Security Validation and Breach Simulation system on TSA systems. This includes the successful and continuous execution of tests as well as analysis of the results that proactively alert on drift from a known-good baseline and validate control configurations.*

*Successful Litigation and FOIA support to multiple stakeholders utilizing the electronic discovery reference model process and pre-discovery planning.*

*Successful installation, deployment and implementation of JIRA (or similar product) and Elastic on TSA and/or DHS component systems.*

*Successful implementation of security validation IT environments at scale to test the effectiveness of network, endpoint, email and cloud controls.*

*Successful hunting on the TSA networks to identify suspicious, malicious, and anomalous activity.*

*Successful data analytic activities that include the collection, transformation and organization of data to help leadership to improve cybersecurity processes, identify opportunities and trends, purchase and launch new products, provide great customer service and make thoughtful decisions. The insights and gains gathered from the analysis will lead to effective and efficient action.*

*Successful threat emulation that converts newly identified unknown attacks into known signatures and deploys them making it possible to block these threats before they have a chance to become widespread on the TSA networks.*

*Successful development of projects using Elastic, JIRA, Python, Splunk, Tanium, Bro and other tools.*

*Successful creation and delivery of cyber threat briefings on a weekly (minimum) basis.*

*Successful establishment and execution of processes, procedures and created content within Bro, Splunk, and Tanium in coordination with the TSA Security Operations Center (SOC)/National Operations Center (NOC).*

*Successful design, build and maintenance of the FO Analysis Network to include the hunt and threat emulation networks, case management, tactical operations and cyber investigative tracking systems.*

*@Required*

1. What is the technical requirement?

*@User: The Requirement document should describe clearly the specific requirements and work required of the contractor**. Tasks are activities that are required to produce the deliverables, services and/or outcomes. These should be defined and detailed.*

*@LLM: Example Answer* ***The Contractor shall perform each of the tasks detailed in the sections below:***

1. *Provide personnel who are specialists within their security discipline and have verifiable experience and/or training in information assurance, IT security, data science and analysis, network intrusion identification and detection (hunt) and focused Incident response (IR), cyber tactical operations and execution, cyber threat emulation operations and execution, malware reverse engineering, development and execution, software development of custom data analysis tools, data science, network maintenance and special projects engineering, litigation support/FOIA, digital forensics, cyber threat intelligence and cyber insider threat.*
2. ***Ensure that all Contractor personnel:***
3. *Understand TSA IT systems, TSA IT security policies, and TSA IT operational groups and Intelligence Community (IC) standards, guidelines and policies.*
4. *Use various information sources (including public, private, and classified sources) to monitor for threats and vulnerabilities on-site at TSA HQ using tools provided by the TSA FO Branch.*
5. *Support the daily operations of the TSA FO Branch on-site at TSA HQ. Support must also be provided on-site at other TSA locations located within the National Capital Region (NCR). Support shall include, but is not limited to tasks of the following nature:*
6. *Managing the daily activities in the Forensic lab to include evidence Intake/Outtake activities, escorting, inventory etc.*
7. *Documenting the day-to-day activities of the personnel within the FO Branch forensics laboratory.*
8. *Developing and maintaining the weekly reporting of FO Branch activities that identify accomplishments and goals.*
9. *Participating in IT security meetings and briefings on-site at TSA HQ.*
10. *Attending Enterprise Architecture meetings and briefings as required on-site at TSA HQ.*
11. *Responding to and mitigating cyber threats; where applicable.*
12. *Support the underlying mission while leveraging budget projections, identifying limitations and planning for contingencies in certain circumstances.*
13. *Avoid major risks in areas that aren’t part of the core mission.*
14. *Establish continuity clauses that ensure limited disruption to the mission operations while improving the competitive posture.*
15. *Maintain clear lines of communication between parties and guarantee mutually beneficial relationships.*
16. *Deliver grammatically correct documentation (i.e. SOPs, Case Reports, ROEs etc.) to include correct spelling and subject/verb agreement.*
17. *Utilize only approved government networks and devices to view, analyze, create, process, or store classified information.*
18. *Ensure all documentation is maintained and current. Updates are applied monthly (minimum).*
19. *Follow department procedures and protocols for troubleshooting and resolving issues as well as handling challenging situations.*
20. *Maintain on-site and off-site continuity and integrity of exhibits, detailed recording and retention of information, secure storage and backup of data, and evaluation of completed analyses.*
21. *Document, design and develop documentation on solutions provided.*
22. *Have sufficient skill sets and knowledge to support limited duration "surge" capabilities to assist Critical Infrastructure and Key Resource (CIKR) partners to respond to major security incidents.*
23. *Have a surge capability that may range from phone consultation to on-site support with containment, eradication, remediation activities, evidence acquisition and investigation during non-business hours for all tasks; as needed.*
24. *All travel is authorized by the TSA prior to incurring any expense and invoiced under the appropriate CLIN in accordance with the applicable Government Travel regulations.*
25. *Have computing capabilities to support on-site and off-site Incident Response capabilities (i.e. fly-away kits).*
26. *Maintain clear lines of communication between parties and guarantee mutually beneficial relationships.*

*@Required*

1. Is there any pertinent technical information that potential vendors need to be aware of?

*@User: For example: historical data relating to the effort, number of cases, baggage throughput, airport size etc.* *If all technical information has been provided, answer “no further information is needed.”.*

*@LLM: Example Answer The following information is provided to demonstrate the estimated labor hours for the subject requirement for each task area.  This data is not provided as a requirement, nor is this data meant to define a level of effort required under this scope of work. This historical estimated data is shared for informational purposes only and may not capture increases as a result of anomalies (non-standard fluctuations within scope) encountered in any given year.*

|  |  |  |
| --- | --- | --- |
| *TASK* | *Estimate*  *Hours* | *Estimate*  *FTEs* |
| *Task 1 - FO ADET and ENG/DEV Services - Data Science and Analysis* |  | *1* |
| *Task 2 - FO ADET and ENG/DEV Services - Network Intrusion Identification and Detection (Hunt) and FO Incident Response (IR)* |  | *2.5* |
| *Task 3 - FO ADET and ENG/DEV Services - Cyber Tactical Operations and Execution* |  | *0.5* |
| *Task 4 - FO ADET and ENG/DEV Services -  Cyber Threat Emulation Operations and Execution* |  | *2.5* |
| *Task 5 - FO ADET and ENG/DEV Services - Malware Reverse Engineering, Development and Execution* |  | *1.5* |
| *Task 6 - FO ADET and ENG/DEV Services - Software Development of Custom Data Analysis Tools* |  | *2* |
| *Task 7 - FO ADET and ENG/DEV Services - Network Maintenance and Special Projects Engineering* |  | *4* |
| *Task 8 - FO ADDA and CTU/I Services - Litigation Support/Freedom of Information Act (FOIA)* | *Up to 80 hours per case.  1 – 256 custodians per case* | *3* |
| *Task 9 - FO ADDA and CTU/I Services - Digital Forensics* | *Up to 360 hours per case.  1 – 25 custodians per case* | *3* |
| *Task 10 - FO ADDA and CTU/I Services - Cyber Threat Intelligence* |  | *3* |
| *Task 11 - FO ADDA and CTU/I Services - Cyber Insider Threat* |  | *2* |
| *Task 12 - All FO Services (FO ADDA, ADET, ENG/DEV and CTU/I Services) - Program Management* |  | *1* |
| *Task 13 - FO ADDA and CTU/I Services - Forensic Lab Management* |  | *1* |
| *Task 14 - FO ADET and ENG/DEV Services -* ***Transition-In*** *(9/29/2022 or FO Services Pop Start Date plus Not-to-exceed 6 months)* |  | *14* |
| *Task 15 - FO ADDA and CTU/I Services –* ***Transition-In*** *(Estimated TSA transfer of CND Services Award Date 01/23/23 plus Not-to-exceed 6 months)* |  | *13* |
| *Task 16 - All FO Services -* ***Transition-Out*** *(6 months prior to FO Services Pop End Date)* |  | *27*  *(Total)* |

*In addition to the information in the above table, the following historical information is provided:*

*Focused Operations Case/Tech Statistics:*

1. *Total FO Cases Processed Per Year (average):   114*
2. *# of Stakeholder Offices Supported: 10 +*
3. *Domestic Travel for Technical Operations Per Year:  6 trips (minimum) / 2 CTRs per trip*
4. *Remote Technical Operations Conducted Per Year:  28*
5. *Audit and Other Security Logs Analyzed Per Day:  \*8 GB + (\*Number set to increase as new data continues to be ingested into security tools)*

*@Optional*

1. What are the specific tasks that are required of the Contractor?

*@User: Explanation* *The specific details regarding the required effort must be provided. If this is a service effort, the hours of availability must be addressed, 8-5, 24/7, etc*

*@LLM: Example Answer Task 1 – FO ADET and ENG/DEV Services - Data Science and Analysis*

*The purpose of this task is to collect, transform, organize and analyze cyber intelligence and other cybersecurity data regarding cybersecurity threats associated with trusted insiders as well as provide analytic support to cyber intelligence-related tactical operations. This analysis is designed and intended to help leadership to improve cybersecurity processes, identify opportunities and trends, purchase and launch new products, provide great customer service and make thoughtful decisions. The insights and gains gathered from the analysis will lead to effective and efficient action.*

***In support of this task the Contractor shall:***

1. *Implement cybersecurity use cases within the FO platforms to identify threat activity indicative of high risk users and sophisticated threat actors.*
2. *Use targeted data ingestion and searching in order to find anomalous and malicious activity on the TSA networks working towards the detection and remediating of sophisticated security threats to the TSA environment.*
3. *Perform advanced analysis to better comprehend, synthesize, and leverage complex scenarios.*
4. *Conduct analysis and assessments of the TSA historical security events and incidents data and other information as appropriate to assess trends and develop a variety of metrics on vulnerabilities, attacks, hacks, phishing, spam, DoS, viral infections, and other security incidents/breaches perpetrated on or against the TSA enterprise systems, IT infrastructure, TSA Personnel or TSA contractors.*
5. *Identify and create intelligence requirements through practices such as threat modeling.*
6. *Generate threat intelligence to detect, respond to, and defeat focused and targeted threats.*
7. *Learn the different sources to collect adversary data and how to exploit and pivot off of it.*
8. *Report: by week, month, quarter, and year, number of attacks/cases by attack/case type, ratio of attack type to aggregate attack volume, number of successful attacks, trends by attack type, overall trends, breaches by attack type, breaches trends, Incident Severity and criticality trends, and other metrics as requested by the TSA FO Branch Manager, or designee, and agreed upon by the Contractor. Incorporate intelligence data into this analysis (classified and unclassified).*
9. *Conduct other analysis and assessments of historical security incident and breaches data as requested by the TSA FO Branch Manager, or designee.*
10. *Make recommendations to the TSA FO Branch Manager, or designee to improve security in risk areas identified by analysis and security event metrics compiled and perform this service on an on-going basis and utilize the results to improve FO services and where applicable generate appropriate correlation rules and detection logic in the TSA FO Data Analytics Tool.*
11. *Deliver the results of the analysis formally from trend analysis and security event metrics on a weekly, monthly and quarterly basis to the FO Branch Manager and others as designated.*
12. *Validate information received externally to minimize the costs of bad intelligence.*
13. *Transform complex data into valuable insights and actions.*
14. *Mine and analyze data from a range of sources as well as understand machine learning.*
15. *Unlock valuable and predictive insights that will influence efficient and effective cybersecurity procurement decisions.*
16. *Ensure detection of Indicators of Compromise (IOCs) by creating alerts in formats such as YARA, OpenIOC etc.*
17. *Move security maturity past IOCs into understanding and countering the behavioral tradecraft of threats.*
18. *Establish structured analytical techniques to successfully accomplish the different security roles.*
19. *Analyze the data and draw logical conclusions and then express to key stakeholders why those data points are significant.*
20. *Analyze an adversary's intent, opportunity, and capability to do harm to develop actionable information that answers key knowledge gaps, pain points, or requirements of an organization.*

*Data Science and Analysis - Performance Requirements:*

1. *Assist the developers with the creation of a tool or toolset that will enhance our data analytic capabilities by providing an efficient, automated platform for the analysis of cyber security cases, cyber threats, cyber intelligence and incident trending analysis. Predictive analytics is required throughout the period of performance of the contract.*
2. *All documentation is maintained and current. Updates are applied monthly (minimum).*
3. *Provide biweekly statistical reporting associated with their findings (trends etc).*
4. *Solve operational cybersecurity data analytical challenges to avoid adversarial impact to the organization’s mission.*
5. *Explore and draw conclusions about the organization’s cybersecurity posture to assist with policy and budget decision making. Match data to usernames, locations, organizations, job descriptions, internal/external events, intelligence. cases, incidents etc.*

*Task 2 - FO ADET and ENG/DEV Services - Network Intrusion Identification and Detection (Hunt) and FO Incident Response (IR)*

*The purpose of this task is to hunt for cyber threats from daily operations and disseminate findings within 24 hours of discovery and provide those services on a 24x7 (24 hours, 7 days a week) basis. While the contractor will perform “onsite” hunting during normal business hours. The hunting staff is required to maintain their availability on a 24x7 basis as cyber incidents requiring action can occur at any time and on any day. The hunt activity includes using targeted data ingestion and searching in order to find anomalous and malicious activity on the TSA networks working towards the detection and remediating of sophisticated security threats to the TSA environment. The team will search for abnormal behaviors on the network, to include network traffic, host information, user activities, and other sources of information. The team provides the coordination and implementation of the core team activities, including server or host, network, and planning functions, to detect, mitigate, and eliminate Advanced Persistent Threats (APTs) from client systems, networks, and data. Analysis of host and network data is performed to identify threats against the systems and networks. Coordination of the operations is conducted with the client and the project lead. In-depth analysis of computer network and host data is conducted to determine threat patterns and unusual behaviors to identify potential Tactics, Techniques, and Procedures (TTPs) employed by adversarial APTs and identify related APT activities and malware within operational networks and systems.*

*The primary purpose of Cyber Hunt services is to proactively and iteratively detect, isolate, and neutralize advanced threats that evade automated security solutions. Cyber Hunt activities start with the premise that threat actors known to target some organizations in a specific industry, or specific systems, are likely to also target other organizations in the same industry or with the same systems. Cyber Hunt activities use information and threat intelligence specifically focused on the proximate incident to identify undiscovered attacks, and investigate and analyze all relevant response activities.*

*Cyber Hunt tasks include: collecting intrusion artifacts (e.g., source code, malware, and trojans) and using discovered data to enable mitigation of potential Computer Network Defense incidents within the enterprise; coordinating with and providing expert technical support to enterprise-wide Computer Network Defense technicians to resolve Computer Network Defense incidents; and correlating incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.*

*Deliverables for Cyber Hunt include, but are not limited to, a Cyber Hunt Report including an artifact list, a summary of potential incidents and resolved incidents, and remediation recommendations for vulnerabilities found based on previous incident data.*

***Knowledge Areas include, but are not limited to:***

1. *Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored])*
2. *Knowledge of general attack stages (e.g., foot-printing and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks, etc.)*
3. *Knowledge of incident categories, incident responses, and timelines for responses.*

***In support of this task and the activities listed above, the Contractor shall:***

1. *Support improvement of Cyber Defense capabilities through development of SOC use cases and detection techniques.*
2. *Perform hunt operations to analyze the overall TSA data systems security posture and to propose improvements. The work will be performed over the period of the contract with a minimum of six trips to field sites to gain perspective from operational personnel. The Contractor shall:*
3. *Develop implementation plans for improvement.*
4. *Provide recommendations and assistance regarding implementation requirements.*
5. *Allow for Government review of findings and recommendation and selection of a preferred improvement strategy.*
6. *Be responsible for the application of defensive cyber counter infiltration operations against APTs and perform host level analysis. This includes identifying incidents, malicious code, malicious binary network traffic, and behavioral analysis.*
7. *Produce all reports in both a classified and unclassified version for distribution to other TSA departments as well as other agencies and organizations within the IC.*
8. *Work with other agencies and organizations within the IC at the direction of designated government TSA FO team leads.*
9. *Research and apply pertinent cyber intelligence within two business day of issuance by the IC.*
10. *Create and deliver Cyber Security Incident Reports.*
11. *Provide support to SOC requests including the triage and analysis of requests from the SOC.*
12. *Provide support to the SOC and FO to perform host level analysis. This includes identifying incidents, continuing analysis to requests, malicious code, malicious binary network traffic, and behavioral analysis.*
13. *Provide threat and vulnerability findings within four hours of validation to the TSA SOC and FO Threat Analysts for tracking and the deployment of proactive countermeasures.*
14. *Properly validate threats/vulnerabilities in accordance with the source, criticality of the device, availability of test devices, etc.*
15. *Attend and participate in weekly DHS/FO meetings and participate in weekly TSA Network Intrusion Working Group meetings with the TSA SOC.*
16. *Accept escalation of suspected threats and vulnerabilities from multiple sources, internal and external.*
17. *Use data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs etc.) to analyze events that occur within their environments for the purposes of mitigating threats.*
18. *Develop cyber indicators to maintain awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber threat/warning assessments.*
19. *Analyze data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.*
20. *Conduct advanced analysis of collection and open-source data to ensure target continuity, profile targets and their activities, and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks, and the applications on them.*
21. *Analyze digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.*
22. *Analyze threats and vulnerabilities to determine their impact upon the TSA IT systems.*
23. *Generate threat intelligence indicators during the course of Hunt operations and apply/fine tune them across the enterprise network.*
24. *Conduct cybersecurity analysis and research in support of FO investigations.*
25. *Examine malicious software, such as bots, worms, and Trojans, to understand the nature of the threat.*
26. *Follow department procedures and protocols for troubleshooting and resolving issues.*
27. *Use a wide range of software applications and tools to diagnose and resolve issues.*
28. *Identify the necessary actions to proactively mitigate risks posed by threats and vulnerabilities.*
29. *Develop, research and maintain proficiency in tools, techniques, countermeasures, and trends in computer and network vulnerabilities, data hiding, and encryption.*
30. *Successfully and continuously execute tests and analyze results that proactively alert on drift from a known-good baseline and validate control configuration.*
31. *Actively hunt the TSA network to identify suspicious, malicious, and anomalous activity.*
32. *Provide processes and procedures and created content within, Elastic, Splunk and Tanium.*

*Network Intrusion Identification and Detection (Hunt) – Incident Response - Performance Requirements:*

1. *Conduct daily hunt analysis of data to identify and detect malicious and or anomalous activity.*
2. *Conduct 6 – 12 special hunt ops as directed by FO leadership. These special operations are generally related to specific incidents that require focused hunt analysis of a specific system’s architecture and security posture. Provide the associated final reports and briefs for information sharing and action to mitigation.*
3. *Be accountable for utilizing a range (3 or more) of intelligence and other cybersecurity resources to hunt for threat actors across the Enterprise.*
4. *Provide, maintain and brief all hunt successes bi-weekly and as requested. These should be accompanied by final reports that include the evidence discovered.*
5. *Supports the underlying business cases while identifying limitations and planning for contingencies.*
6. *Avoids major risks that aren’t part of the core, cybersecurity mission.*
7. *Establishes continuity clauses that ensure limited disruption to daily operations while improving the competitive posture.*
8. *Completes* ***up to 12*** *hunt operations per year.*
9. *Completes all required documentation* ***prior to*** *each hunt operation. The require documentation includes:*
   1. *Threat Hunt Operations plans to include:*
      1. *Notifications to “approved” stakeholders (Leadership, TSA SOC etc.)*
      2. *Provision of technical information to the “approved” stakeholders for de-confliction purposes.*
      3. *Contingency planning*
10. *Completes all required activities* ***upon completion*** *of each Threat Hunt operation.* 
    1. *Threat Hunt Final Reports that include:*
       1. *Findings*
       2. *Recommendations*
       3. *Provision of all findings for the creation of POAMs for remediation.*
    2. *Threat Hunt Oral Presentations that include the final report contents.*
       1. *PPT and oral brief of the operation at the Biweekly Brief*
       2. *PPT and oral brief to other stakeholders, as required.*
11. *All documentation is maintained and current. Updates are applied monthly (minimum).*
12. *Ensures that the follow documentation is updated monthly and remains current:*
    1. *Threat Hunt SOP(s)*
    2. *Threat Hunt equipment and software (all current security updates/patches applied)*
13. *Provides support, documentation to and other threat emulation duties required for the DHS CSP audit held every 3 years.*

*Task 3 - FO ADET and ENG/DEV Services - Cyber Tactical Operations and Execution*

*The purpose of this task is to provide cyber tactical operations and execution support to level the cyber battlefield. This includes altering an enemy’s perception of reality through delays and disinformation which can reveal attack methods and provide the attributions needed to identify the adversary’s strategy. Delaying and dissuading also provides the essential time for FO’s forensics team to analyze, identify, and mitigate attack vectors that could expose inherent vulnerabilities to operational and support systems.*

***In support of this task the Contractor shall:***

1. *Build and maintain a Tactical Operations system.*
2. *All documentation is maintained and current. Updates are applied monthly (minimum).*
3. *Monitor and report on all Tactical Operations system activity.*
4. *Provide timely reporting of all tactical operations activity/incidents as designated by the FO Branch Manager (FO COR and BM) or designee.*

*Cyber Tactical Operations and Execution - Performance Requirements:*

1. *Effectively detect attacks that have infiltrated an organization's network*
2. *Attacker control*
3. *Understand and identify what assets have been compromised (who, how, why, when etc)*

*Task 4 - FO ADET and ENG/DEV Services - Cyber Threat Emulation Operations and Execution*

*The purpose of this task is to provide a Threat Emulation Team (TET) to search for abnormal behaviors on the network, to include network traffic, host information, user activities, and other sources of information. The team provides the coordination and implementation of the core team activities, including server or host, network, and planning functions. They use tactics, techniques, and procedures (TTPs) to emulate real-world threats in order to train and measure the effectiveness of the people, processes, and technology used to defend environments.*

***In support of this task the Contractor shall:***

1. *Utilize authorized tools that are both native and deployed to the environment to perform Threat Emulation Team activities.*
2. *Use TTPs to emulate real-world threats in order to train and measure the effectiveness of the people, processes, and technology used to defend environments.*
3. *Engage with other TSA offices to gain access to various information sources to support Threat Emulation Team activities.*
4. *Review all information collected that can provide indicators of abnormalities or malicious activity.*
5. *Generate threat intelligence indicators during the course of Threat Emulation operations and apply and fine tune them across the enterprise network.*
6. *Research and remain up to date with emerging threats and Threat Emulation methodologies.*
7. *Utilize the Cyber Threat Framework (ODNI) and production of Threat Emulation findings in said format.*
8. *Map Cyber Key Terrain and generate priority target lists.*
9. *Provide recommendations on enhancing the Threat Emulation Team capabilities.*
10. *Engage in project meetings to gain knowledge of changes to the infrastructure and information sources that will aid the Threat Emulation Team.*
11. *Conduct research on commercial and open source tools that may address capability gaps in detecting and/or blocking malicious activity. The TET leverages the full spectrum of TTPs of sophisticated threat actors and assists in verifying and improving cyber defense detection capabilities.*
12. *Be familiar with: development of attack vectors, system and infrastructure reconnaissance, collection of open‐source intelligence, enumeration, and foot-printing of target networks and services, and develop exploit payloads and system backdoors.*
13. *Create and edit customized scripts utilized in Threat Emulation operations, preferably in Python or Power Shell.*
14. *Simulate attacker behavior through external penetration, exploit development, and lateral movement.*
15. *Conduct in-depth analysis of computer network and host data to determine threat patterns and unusual behaviors to identify potential TTPs employed by adversarial APTs and identify related APT activities and malware within operational networks and systems.*

*Cyber Threat Emulation Operations and Execution - Performance Requirements:*

1. *Conduct 6 – 12 special threat emulations operations as directed by FO leadership. These special operations are generally related to specific incidents that require focused emulation analysis of a specific system’s architecture and security posture. Provide the associated final reports and briefs for information sharing and action to mitigation.*
2. *Be accountable for utilizing a range (3 or more) of intelligence and other cybersecurity resources for threat emulation operations.*
3. *Provide, maintain and brief all threat emulation successes at the completion of each operations and as requested. These should be accompanied by final reports that include the evidence discovered.*
4. *Supports the underlying business cases while identifying limitations and planning for contingencies.*
5. *Avoids major risks that aren’t part of the core, cybersecurity mission.*
6. *All documentation is maintained and current. Updates are applied monthly (minimum).*
7. *Establishes continuity clauses that ensure limited disruption to daily operations while improving the competitive posture.*
8. *Completes* ***up to 12*** *Threat Emulation operations per year.*
9. *Completes all required documentation* ***prior to*** *each Threat Emulation operation. The require documentation includes:*
   1. *Threat Emulation Operations plans to include:*
      1. *Notifications to “approved” stakeholders (Leadership, TSA SOC etc.)*
      2. *Provision of technical information to the “approved” stakeholders for de-confliction purposes.*
      3. *Contingency planning*
10. *Completes all required activities* ***upon completion*** *of each Threat Emulation operation.* 
    1. *Threat Emulation Final Reports that include:*
       1. *Findings*
       2. *Recommendations*
       3. *Provision of all findings for the creation of POAMs for remediation.*
    2. *Threat Emulation Oral Presentations that include the final report contents.*
       1. *PPT and oral brief of the operation at the Biweekly Brief*
       2. *PPT and oral brief to other stakeholders, as required.*
11. *Ensures that the follow documentation is updated monthly and remains current:*
    1. *Threat Emulation Program Rules of Engagement*
    2. *Threat Emulation SOP(s)*
    3. *Threat Emulation Test environment (all current security updates/patches applied)*
    4. *Threat Emulation equipment and software (all current security updates/patches applied)*
12. *Provides support, documentation to and other threat emulation duties required for the DHS CSP audit held every 3 years.*

*Task 5 - FO ADET and ENG/DEV Services - Malware Reverse Engineering, Development and Execution*

*The purpose of this task is to create “benign” malware products for all assessments and ad-hoc projects. This includes testing internal/external defenses through custom exploitation development contextual to the TSA environment. This also involves designing, implementing and maintaining a threat simulation lab managed for use during Threat Emulation exercises. This task will provide these services on a 24x7 (24 hours, 7 days a week) basis. While the contractor will perform “onsite” malware tasks during normal business hours. The malware staff shall maintain their availability on a 24x7 basis as cyber incidents requiring action can occur at any time and on any day.*

***In support of this task the Contractor shall:***

1. *Create and deliver classified and unclassified intelligence reports based on intelligence, threats, and vulnerabilities utilizing proper safeguards.*
2. *Create “benign” malware products (Malware Development) for all assessments and ad-hoc projects.*
3. *Test internal/external defenses through “custom” exploitation development contextual to the TSA environment.*
4. *Design, implement, maintain a threat simulation lab managed for use during Threat Emulation exercises.*
5. *Set up and maintain a lab network to test exploitation techniques and software, and also provide an environment for training defenders on attack scenarios.*
6. *Provide leadership in coordinating, assessing, and developing Advanced Threat Emulation Team operations.*
7. *Automate tasks via scripting and/or custom code programs.*
8. *Maintain and gather intelligence from daily operations and disseminate within 24 hours of discovery.*
9. *Support improvement of Cyber Defense capabilities through development of SOC use cases and detection techniques.*
10. *Produce After action reports with findings in addition to details on how the target could have mitigated or prevented the action on objective.*
11. *Follow department procedures, protocols, and rules of engagement when conducting Advanced Threat Emulation Team operations.*
12. *Be responsible for the application of defensive cyber counter infiltration operations against APTs and perform host level analysis. This includes identifying incidents, malicious code, malicious binary network traffic, and behavioral analysis.*

*Malware Reverse Engineering, Development and Execution – Performance Requirements:*

1. *Provide reverse engineering of all malicious artifacts as needed.*
2. *Provide malware development and execution as a part of the 6 – 12 special threat emulations operations as directed by FO leadership. These special operations are generally related to specific incidents that require focused emulation analysis of a specific system’s architecture and security posture. Provide the associated final reports and briefs for information sharing and action to mitigation.*
3. *All documentation is maintained and current. Updates are applied monthly (minimum).*
4. *Be accountable for utilizing a range (3 or more) of intelligence and other cybersecurity resources for malware development and execution to support the threat emulation operations.*
5. *Provide, maintain and brief the malware development and execution portion of all threat emulation exercises at the completion of each operation and as requested.*
6. *Supports the underlying business cases while identifying limitations and planning for contingencies.*
7. *Avoids major risks that aren’t part of the core, cybersecurity mission.*
8. *Establishes continuity clauses that ensure limited disruption to daily operations while improving the competitive posture.*
9. *Completes* ***up to 12*** *malware development and execution activities in support of the Threat Emulation operations per year.*
10. *Support the completion of all required documentation* ***prior to*** *each Threat Emulation operation. Contingency planning*
11. *Support all required activities* ***upon completion*** *of each Threat Emulation operation.*
12. *Provides support, documentation to and other threat emulation duties required for the DHS CSP audit held every 3 years.*

*Task 6 - FO ADET and ENG/DEV Services - Software Development of Custom Data Analysis Tools*

*The purpose of this task is to provide software development support to assist in the creation and refinement of specialized and customized FO data analytic tools. This function is expected to be multidisciplinary, with the ability to support other services within the FO Branch.*

***In support of this task the Contractor shall:***

1. *Develop and implement a single Commercial-off-the-Shelf (COTS) Cyber Threat Intelligence Lifecycle Analytics platform for use in the FO environment.*
2. *Multitask and be flexible to provide cross-functional support.*
3. *Research and develop tools for eDiscovery, forensics, cyber intelligence, threat emulation, advanced detection and identification and high risk user monitoring operations.*
4. *Develop a mechanism for tracking cases.*
5. *Perform software development, testing, and deployment of specialized tools used for big data analytics and other projects as assigned related to:*
6. *Cyber Threat Intelligence, Detection & Identification Platform*
7. *Enterprise Tactical Operations Tool*
8. *Case Tracking Tool*
9. *Other Tools (as requested)*
10. *Utilize aspects of the Agile process to measure different aspects of the development process to completion.*
11. *Implement automation and orchestration capabilities within the FO environment.*
12. *Document design and development documentation on solutions provided.*
13. *Follow department procedures and protocols for troubleshooting and resolving issues.*
14. *Use a wide range of software applications and tools to diagnose and resolve issues.*
15. *Maintain, configure, and install all supported hardware and software residing within EAS and provides support for all FO engineering special projects.*

*Software Development of Specialized, Custom Data Analytics Tools – Performance Requirements:*

1. *Provide a development plan for each development projects within 1 month of project commencement that should include:*
   1. *Phases of the development process*
   2. *Timeline*
   3. *Description of the project*
   4. *Project Status*
   5. *Other items as needed*
   6. *Software, hardware, license requirements*
   7. *Security measures*
2. *All documentation is maintained and current. Updates are applied monthly (minimum).*
3. *Aspects of the Agile process that ensure the development of an easy to use, maintain and secure product is developed.*
4. *Provide biweekly status updates to FO leadership.*

*Task 7 - FO ADET and ENG/DEV Services - Network Maintenance and Special Projects Engineering*

*The purpose of this task is to provide a Security Engineering Team (SET) to provide network maintenance, FISMA compliance and special projects engineering support. The SET maintains, configures, and installs all supported hardware and software residing within EAS and provides support for all FO engineering special projects. provide those services on a 24x7 (24 hours, 7 days a week) basis. While the contractor will perform “onsite” maintenance during normal business hours. We require that the staff maintain their availability on a 24x7 basis as cyber incidents requiring action can occur at any time and on any day. This team performs engineering and system administration services on all FO systems located in on-premises, in the cloud and in wireless environments. These systems include threat emulation, custom big data analytics, open-source and COTS/Government-off-the-Shelf (GOTS) tools as listed below:*

1. *Case/Incident, Cyber Threat, Cyber Intelligence Trending Tracking Tool*
2. *Enterprise Tactical Operations Tool*
3. *Litigation Support/FOIA and Forensics Tools*
4. *Hunting and Threat Emulation Tools*
5. *Other FO Development Projects (As Assigned)*

*In support of this task the Contractor shall:*

1. *Implement automation and orchestration capabilities within the FO environment.*
2. *Document, design and development documentation on on-premises and cloud-based solutions provided. Documentation includes standard operating procedures (SOPs), Technical documentation etc.*
3. *Provide support for TSA Public Key Infrastructure (PKI) functions, including system administrative support for creating and setting up certificates on systems. Must provide analysis related to the design, development, security and integration of hardware, software, man-machine interfaces and all system level requirements to provide an integrated IT solution.*
4. *Perform health and wellness monitoring of the FO FISMA Systems.*
5. *Perform administration, maintenance, and updates of forensic applications to ensure they remain function.*
6. *Ensure that updates to applications and systems shall be carefully planned and scheduled so as to not affect any on-going or active investigations.*
7. *Review the health and well-being of all security technologies including firewall, router, Virtual Private Network (VPN), Intrusion Detection System (IDS) sensors, Proxy, wireless, PKI, and switch changes within FO FISMA Systems. The results of which shall be captured and reported in the monthly FO Network Health and Wellness Reports deliverable on a monthly basis.*
8. *Travel to locations where Enterprise Analysis System (EAS) devices are located for system administration and/or repair if needed.*
9. *Ensure that all changes required follow the proper Request for Change (RFC) process, have been approved through the appropriate Change Control Board (CCB) and are properly tested before deployment to the production FO FISMA Systems.*
10. *Recommend and implement technologies/changes that will enhance the operations and/or security of the FO FISMA Systems.*
11. *Document all recommendations and changes and provide it to the FO Branch Manager, or his designee.*
12. *Ensure that all TSA change control processes are followed, and all changes are approved prior to implementation.*
13. *Coordinate with other TSA offices in order to have FO technologies implemented within the TSA Systems.*
14. *Create and deliver Security and Vulnerability Status reports all systems managed by the Contractor on a monthly basis.*
15. *Administer, review and provide recommendations for the following devices, both hardware and software (Windows, Macintosh and UNIX/Linux based), including laptops, desktops, PDAs, printers, mobile computing devices, mobile electronic media, Active Directory Servers, member servers, other workgroup servers outside of the main Active Directory realm, other technology devices such as forensic write blocking, and imaging for the FO FISMA Systems.*
16. *Assist in the management of all Operating Systems, tools and applications utilized by IAD Security Engineers, as needed.*
17. *Develop integrated system test requirement, strategies, devices and systems.*
18. *Conduct overall system level testing and security testing.*
19. *Design and integrate information security suites, tools, capabilities into delivered solutions to ensure federal and commercial security best practices.*
20. *Support TSA IAD Enterprise Projects as an IAD/FO representative on FO Integrated Projects.*

***Network Maintenance and Special Projects Engineering – Performance Requirements:***

1. *Work with the FO leadership team to ensure licenses software and hardware are renewed as needed with adequate leeway for the processing of payments (6 – 8 months).*
2. *Maintain 100% FISMA complaint networks for all FO operations at all times. Provide monthly reporting showing compliance.*
3. *Apply security patches, updates etc. as directed. Some require application within 12 hours of notification.*
4. *All documentation is maintained and current. Updates are applied monthly (minimum).*

*Task 8 - FO ADDA and CTU/I Services - Litigation Support/Freedom of Information Act (FOIA)*

*The purpose of this task is to discover data applicable to legal proceedings such as litigation, government investigations, or Freedom of Information Act (FOIA)requests, where the information sought is in electronic format (often referred to as electronically stored information or ESI). Electronic discovery is subject to rules of civil procedure and agreed-upon processes, often involving review for privilege and relevance before data are turned over to the requesting party. The team will search for based upon “keywords” and “time frames” provided by the requestor. Coordination of the discovery process is conducted with the client and the project lead.*

***Knowledge Areas include, but are not limited to:***

1. *Knowledge of, understanding and experience with the stages of the Electronic Discovery Reference Model (EDRM).*
2. *Knowledge of the Federal Rules of Civil Procedures (FRCP).*

***In support of this task and the activities listed above the Contractor shall:***

1. *Adhere to and utilize and implement all applicable cyber aspects of the EDRM to include the pre-discovery planning process.*
2. *Work across the agency offices and programs to achieve data collection.*
3. *Interface with the office of Chief Council and FOIA to scope, collect and analyze electronic data for use in cases regarding FOIA, civil, and criminal court cases.*
4. *Process a minimum of 25 TB of data per week.*
5. *Sources shall include (but are not limited to), Cloud-based files, Email Files, Text Messages, Call Detail Records, Log Files, Chat Logs.*
6. *Ensure that specialized tasks are completed on the data recovered to include: de-duplication, data culling and de-NISTing.*
7. *Be responsible for all facets of eDiscovery requests associated with FO cases.*
8. *Comply with standard process for eDiscovery as outlined in the Electronic Discovery Reference Model (EDRM to include Identification, Preservation, Collection, Processing, Review and final Reporting.*
9. *Process and track requests for service for all requests received by the eDiscovery team, including verification of all related deliverables.*
10. *Track evidence inventory for intake and release of all evidence items delivered to the eDiscovery team. This includes insuring proper handling and maintenance of evidence and chain of custody records.*
11. *Perform forensics collection of eDiscovery data using EnCase® software and Access Data products, as well as other existing tools.*
12. *Perform daily analytical actions in the performance of eDiscovery and reporting.*
13. *Assist in developing, managing, communicating, and implementing an eDiscovery program.*
14. *Provide reports of such data and categorize and manage large collections of data to maintain file integrity and chain of custody.*
15. *Provide support, reports, and all related deliverables on ‘chain of custody’ matters; and operate and maintain all eDiscovery systems.*
16. *Create and deliver e-Discovery reports on an as needed basis.*
17. *Perform case reviews to insure analysis reports meet acceptable standards as defined by policy.*
18. *Testify as an expert witness and clearly articulate the circumstances with how a case was handled from an evidentiary perspective.*
19. *Work closely with the eDiscovery case requestor and shall provide a status report to the requestor and the TSA FO Branch Manager, or her designee, within two weeks.*
20. *Include a description of the case, start date, target completion date, and a brief explanation for any expected delays in completion.*
21. *Develop and maintain the biweekly eDiscovery activities report that identifies eDiscovery team accomplishments and goals.*

*Litigation Support/FOIA – Performance Requirements:*

1. *Process cases that have completed the FO case intake process and will provide an acknowledgement of receipt to the requestor within 24 hours of receipt.*
2. *Process cases that have completed the FO case intake process and will provide a status report and pre-discovery plan from the analyst to the requestor within 2 days of assignment.*
3. *All documentation is maintained and current. Updates are applied monthly (minimum).*
4. *All eDiscovery best practices and SOPs are followed without failure. (ex. chain of custody, pre-discovery plans, secure containers and evidence handling etc.)*
5. *Court testimony by the examiners will be required as needed.*
6. *eDiscovery case tracking statistics will be provided during the monthly program management review meetings.*

*Task 9 – FO ADDA and CTU/I Services - Digital Forensics*

*The purpose of this task is to enhance TSA’s security posture through digital forensic analysis. FO continually researches and implements forensics and network investigative technologies. The examiners will provide these services on a 24x7 (24 hours, 7 days a week) basis. While the contractor will perform “onsite” forensics during normal business hours. The forensic staff is required to maintain their availability on a 24x7 basis as cyber incidents requiring action can occur at any time and on any day.FO conducts cyber investigations within TSA through the use of host-based forensics, network forensics, log based forensics, cloud forensics, mobile forensics, insider threat, intrusion detection, reverse engineering, and malware analysis. FO maintains its own network that supports the various cyber investigations it conducts.*

***Knowledge Areas include, but are not limited to:***

1. *Knowledge of different deadbox, cloud, virtual and network-based forensic techniques.*
2. *Knowledge of general attack stages (e.g., foot-printing and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks, etc.)*
3. *Knowledge of incident categories, incident responses, and timelines for responses.*

***In support of this task and the activities listed above the Contractor shall:***

1. *Perform forensics collection using EnCase® software and Access Data products, and analyze packet traces and raw log dumps.*
2. *Provide support for, reporting on, and all related deliverables required for ‘chain of custody’ matters.*
3. *Understand computer forensics and provide the TSA FO Branch with individuals having verifiable forensic examination experience and/or certifications.*
4. *Understand and analyze Transmission Control Protocol/Internet Protocol (TCP/IP) and PCAP and provide the TSA FO Branch with individuals having verifiable packet analysis experience and/or certifications.*
5. *Understand and analyze enterprise networks and provide the TSA FO Branch with individuals having verifiable enterprise network experience and/or certifications.*
6. *Include a description of the case, start date, target completion date, and a brief explanation for any expected delays in completion.*
7. *Perform forensics collection using EnCase® software or equal product, and analyze packet traces and raw log dumps.*
8. *Include a description of the case, start date, target completion date, and a brief explanation for any expected delays in completion of cases.*

*Digital Forensics – Performance Requirements:*

1. *Process cases that have completed the FO case intake process and will provide a status report to the requestor within 2 weeks.*
2. *All documentation is maintained and current. Updates are applied monthly (minimum).*
3. *All digital forensic best practices and SOPs are followed without failure. (ex. chain of custody, secure containers and evidence handling etc.)*
4. *Court testimony by the examiners will be required as needed.*
5. *Forensic case reports will be provided within 2 weeks of case analysis completion. The reports will include the evidence found.*

*Task 10 - FO ADDA and CTU/I Services - Cyber Threat Intelligence*

*The purpose of this task is to hunt for cyber threats from daily operations and generate Cyber Threat Intelligence Analysis Reports (CTARS), Threat Profiles for dissemination to various stakeholders. The analysts will provide these services on a 24x7 (24 hours, 7 days a week) basis. While the contractor will perform “onsite” cyber threat intelligence during normal business hours. The analyst staff is required to maintain their availability on a 24x7 basis as cyber incidents requiring action can occur at any time and on any day. This service includes the collection and analysis of intelligence regarding cyber security threats and vulnerabilities as well as the direct and coordinated response to such threats and vulnerabilities. The Contractor performs their duties under the direction and guidance of a Cyber Security Intelligence Lead.*

***Knowledge Areas include, but are not limited to:***

1. *Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non-nation state sponsored], and third generation [nation state sponsored])*
2. *Knowledge of general attack stages (e.g., foot-printing and scanning, enumeration, gaining access, escalation of privileges, ransomware, maintaining access, network exploitation, covering tracks, etc.)*
3. *Knowledge of incident categories, incident responses, and timelines for responses.*

***In support of this task and the activities listed above the Contractor shall:***

1. *Obtain and maintain a current understanding of the TSA IT systems, TSA IT policies, and TSA IT operational groups.*
2. *Have this understanding within 30 days of acceptance on the program.*
3. *Monitor various information sources (including public, private, and classified sources) for threats and vulnerabilities using tools provided by TSA FO.*
4. *Ensure that only approved classified government networks and devices are utilized to view, analyze, create, process, or store classified information.*
5. *Create and deliver Classified Cyber Threat Intelligence Reports based on intelligence, threats, and vulnerabilities utilizing proper safeguards.*
6. *Ensure that all classified information is properly marked, handled, processed, stored, and destroyed as necessary.*
7. *Accept escalation of suspected threats and vulnerabilities from multiple*
8. *sources, internal and external.*
9. *Analyze threats and vulnerabilities to determine their impact upon the TSA IT systems.*
10. *Identify the necessary actions required to proactively mitigate risks posed by threats and vulnerabilities.*
11. *Provide response for advanced attacks to the TSA infrastructure.*
12. *Perform advanced forensic examination and mitigation for advanced attacks to the TSA infrastructure to include suspected zero day attacks.*
13. *Provide malware reverse engineering for all malware in the TSA network that is previously unknown.*
14. *Reverse engineer malware as necessary.*
15. *Provide a detailed malware reverse engineering report within 24 hours of completing the malware reverse engineering. This report shall be produced in both a classified and an unclassified version for distribution to other TSA departments as well as other agencies and organizations within the intelligence community.*
16. *Work with other agencies and organizations within the intelligence community at the direction of designated government TSA FO team members.*
17. *Notify TSA FO regarding procedures and requirements discussed with the intelligence community.*
18. *Research and obtain pertinent cyber-intelligence within 1 business day of issuance by intelligence agencies.*
19. *Create and deliver Cyber Security Incident Reports.*
20. *Provide threat and vulnerability findings within 4 hours of validation to the TSA SOC Threat Analysts for tracking and the deployment of proactive countermeasures.*
21. *Expected to properly validate threats / vulnerabilities in accordance with the source, criticality of the device, availability of test devices, etc.*
22. *Attend a weekly DHS FO meeting and participate in a weekly TSA Network Intrusion Working Group meeting.*
23. *Create and deliver threat briefs and briefings on a daily, weekly, biweekly, quarterly and ad hoc basis.*

***Cyber Threat Intelligence – Performance Requirements:***

1. *Provide daily cyber intelligence reporting specific to our priority requirements.*
2. *All documentation is maintained and current. Updates are applied monthly (minimum).*
3. *Provide reporting for at least 1 meeting per week.*
4. *Provide biweekly (as ad hoc) cyber intelligence briefings that illustrate the results of their analysis and the resultant written products that are understandable by non-technical readers.*
5. *Review intelligence communication on all networks daily and forward to stakeholders as needed.*
6. *Perform daily outreach activities with members of the community for information sharing and timely reporting which includes the collection and delivery of cyber threat indicators.*

*Task 11 – FO ADDA and CTU/I Services - Cyber Insider Threat*

*“The Department of Homeland Security National Cybersecurity and Communications Integration Center advises that “insider threats, to include sabotage, theft, espionage, fraud, and competitive advantage are often carried out through abusing access rights, theft of materials, and mishandling physical devices.” Threats can also result from employee carelessness or policy violations that allow system access to malicious outsiders. These activities typically persist over time, and occur in all types of work environments, ranging from private companies to government agencies.” - CISA*

*The purpose of this task is to collect and analyze intelligence (monitoring) regarding cyber threats associated with trusted insiders as well as process and coordinate the response to such threats. The Contractor performs their duties under the direction and guidance of a Senior Cyber Insider Threat Team Lead.*

***Knowledge Areas include, but are not limited to:***

1. *Knowledge of types insider threats and how to detect them.*
2. *Knowledge of the types of security risks that can exists within the targeted organization. This doesn’t mean that the actor must be a current employee or officer in the organization. They could be a consultant, former employee or other trusted partner.*
3. *Knowledge of incident categories, incident responses, and timelines for responses for insider threat cases.*

***In support of this task and the activities listed above the Contractor shall:***

1. *Provide security event monitoring for all the Transportation Security Administration (TSA) unclassified systems.*
2. *Administer, maintain, and manage the devices performing collection, storage, normalization, integration, and correlation of system and network logs, events, data, and information from various sources in the classified system’s infrastructure.*
3. *Collect, document, correlate and analyze security events and incidents impacting the unclassified systems.*
4. *Analyze network traffic patterns and anomalies expressed within the logs, events, data, and information collected from various sources within the Enterprise.*
5. *Detect, identify and confirm security events, intrusions, attacks, and security breaches.*
6. *Notify the TSA FO Branch Manager, or her designee, the SO and the Information Systems Security Officer (ISSO) of detected security incidents.*
7. *Assist the TSA FO Branch Manager, or his designee, and perform actions in support of the TSA Cyber Insider Threat program.*
8. *Create, maintain and continually update SOPs, guidelines, reports and other documents pertaining to the operation, maintenance and upkeep of the TSA Cyber Insider Threat program.*
9. *Collaborate, communicate and coordinate with other TSA and DHS components, and/or any other group or entity, to support and facilitate the remediation, mitigation and resolution of security incidents that transpired on TSA’s classified networks.*
10. *Ensure that the services provided under this contract continuously adapt and evolve as technological advancements (i.e. mobile computing, IPv6, etc.) and DHS departmental policy changes occur.*
11. *Look for detect security events, intrusions, attacks, policy violations, and security breaches associated with insider threats.*
12. *Notify the TSA FO Branch Manager of security incidents detected on TSA’s unclassified networks.*
13. *Analyze logs and events from any other device types which may send logs or events to the insider threat system for analysis.*
14. *Open a case in the TSA FO Branch ticket management system for all cyber investigations performed, or security incidents handled, as part of this service.*
15. *Upon detection or notification of a critical security event or insider threat, open an investigation in the TSA FO Branch ticket management system within 30 minutes from detection, identification or notification.*
16. *Collect and maintain information pertinent to security investigations and incidents in a form which can support current and/or future analysis, situational awareness, and law enforcement investigation efforts.*
17. *Assess and report the risk or threat level of suspected or confirmed incidents.*
18. *Provide documentation detailing any additional information that it will collect and maintain for each security investigation.*
19. *This documentation shall be submitted for review and acceptance by TSA FO Federal employees within 30 calendar days from this contract award.*

***Cyber Insider Threat – Performance Requirements:***

1. *Provide reporting for at least 1 meeting per week.*
2. *Provide biweekly (as ad hoc) insider threat briefings that illustrate the results of their analysis, trends and the resultant written products that are understandable by non-technical readers.*
3. *All documentation is maintained and current. Updates are applied monthly (minimum).*
4. *Review insider threat-related communication on all networks daily and forward to stakeholders as needed.*
5. *Perform daily outreach activities with members of the community for information sharing and timely reporting which includes the collection and delivery of threat indicators.*

*Task 12 - All FO Services (FO ADDA, ADET, ENG/DEV and CTU/I Services) - Program Management*

*The purpose of this task is to oversee the complex operations of a contracts and make sure all of the interconnected parts work together. Responsibilities include laying out a strategy, setting objectives, overseeing projects, managing people, and analyzing the data.*

***Knowledge Areas include, but are not limited to:***

1. *Knowledge of Program Management concept similar to that of program management program (PMP) certificate holder.*

***In support of this task and the activities listed above the Contractor shall:***

1. *Ensure the Government is satisfied with the products or services being performed/obtained under this contract.*
2. *Ensure all positions herein are occupied by qualified, experienced, reliable and professional personnel.*
3. *Delegate and hold him/herself as well as his/her workers to a high standard and act decisively.*
4. *Manage Risk.*
5. *Improve processes.*

***Program Management – Performance Requirements:***

1. *Ensure all deliverables are provided to Government as directed herein.*
2. *Meet with the FO Branch Manager monthly (minimum) to ensure contract requirements are met and to discuss items for improvement.*
3. *Resolve all personnel challenges, as necessary in a timely manner.*
4. *Possess an understanding of each tasking in order to ensure the tasks are carried out in accordance with the requirements herein, best practices, guidelines and policies.*

*Task 13 - FO ADDA and CTU/I Services - Forensic Lab Management*

*The purpose of this task is to be responsible for the day-to-day management for the central digital devices laboratory. Closely working with the Focused Operations Team Leads and the Branch Manager in the central laboratory to develop and enforce lab best practices. Digital forensic analysis will be performed, as needed.*

***Knowledge Areas include, but are not limited to:***

1. *Knowledge digital forensics (dead box, network-based, cloud, mobile etc.)*
2. *Knowledge of digital lab operation best practices.*

***In support of this task and the activities listed above the Contractor shall:***

1. *Manage resources and staffing, monitor performance, drive efficiency, motivate and manage professional development of staff as it relates to digital forensics and forensic lab processes.*
2. *Write and maintain laboratory policy documents and procedures for incorporation into the quality management system.*
3. *They will work to ensure forensic lab process and procedures are implemented and adhered to.*
4. *Undertake analysis of forensic and other FO case and analytical information and the reports.*
5. *Possess at least 5 years of experience performing digital forensic analysis*
6. *Perform digital forensic analysis, as needed.*
7. *Oversee development of staff to ensure all digital forensic analysts perform digital forensics in accordance with policy and best practices.*
8. *Work with the Government to ensure all lab equipment is maintained in working condition to include current licensing etc.*

***Forensic Lab Management – Performance Requirements:***

1. *Provide reporting as described herein and in accordance with digital forensics best practices as provided by the Government.*
2. *Monthly Lab Inventory of all Focused Operations assets stored and/or utilized in the lab. All assets must be reconciled.*
3. *Report all missing equipment/software immediately to Focused Operations Government leadership.*
4. *Possess and maintain a digital forensic certification (ex. CFCE, GCFE/A, CHFI)*
5. *Manage evidence Intake/Outtake and Evidence Storage.*
6. *Other tasks as necessary to maintain compliant lab processes.*
7. *Perform digital forensic analysis (as needed) in accordance with policy and best practices.*
8. *Create and maintain documentation and procedures for lab management.*

*Hours of work for all requirements except “Hunting” will be Monday through Friday, except Federal holidays. Contractor is expected to provide sufficient coverage during the core hours of 8:00 of 4:30, Washington D.C. time. Hunt and Malware Operations will be “on-call” on a 24x7 basis for emergency situations.*

*@ Required*

1. Provide any security requirements

*@User: i.e., information/physical Security, access to buildings/access to network/vetting/clearances.* *Insert TSA Requirements language as applicable. If there are no security requirements, answer “none”, or “not applicable”)*

*@LLM: Example Answer All Contractor personnel supporting Tasks 1 – 11 including the Program Manager must have a Top Secret Sensitive compartmented Information (TS/SCI) clearance. Contactor personnel supporting Task 7 must have a Secret clearance.*

*Contractor personnel will be required to obtain a Personal Identity Verification (PIV) badge upon successful adjudication of the background clearance. The PIV badge is a TSA requirement and required for logical and physical access to TSA facilities and network.*

*DD254 Requirements will be provided.*

*The Contractor may access classified material at the following TSA facilities:*

*TSA Headquarters*

*6595 Springfield Center Drive,*

*Springfield, VA*

*Freedom Center*

*13555 EDS Dr*

*Herndon VA*

***Insert TSA-RQMTS; CONTRACTOR PERSONNEL ACCESS TO TSA FACILITIES, INFORMATION AND/OR SYSTEMS (SEP 2020)***

*@ Required*

1. What are the vendor personnel training requirements?

*@User: Explanation –* *use this section to address any training requirements of the vendor during on boarding and performance. Examples include any OLC training for the use of Government computers, security, etc. Do not include training that is already stated elsewhere, i.e. through 52.224-3 Alt-1 or in ITAR language. Insert TSA Requirements language as applicable. If there are no Vendor personnel training requirements, answer “none” or “not applicable”.*

*@LLM: Example Answer.-*

*Insert* ***TSA-RQMTS; CONTRACTOR EMPLOYEE TRAINING REQUIREMENTS (SEP 2020)***

*@Required*

1. Is there any required travel?

*@User: Explanation* *If travel is a requirement for accomplishment of the services describe any limitations related to vendor travel, as well as any reimbursement process, as applicable. Cite the Federal Travel Regulation (FTR) as applicable.*

*@LLM: Example Answer In accordance with the Federal Travel Regulation (FTR) Chapter 300.3.1, the official station is defined as a mileage radius of 50 miles from TSA HQ in Springfield VA. On occasion, a contractor resource may be required to travel to a location more than 50 miles from the official station. In cases like this, the Government will reimburse the Contractor in accordance with the FTR. Reimbursement for travel will be authorized in accordance with the FTR. All travel must be approved in advance by the Contracting Officer.*

*IAD has multiple contracts supporting the office. In the instance where contractors from various contracts need to travel together, every effort will be made on behalf of the Contractor to maximize cost efficiencies.*

*@ Required*

1. What is the base period of performance?

*@User: Explanation* *This is the initial period of performance that is funded. If the action is to be incrementally funded due to a Continuing Resolution, include the full period that would be funded otherwise. Transition In needs to be included in the calculation.*

*@LLM: Example Answer The base period of performance is one year (12 months) from contract award.*

*@ Required*

1. Are there anticipated option periods?

*@User:* *Explanation provide the number of option periods and length for each. If there are no option periods anticipated, answer “none” or “not applicable”.*

*@LLM: Example Answer – 4 one year options*

*@Required*

1. What are the deliverables and schedule?

*@User: Service type deliverables (reports) should be clearly defined with submittal dates, format requirements and periodicity. Specify electronic or physical delivery of reports and recipients. Electronic delivery must address limitations on size as well as recipient addresses. Supplies/Hardware should include quantity delivered, time and place.*

*@LLM: Example Answer Key deliverables and timelines are represented in the chart below. This chart is the anticipated schedule developed by the Government. However, the Contractor can propose an alternative schedule to be approved by the Government as part of the Initial FO Program/Project Implementation and Management Plan. The Contractor shall provide a report of progress through the end of the previous month at the beginning of each month. The report will detail each task to include:*

1. *Project schedule from initiation through completion with work started and completed*
2. *Issues that possibly put the schedule at risk*
3. *Items of interest by the Contractor and items known to be of interest to the Government.*

| ***DELIVERABLE*** | ***DUE DATE*** | ***FORMAT*** |
| --- | --- | --- |
| *Project Kick Off Meeting* | *Award +20 days* | *Electronic copy to COR, FO BM and IAD Senior Leadership team (SLT).* |
| *Initial FO Program/Project Implementation and Management Plan for all tasks* | *Strategy approval + 10 Days* | *Electronic copy to COR, BM and IAD SLT.* |
| *Quality Control Plan* | *Quarterly* | *Electronic copy to COR and FO BM.* |
| *Program Management Reviews (PMRs) – Includes: Monthly FO Program Status Report and Brief (Staffing Plan, Forensic Lab Readiness/Management, Deliverables, Program Projects Status etc.)* | *Monthly* | *Electronic copy, Brief to COR, FO BM and IAD SLT.* |
| *FO Project Development Kickoff and Release Plan and Project Development Review (Maximum of 6 per year)* | *Per project* | *Electronic copy to FO COR and BM.* |
| *FO Networks Engineering and Development Project,* ***FISMA Compliance****, Network Health and Wellness Reports* | *Weekly, Monthly, Quarterly, Yearly* | *Electronic copy to FO COR and BM.* |
| *SOC/FO Significant Case Briefs (1 per day)* | *Daily (business days), Ad Hoc* | *Electronic copy to IAD Deputy (Chief Information Security Officer) CISO.* |
| *FO cyber trend analysis and security incident metrics (Data Science, Insider Threat, Forensics and Cyber Intelligence)* | *Weekly, Monthly, Quarterly, Yearly* | ***Unclassified:*** *Electronic copy to participants, FO COR and BM and IAD SLT and* ***Classified:*** *Electronic copy to participants and IAD SLT.* |
| *FO/SOC Cyber Threat Briefs (All Tasks)* | *Bi-Weekly, Ad-Hoc* | ***Unclassified:*** *Electronic copy to participants, FO COR and BM and IAD SLT and* ***Classified:*** *Electronic copy to participants and IAD SLT.* |
| *Insider Threat, Forensics, Tactical Operations, eDiscovery, Threat Emulation/ Detection and Identification Pre Assessment Rules of Engagement (ROE), Operations Plans (as applicable) and Post Assessment Final Reporting (Maximum of 6 off-site per year with a maximum of 25 total to include remote\*)* | *To be completed NLT 10 days prior to assessment.* | *Electronic copy to FO COR and BM and IAD SLT* |
| *Insider Threat, Forensics, Tactical Operations, eDiscovery, Threat Emulation (TE)/ Detection and Identification Pre Assessment Operations Plans (as applicable) and Post Assessment Final Reporting (6 to 12 TE and Hunt operations off-site per year with a maximum of 25 total to include remote\*)* | *To be completed NLT 10 days prior to assessment.* | *Electronic copy FO COR and BM, applicable SO and IAD SLT.* |
| *Tactical Operations Communications Concept of Operations* | *30 days from established Course of Action (COA) of approved Concept of Operation.* | *Electronic copy to FO COR and BM and IAD SLT.* |
| *Insider Threat, Cyber Threat Intelligence (CTIR), Forensics, Tactical Operations Cases Executive Summaries and Full Reports* | *Daily (CTI), Per case, Per Operation* | *Electronic copy to FO COR and BM and IAD SLT.* |
| *Standard Operating Procedures (SOPs), Pre-Discovery Plans, Rules of Engagement ROEs, Operations Plans, CONOPs and other required documentation (ex. DHS CSP documentation) (Anticipate 25 per year each with a maximum of 30)* | *Per Case, Per Operation, Ad Hoc* | *Electronic copy to FO COR and BM.* |

*\*Assessments of remotely accessible systems.*

*@Required*

1. Are there any packaging/marking/shipping instructions for the

deliverables? Provide the instructions.

*@User:* *Provide Shipping address, email addresses, etc. Insert TSA Requirements language as applicable. If there are no packaging/marking/shipping instructions, answer “none” or “not applicable”.*

*@LLM: Example Answer Insert* ***TSA-RQMTS; PACKAGING AND MARKING REQUIREMENTS FOR TRANSPORTATION SECURITY SCREENING EQUIPMENT UNDER PRODUCTION AND/OR EXISTING MAINTENANCE SERVICES (SEP 2020)***

***Insert TSA-RQMTS; REQUIRED CONTRACTOR PROPERTY DELIVERY REPORTING (SEP 2020)***

*@ Required*

1. Where is the work to be performed?

*@User:* *List all locations. Identify if work is to be performed remotely.*

*@LLM: Example Answer The Contractor staff shall work at TSA Headquarters offices located in Springfield, Virginia at 6595 Springfield Center Drive, Springfield, VA. Site visits to TSA field offices and airports may also be required. There will be 5 – 25 contractors working from TSA HQ daily depending upon the needs of the organization. Telework (requires approval) will be considered for special circumstances*

*@ Required*

1. Is there a specific number of hours, level of effort or manhours stipulated by the Government? What are they?

*@User: Explanation* *Providing the estimated number of hours/LOE/FTEs provides clarity into the general scope of the effort. If they are not known, or do not apply, answer “No” or “not applicable”.*

*@LLM: Example Answer*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ***Labor Categories*** | ***Category*** | ***Yearly Hours*** | ***Monthly Hours*** | ***FTE*** |
| *IT Program Manager (Offsite)* | *Program Manager II* | *1040* | *86.67* | *0.5* |
| *Developer/Software Engineer (Offsite)* | *IT Specialist III* | *4160* | *346.67* | *2* |
| *Database Administrator (DBA) (SQL Server)(Offsite)* | *Technical Architect III* | *8320* | *693.33* | *4* |
| *Senior Developer/Software Engineer (Offsite)* | *Technical Architect IV* | *10400* | *866.67* | *5* |
| *Developer/Software Engineer (Offsite) - ATO/Migration Support* | *IT Specialist III* | *3120* | *260.00* | *1.5* |
| *Senior Architect/Solution Architect (Offsite)* | *Technical Architect IV* | *3040* | *253.33* | *1.46* |
| *Training Specialist* | *Analyst I* | *3080* | *236.67* | *1.98* |
| *Technical Writer* | *Analyst I* | *5160* | *410.00* | *2.48* |
| *Project Manager (Offsite)* | *Program Manager I* | *8320* | *541.00* | *4* |
| *Senior Developer/Software Engineer (Offsite) - PPBE Requirement Analyst)* | *Technical Architect IV* | *4160* | *346.67* | *2* |
| *Senior Developer/Software Engineer (Offsite) - OCM Analyst* | *Technical Architect IV* | *2080* | *173* | *1* |
| ***Total Direct Labor Costs*** |  | ***52,880*** |  | ***27.54*** |

*@Optional*

1. Are there specific Labor Categories (LCATs) required by the Government

to perform the effort?

*@User: Explanation –**if the Government has stipulated specific labor categories for the services to be provided, the categories need to be listed. This information may also be listed under Key Personnel qualifications and requirements. . If they are not known, or do not apply, answer “No” or “not applicable*

1. *@LLM: Example Answer Task Order Program Manager*
2. *Senior Engineer*
3. *Senior Hunt Operator*
4. *Senior Digital Forensics Examiner*
5. *Malware Analyst/Developer*
6. *Cyber Threat Intelligence Analyst*

*@Optional*

1. Is there any Key Personnel that must be identified in the resulting contract? What are the qualifications and requirements for all personnel?

*@User: Explanation* *Identifying the Key Personnel provides clarity into the critical aspects of the requirement., Provide those labor categories that are to be identified as Key, as well as any applicable skill level, such as journeyman, entry level. . If they are not known, or do not apply, answer “No” or “not applicable..*

*@LLM: Example Answer Key Personnel*

*The following roles are designated as Key Personnel under this task order:*

1. *Task Order Program Manager*
2. *Senior Engineer*
3. *Senior Hunt Operator*
4. *Senior Digital Forensics Examiner*
5. *Malware Analyst/Developer*
6. *Cyber Threat Intelligence Analyst*

*The above Key Personnel are listed as such due to the critical role they play in the discovery, analysis and mitigation of sophisticated cyber threats.*

*The minimum qualification requirements are described below.*

*Task Order Program Manager*

*The Contractor shall provide a designated Program Manager for this task order with the following qualifications:*

1. *A minimum of* ***7*** *years of cybersecurity program management experience relevant to this task order including* ***3*** *years of direct support for the US Government*
2. *A Bachelor’s Degree in IT, computer science, business or engineering OR a minimum of 10 years of relevant experience*
3. *At least one of the following certifications:*
4. *Certified Information Systems Security Professional (CISSP)*
5. *Information Systems Security Engineering Professional (ISSEP)*
6. *Project Management certification from Project Management Institute (PMI) Project Management Professional (PMP)*
7. *Defense Acquisition Workforce Improvement Act (DAWIA) Program/Project Management (P/PM) certification Level III*
8. *Federal Acquisition Contracting (FAC) - P/PM certification Level II or III*

*Senior Engineer*

*The Contractor shall provide a designated lead Senior Engineer with the following qualifications:*

1. *A Bachelor’s Degree in IT, computer science, business or engineering OR a minimum of* ***7*** *years of work experience similar to Task 8 to include verifiable experience and/or training in information assurance, IT security, network engineering, FISMA and system engineering*
2. *Understanding of local area network/wide area network (LAN/WAN) protocols (Transmission Control Protocol/Internet Protocol [TCP/IP], Domain Name Server [DNS Dynamic Host Configuration Protocol (DHCP), VPN, remote access, etc.*
3. *Possess or be able to acquire the following certification within 6 months of entry on duty (EOD): CCNA, CCNP, MCSE*

*Senior Hunt Operator*

*The Contractor shall provide a designated lead Hunt Operator with the following qualifications:*

1. *A minimum of* ***5*** *years of incident response and hunt experience relevant to this task order including 3 years of direct support for the US Government*
2. *A Bachelor’s Degree in IT, computer science, business or engineering OR a minimum of* ***5*** *years of relevant experience*
3. *Possess the GIAC Certified Incident Handler (GCIH) or equivalent certification*

*Senior Digital Forensics Examiner*

*The Contractor shall provide a designated lead Digital Forensic Examiner with the following qualifications:*

1. *A minimum of* ***5*** *years of digital forensic experience relevant to this task order including 3 years of direct support for the US Government*
2. *A Bachelor’s Degree in IT, computer science, business or engineering OR a minimum of* ***5*** *years of relevant experience.*
3. *Possess the GIAC Certified Forensic Analyst (GCFA) or equivalent certification.*
4. *Previous Forensic Lab Management experience desired.*

*Malware Analyst/Developer*

*The Contractor shall provide a designated lead Malware Analysts/Developer with the following qualifications:*

1. *A minimum of* ***7*** *years of malware analysis, reverse engineering and malware development experience relevant to this task order including 3 years of direct support for the US Government*
2. *A Bachelor’s Degree in IT, computer science, business or engineering OR a minimum of* ***7*** *years of relevant experience*
3. *Possess the GIAC Reverse Engineering Malware (GREM) or equivalent certification*

*Cyber Threat Intelligence Analyst*

*The Contractor shall provide a designated lead Cyber Threat Intelligence Analyst with the following qualifications:*

1. *A minimum of* ***7*** *years of malware analysis, reverse engineering and malware development experience relevant to this task order including 5 years of direct support for the US Government*
2. *A Bachelor’s Degree in IT, computer science, business or intelligence analysis OR a minimum of* ***7*** *years of relevant experience*
3. *Possess the GIAC Cyber Threat Intelligence (GCTI) or equivalent certification*

*6.0 ALL PERSONNEL MINIMUM QUALIFICATIONS PER TASK*

*All Contractor personnel supporting this task order shall meet the following minimum qualifications for all Tasks:*

*All Contractor personnel supporting this task order must have at a minimum:*

1. *Familiarity with NIST and FISMA compliance requirements.*
2. *Understanding of TSA, DHS, and/or DOD IT systems, IT security policies, and IT operational groups and IC standards, guidelines and policies.*
3. *Excellent communication, comprehension, follow-through and documentation skills. This includes the ability to convey complex and technical information to different audiences, prepare and produce detailed reports and documents that follow TSA guidelines, and deliver presentations to all levels.*
4. *Advanced analysis skills to better comprehend, synthesize, and leverage complex scenarios.*
5. *Ability to operate on own initiative and as part of a team, accounting for own actions and decision making during examination processes including working closely with team members to fulfill end user and departmental needs.*

*6.1 Task 1: FO ADET and ENG/DEV Services - Data Science and Analysis*

*Contractor personnel supporting Task 1 shall have:*

1. *A minimum* ***5*** *years of experience building descriptive, predictive, and prescriptive models with data and at least* ***3*** *years of work experience similar to Task 1. This experience should include data engineering, statistics, machine learning, and predictive modeling in support of the development of applications and analytical workflows supporting data analysis, threat modeling, targeting, entity resolution, and big data analytics.*
2. *A minimum of a Bachelor’s degree in a quantitative or technical field such as Computer Science, Economics, Engineering, Mathematics, Finance, Statistics, Operations Research or similar. MS degree is highly desirable.*
3. *A Security+ certification or have the ability to obtain this certification within the 120 days of employment.*
4. *Expertise with languages and frameworks such as Spark, Scala, Java, R, Python, JIRA, ELK and SQL.*
5. *Basic understanding and/or experience working in a Linux computing environment.*
6. *A combination of analytical skills, technical prowess and business acumen needed to effectively analyze massive data sets while thinking critically and shifting assumptions on the go, ultimately transforming raw intelligence into concise and actionable insights.*

*6.2 Task 2: FO ADET and ENG/DEV Services - Network Intrusion Identification and Detection (Hunt) and FO Incident Response (IR)*

*Contractor personnel supporting Task 2 shall have:*

1. *A minimum of* ***5*** *years of work experience similar to Task 2 to include:*
   1. *Assessing APT threats, attack methodologies, forensics analysis techniques, malware analysis, attack surface comprehension, Advanced Detection and Identification Team Operations, Cyber Threat Emulation operations, Cyber Advanced Threat Emulation Team operations and research, identification, and verification of new APT TTPs.*
   2. *Developing content for FO and SOC systems.*
   3. *Conducting security testing and computer system diagnostics.*
2. *Knowledge and expertise in:*
3. *Hacking and intrusion techniques.*
4. *NetFlow and PCAP analysis.*
5. *Cyber Advanced Detection and Identification Team Operations, SOC support, and coordination with security teams to strengthen the overall security posture in addition to developing mitigations, including signature development and working with incident management teams to better design and implement signatures and response policies and procedures.*
6. *Familiarity with general investigative techniques (Law Enforcement and Digital Forensic).*
7. *A high level of understanding in relation to computer data storage, Windows operating system file directory structures, electronic directory file management, and applications software, including Microsoft Word and Excel.*

*6.3 Task 3: FO ADET and ENG/DEV Services - Cyber Tactical Operations and Execution*

*Contractor personnel supporting Task 3 shall have:*

1. *A minimum of* ***5*** *years of work experience similar to Task 3 and Task 2.*

*6.4 Task 4: FO ADET and ENG/DEV Services - Cyber Threat Emulation Operations and Execution*

*Contractor personnel supporting Task 4 shall have:*

1. *A minimum of* ***5*** *years of work experience similar to Task 4.*
2. *Knowledge and experience in Cyber Threat Emulation operations, Threat Emulation Team operations, SOC support, and coordination with security teams to strengthen the overall security posture in addition to developing mitigations, including signature development and working with incident management teams to better design and implement signatures and response policies and procedures.*

*6.5 Task 5: FO ADET and ENG/DEV Services - Malware Reverse Engineering, Development and Execution*

*Contractor personnel supporting Task 5 shall have:*

1. *At least* ***7*** *years of experience in a cyber investigative role and at least 5 years of experience in cyber security operations and/or cyber threat intelligence analysis relevant to Task 5. This includes experience in:*
2. *Setting up and maintaining a lab network to test exploitation techniques and software, and also provide an environment for training defenders on attack - scenarios.*
3. *Both open source and/or commercial pen-testing tools and hacking tools.*
4. *A relevant Bachelor’s degree such as IT, computer science, business or engineering or* ***10*** *years of experience*
5. *A threat emulation certification such as GPEN, OSCP, or equivalent within one month of employment.*
6. *Expertise in hacking and intrusion techniques and prior experience with security testing and computer system diagnostics. Mobile device hacking experience a plus.*
7. *Have familiarity with fuzzing to assess software for vulnerabilities.*

*6.6 Task 6: FO ADET and ENG/DEV Services - Software Development of Custom Data Analysis Tools*

*Contractor personnel supporting Task 6 shall have:*

1. *A minimum of* ***5*** *years of work experience similar to Task 6.*
2. *Familiarity and experience with development of Elastic (ELK) and JIRA/Confluence platforms.*
3. *Familiarity with Windows, UNIX, and Advanced Hat Linux environments.*
4. *Solid knowledge of a scripting language and able to read, modify, and write shell scripts.*
5. *A high level of understanding in relation to computer data storage, Windows operating system file directory structures, and electronic directory file management.*

*6.7 Task 7: FO ADET and ENG/DEV Services - Network Maintenance and Special Projects Engineering*

*Contractor personnel supporting Task 7 shall have:*

1. *A minimum of* ***7*** *years of work experience similar to Task 7 to include verifiable experience and/or training in information assurance, network engineering, FISMA and system engineering.*
2. *Familiarity with Windows, UNIX, and Advanced Hat Linux environments.*
3. *Solid knowledge of a scripting language and able to read, modify, and write shell scripts.*
4. *A high level of understanding in relation to computer data storage, Windows operating system file directory structures, electronic directory file management, and applications software, including Microsoft Word and Excel.*
5. *Understanding of local area network/wide area network (LAN/WAN) protocols (Transmission Control Protocol/Internet Protocol [TCP/IP], Domain Name Server [DNS], Dynamic Host Configuration Protocol [DHCP], VPN, remote access, etc.).*
6. *Possess or be able to acquire the following certification within 6 months of entry on duty (EOD): CCNA, CCNP, MCSE.*

*6.8 Task 8: FO ADDA and CTU/I Services - Litigation Support/Freedom of Information Act (FOIA)*

*Contractor personnel supporting Task 8 shall have:*

1. *A minimum of* ***3*** *years of work experience similar to Task 8 to include verifiable experience and/or training in information assurance, network engineering, forensics or eDiscovery.*
2. *A high level of understanding in relation to computer data storage, Windows operating system file directory structures, electronic directory file management, and applications software, including Microsoft Word and Excel.*
3. *Possess or be able to acquire the following certification within 6 months of entry on duty (EOD): ACEDS EDTech certification.*

*6.9 Task 9: FO ADDA and CTU/I Services - Digital Forensics*

*Contractor personnel supporting Task 9 shall have:*

1. *A minimum of* ***5*** *years of work experience similar to Task 9 to include verifiable experience and/or training in information assurance, network engineering, forensic or hunting.*
2. *Familiarity with Windows, UNIX, and Advanced Hat Linux environments.*
3. *Solid knowledge of a scripting language and able to read, modify, and write shell scripts.*
4. *A high level of understanding in relation to computer data storage, Windows operating system file directory structures, electronic directory file management, and applications software, including Microsoft Word and Excel.*
5. *Possess or be able to acquire the following certification within 6 months of entry on duty (EOD: GCFE, GCFA, CFCE, CCE, GNFA, CHFI.*

*6.10 Task 10: FO ADDA and CTU/I Services - Cyber Threat Intelligence*

*Contractor personnel supporting Task 10 shall have:*

1. *A minimum of* ***3*** *years of work experience similar to Task 10 to include verifiable experience and/or training in information assurance, network engineering and cyber intelligence.*
2. *Possess or be able to acquire the following certification within 6 months of entry on duty (EOD): GCTI, GOSI or equivalent.*

*6.11 Task 11: FO ADDA and CTU/I Services - Cyber Insider Threat*

*Contractor personnel supporting Task 11 shall have:*

1. *A minimum of* ***5*** *years of work experience similar to Task 11 to include verifiable experience and/or training in information assurance, network engineering, forensics, eDiscovery, hunting, or cyber intelligence.*
2. *Familiarity with Windows, UNIX, and Advanced Hat Linux environments.*
3. *Understanding of local area network/wide area network (LAN/WAN) protocols (Transmission Control Protocol/Internet Protocol [TCP/IP], Domain Name Server DNS], Dynamic Host Configuration Protocol [DHCP], VPN, remote access, etc.).*
4. *Possess or be able to acquire the following certification within 6 months of entry on duty (EOD: ITPM or DHS equivalent.*

*@Optional*

1. Is there any Government Furnished Equipment (GFE) or Information (GFI) to be provided?

*@User: Explanation* *Describe what is to be provided, when it is to be provided and by whom. If no GFE or GFI is to be provided, answer “none” or “not applicable”.*

*@LLM: Example Answer The Government shall provide computer automation equipment to connect to the TSA network in order to accomplish the tasks contained within this task order. Under no circumstances shall the Contractor-company or Contractor-personally owned equipment be connected to the TSA computing environment. Additionally, use of company email for official TSA business is prohibited.*

*The Contractor shall be provided access to the following Government resources:*

1. *The TSA network.*
2. *Laptop computers and peripheral accessories; New Contractor employees must come to the Government site for assigned Government furnished equipment (GFE) and they must physically connect their laptop to the TSA network for the first-time logon so that it can write their profile locally; and*
3. *Flash drives and smart phones, as required.*

*All equipment and data provided to the Contractor or collected by the Contractor for the purpose of work performance shall not be used outside of the Contract to which this task order applies. At the end of the task order, the Contractor and all subcontractors shall return all equipment and return data and destroy additional copies of said data files in accordance with the latest DHS 4300 policy.*

*@Required*

1. Describe any Transition in and Transition out requirements required for the effort.

*@User: Explanation* *Address the activities that will be required of the vendor while onboarding/transitioning from the previous contractor. At the end of the contract period, address what transition out activities are required. If transition is not included in the effort, answer “none” or “not applicable”.*

*@LLM: Example Answer Task 14 - FO ADET and ENG/DEV Services - Transition-In*

*(After Entrance on Duty (EOD) not-to-exceed 2 months)*

*The purpose of this task is to transition all tasks associated with the previous contract from the previous contracting company to the new company. The transition period duration is not-to-exceed 2 months. It will begin after completion of EOD.* ***During this period Task 1 through Task 8 and Task 12******will begin.*** *During this period the below minimum tasks and requirements must be successfully completed during the transition period.*

***In support of this task and the activities listed above the Contractor shall:***

1. *The contractor’s transition office shall be physically located at TSA HQ and other TSA sites within the National Capital Region (NCR).*
2. *Communicate progress weekly with the COR and FO Branch Manager. Email and verbal communication will suffice.*
3. *Appoint and identify to the Government a Transition Manager (within 2 days of contract award) with the authority to accept direction from the Government and accomplish all work necessary to successfully facilitate contract transition. This authority need not include the authority to bind the company contractually.*
4. *Prepare and submit its list of personnel positions requiring IT system access.*
5. *Submit all remaining security clearance paperwork (must be submitted to the COR within 30 days of award).*
6. *Begin the performance of all tasks herein to ensure a smooth transition.*
7. *Acquire all system and application documentation (ex. SOPs, ROEs, Ops Plans, Case Reports, passwords, URLs etc.)*
8. *Develop and submit TSA onsite schedule to ensure adequate task coverage at TSA HQ, Annapolis Junction and the Freedom Center (when applicable).*
9. *The Contractor shall assume custody of the Government property for use in the performance of the work described herein. Each contractor will receive and sign for each TSA GFE assigned to them.*
10. *Executed Receipt of Property documents will be delivered to the Government on a date or dates mutually agreeable to the contracting parties.*
11. *All COR transition-in requirements to bring all personnel on board.*
12. *Read and sign all required cybersecurity and other paperwork. (ex. Rules of Behavior)*
13. *Read and ensure familiarity and understanding of applicable cyber security documentation (ex. TSA 1400, DHS 4300 A and B, E.O. 13587 etc.)*
14. *Complete all initial Online Learning Center (OLC) training.*
15. *Other activities as needed to ensure a smooth transition.*

*Task 15 – FO ADDA and CTU/I Services – Transition-In*

*(TSA transfer of CND Services estimated May 2023 not-to-exceed 2months)*

*The purpose of this task is to transition all tasks associated with the previous contract from the previous contracting company to the new company. The transition period duration is not-to-exceed 2 months). It will begin upon award of the FY23 Computer Network Defense (CND) contract. During this period Task 9 through Task 11, Task 14 through Task 16 and Task 13 will begin. Upon completion of this transition period, the contractor will perform all tasks (Task 1 through Task 16) requirements herein. During this period the below minimum tasks and requirements must be successfully completed during this transition period.*

***In support of this task and the activities listed above the Contractor shall:***

1. *The contractor’s transition office shall be physically located at TSA HQ and other TSA sites within the National Capital Region (NCR).*
2. *Communicate progress weekly with the COR and FO Branch Manager. Email and verbal communication will suffice.*
3. *Appoint and identify to the Government a Transition Manager (within 2 days of contract award) with the authority to accept direction from the Government and accomplish all work necessary to successfully facilitate contract transition. This authority need not include the authority to bind the company contractually.*
4. *Prepare and submit its list of personnel positions requiring IT system access.*
5. *Submit all remaining security clearance paperwork (must be submitted to the COR within 30 days of award).*
6. *Begin the performance of all tasks herein to ensure a smooth transition.*
7. *Acquire all system and application documentation (ex. SOPs, ROEs, Ops Plans, Case Reports, passwords, URLs etc.) Develop and submit TSA onsite schedule to ensure adequate task coverage at TSA HQ, Annapolis Junction and the Freedom Center (when applicable).*
8. *The Contractor shall assume custody of the Government property for use in the performance of the work described herein. Each contractor will receive and sign for each TSA GFE assigned to them.*
9. *Executed Receipt of Property documents will be delivered to the Government on a date or dates mutually agreeable to the contracting parties.*
10. *All COR transition-in requirements to bring all personnel on board.*
11. *Read and sign all required cybersecurity and other paperwork. (ex-Rules of Behavior)*
12. *Read and ensure familiarity and understanding of applicable cyber security documentation (ex. TSA 1400, DHS 4300 A and B, E.O. 13587 etc.)*
13. *Complete all initial Online Learning Center (OLC) training.*
14. *Other activities as needed to ensure a smooth transition.*

*Task 16 - All FO Services - Transition-Out*

*(6 months prior to FO Services Pop End Date)*

*The purpose of this task is to transition all tasks associated with the previous contract from the previous contracting company to the new company. The transition period duration is 6 months (6 months prior to FO Services Pop End Date). During this period Task 1 through Task 16 will continue to be performed until the FO Services Pop End Date as the Government deems appropriate to ensure a smooth transition to the new contract holder. During this period the below minimum tasks and requirements must be successfully completed during this transition period. During this period Tasks*

***In support of this task and the activities listed above the Contractor shall:***

1. *The contractor’s transition office shall be physically located at TSA HQ and other TSA sites within the National Capital Region (NCR).*
2. *Communicate progress weekly with the COR and FO Branch Manager. Email and verbal communication will suffice.*
3. *Appoint and identify to the Government a Transition Manager (6 months prior to the beginning of the transition-out) with the authority to accept direction from the Government and accomplish all work necessary to successfully facilitate contract transition. This authority need not include the authority to bind the company contractually.*
4. *Prepare and submit its list of personnel positions requiring cessation of IT system access.*
5. *Ensure the incoming contractor has access to all system and application documentation (ex. SOPs, ROEs, Ops Plans, Case Reports, passwords, URLs etc.)*
6. *Ensure all tasks are completed and FO operations continue as normal during the transition.*
7. *Develop and submit TSA onsite schedule to ensure adequate task coverage at TSA HQ, Annapolis Junction and the Freedom Center (when applicable) during the transition.*
8. *The Contractor shall return all Government property used in the performance of work described herein. Each contractor will return all TSA GFE assigned to them to the COR or other assigned FO contact no later than the last day of the Pop End Date.*
9. *Executed Receipt of Property documents will be delivered to the Government on a date or dates mutually agreeable to the contracting parties.*
10. *All COR transition-out requirements to bring all personnel off of the contract.*
11. *Ensure all applicable personnel are “read out” of applicable programs. The COR will schedule this activity.*
12. *Close out all accounts.*
13. *Other activities as needed to ensure a smooth transition-out.*

*@ Required*

1. What are the Government Specifications, Standards and Executive

Orders, etc. that must be adhered to in accomplishing this effort.

*@User: Explanation –* *Provide a listing of required policies, standards, guidelines and statutory requirements that must be followed. As applicable, the ITAR language, as well as 508 Compliance terms will be inserted here also.*

*@LLM: Example Answer The Contractor shall be familiar with and adhere to Federal policies, program standards, and guidelines such as, but not limited to, those listed below or later versions as amended:*

| ***REFERENCE*** | ***DESCRIPTION / TITLE*** |
| --- | --- |
| ***FISMA*** | *Federal Information System Modernization Act (FISMA) (2014)* |
| ***FIPS 199*** | *Federal Information Processing Standards (FIPS) Publication 199 - Standards for Security Categorization of Federal Information and Information Systems* |
| ***FIPS 200*** | *Minimum Security Requirements for Federal Information and Information Systems* |
| ***NIST SP 800-30 Rev 1*** | *National Institute of Standards and Technology (NIST) Guide for Conducting Risk Assessments* |
| ***NIST SP 800-35*** | *Guide to Information Technology Security Services* |
| ***NIST SP 800-37 Rev 2*** | *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* |
| ***NIST SP 800-39*** | *Managing Information Security Risk: Organization, Mission, and Information System View* |
| ***NIST SP 800-44 Version 2*** | *Guidelines on Securing Public Web Servers* |
| ***NIST SP 800-53 Rev 4*** | *Security and Privacy Controls for Federal Information Systems and Organizations* |
| ***NIST SP 800-53A Rev 4*** | *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans* |
| ***NIST SP 800-61 Rev 2*** | *Computer Security Incident Handling Guide* |
| ***NIST SP 800-83 Rev 1*** | *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* |
| ***NIST SP 800-86*** | *Guide to Integrating Forensic Techniques into Incident Response* |
| ***NIST SP 800-101 Rev 1*** | *Guidelines on Mobile Device Forensics* |
| ***NIST SP 800-115*** | *Technical Guide to Information Security Testing and Assessment* |
| ***NIST SP 800-128*** | *Guide for Security-Focused Configuration Management of Information Systems* |
| ***NIST SP 800-137*** | *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* |
| ***NIST SP 800-150*** | *Guide to Cyber Threat Information Sharing* |
| ***NIST SP 800-153*** | *Guidelines for Securing Wireless Local Area Networks (WLANs)* |
| ***NIST SP 800-160 Vol 1*** | *Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems* |
| ***NIST SP 800-171******Rev 1*** | *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* |
| ***NIST SP 800-171A*** | *Assessing Security Requirements for Controlled Unclassified Information* |
| ***NIST SP 800-181*** | *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework* |
| ***P.L. 93-579*** | *Public Law 93-579 Privacy Act, December 1974 (Privacy Act)* |
| ***40 U.S.C. 11331*** | *Responsibilities for Federal Information Systems Standards* |
| ***OMB M-19-03*** | *Office of Management and Budget (OMB) Memorandum 19-03, Strengthening the Cybersecurity of Federal Agencies by enhancing the High Value Asset Program* |
| ***OMB A-130*** | *OMB Circular A-130, Managing Information as a Strategic Resource* |
| ***BOD 18-02*** | *Department of Homeland Security’s Binding Operational Directive 18-02, Securing High Value Assets* |

*@ Required*