REQUEST FOR INFORMATION (RFI) #: 47HAA023N0002

Security Engineering and Operations Support III
(CISO Support III)

in support of:

General Services Administration (GSA) Information Technology (IT)
Office of the Chief Information Security Officer (OCISO)

Issued by:
General Services Administration
Office of Internal Acquisition
1800 F Street, NW
Washington, D.C. 20405

March 6, 2023

Disclaimer

This Request for Information (RFI) is for planning purposes only and is not a Request for Quotes (RFQ), Request for Proposals (RFP), Invitation for Bids (IFB) or an obligation on the part of the Government to acquire any services. Responses to this RFI are not offers and can/will not be accepted by the Government to form a binding contract. The Government reserves the right to determine how it should proceed as a result of this notice. Furthermore, those who respond to this RFI should not anticipate feedback with regard to their submission. The Government will not pay any cost incurred in response to this RFI. All costs associated with responding to this RFI will be solely at the responding party's expense. The information provided in this RFI is subject to change and is not binding on the Government. Failure to respond will not in any way prevent a potential offeror from participation in any future solicitations.

You are requested to respond to this RFI via electronic mail to Contract Specialist Kenya McPherson, kenya.mcpherson@gsa.gov and Contracting Officer, Erica Pelham at erica.pelham@gsa.gov no later than **March 24, 2023 at 10:00 AM EST.**

INTRODUCTION

The GSA consists of two services, the Federal Acquisition Service (FAS) and the Public Building Service (PBS). FAS serves as the acquisition and procurement arm of the Federal Government, offering equipment, supplies, telecommunications, and integrated Information Technology (IT) solutions to Federal agencies. PBS is charged to provide superior workplaces for Federal customer agencies at good economies to the American taxpayer. The GSA has consolidated Service/Staff Office (S/SO) IT service organizations into a single, agency-wide entity, branded "GSA IT," headed by the Chief Information Officer (CIO). The GSA Office of the Chief Information Security Officer (OCISO) reflects this consolidation. This consolidated information security approach allows GSA to build on its strengths while minimizing weaknesses and gaps in security.

The OCISO is organized with an enterprise-wide approach to IT Operation Security with services delivered through five distinct security divisions.

a. The Security Engineering (SecEng) Division (ISE) provides and manages various security programs and services. ISE provides security architecture review and consulting and engineering support for systems and emerging IT and IT security initiatives. ISE manages GSA's FedRAMP sponsorship program to assist qualified CSP solutions to achieve FedRAMP agency approval. ISE runs a DevSecOps program to cultivate the change and shift security to the left and is establishing an AppSec program. ISE performs software security review as part of the CTO IT Standard software approval process. ISE manages Payment Card Industry Data Security Standard (PCI DSS) compliance. The division is also responsible for developing and maintaining agency technical guidelines and standards.

b. The Identity Credential, and Access Management (ICAM) Shared Services Division (ISI) supports consolidating and coordinating ICAM-related capabilities to focus on improving ICAM governance across GSA IT. The Division is also responsible for managing C-SCRM assurance for GSA IT and its systems, and also supports agency-wide C-SCRM activities. Additionally, the division leads Zero Trust Architecture strategy efforts, to include leading a Program Management Office overseeing a series of Zero Trust initiatives.

c. The SecOps Division (ISO) is responsible for providing security and protection of the

GSA assets including people, technology, and data. The SecOps team consists of Vulnerability Management, Security Operations Centers, Incident Response Provides real-time operational security through the Security Operations Center (SOC) and enterprise network security capabilities. This office manages network security defenses (e.g., intrusion detection system, intrusion prevention system, firewalls, and security incident and event management) and operational maintenance of the tools utilized by OCISO. The division also provides manual and automated assessment services including vulnerability and compliance management and automated penetration testing.

d. The Policy and Compliance Division (ISP) provides management and maintenance of the GSA security authorization, Plan of Action and Milestones (POA&M), Continuous Monitoring and ongoing authorization (OA) using a Governance, Risk and Compliance (GRC) tool. The division also manages Security Training programs. Further, the division develops and maintains GSA security policies and procedural guidelines as well as security audit coordination efforts.

e. The Information Systems Security Officer (ISSO) Support Division (IST) IST provides Information System Security Officer (ISSO), Information System Security Manager (ISSM), Security Assessor and Penetration Tester cybersecurity services to support all Staff Offices and all of GSA's information systems. The division facilitates integrating IT security in programs and compliance with required security and privacy requirements. Cybersecurity service delivery provided by IST assists the CISO and Authorizing Officials during the independent assessment process to grant an Authority to Operate (ATO). IST also serves stakeholders in an advisory and consultative capacity on a multitude of Federal cyber security initiatives that have government-wide impact.

The GSA develops, manages, and operates a variety of business line applications and General Support Systems (GSSs) as part of its mission and business functions. These business applications must comply with Federal laws and GSA regulations, policies, and guidelines.

PURPOSE

The purpose of this effort is to acquire Security Operations, Security Engineering, Policy and Compliance, Assessment and Authorization (A&A), and ISSO support to provide centralized IT security services for the GSA through the OCISO. The contractor shall provide IT security technology support and provide independent assessments and recommendations of the GSA IT infrastructures, policies, and procedures.

GSA must comply with the Federal Information Security Management Act (FISMA), Presidential Decision Directives (PDD) 62 and 67, Homeland Security Presidential Directive (HSPD) 7 and 12, and various Office of Management and Budget (OMB) Circulars and Executive Orders to ensure critical and sensitive information and infrastructure are adequately protected and continuity of operations are assured.

Additionally, Federal security requirements and guidelines are included in the following publications, which are linked below:

National Institute of Standards and Technology (NIST):

a. NIST 800-18 http://go.usa.gov/8CzR
b. NIST 800-34 http://go.usa.gov/8Cu3
c. NIST 800-37 http://go.usa.gov/8Cum
d. NIST 800-47 http://go.usa.gov/8CJB
e. NIST 800-53 http://go.usa.gov/8CJe

Federal Information Processing Standards (FIPS) Publication (PUB):

a. FIPS 199 http://go.usa.gov/8CSH
b. FIPS 200 http://go.usa.gov/8Ch4

GSA security requirements, guidelines, and future updates are also applicable to the requirements of this TO.

1. GSA Procedural Guide: CIO IT Security 06-30 “Managing Enterprise Risk: Security Assessment and Authorization” (CA, PL & RA)
2. GSA Procedural Guide: CIO IT Security 09-44 “Plan of Action and Milestones (POA&M)”
3. PCI DSS Requirements and Security Assessment Procedures Version 3.0
4. GSA Procedural Guide: CIO IT Security 11-51 “Conducting Penetration Test Exercise Guide”
5. GSA IT Security Policy (GSA Order P. 2100.1K)
6. GSA Procedural Guide: CIO IT Security 12-66 “Continuous Monitoring”
7. GSA Procedural Guide: CIO IT Security 14-68 “Lightweight Security Authorization Process”

As these and any other or additional Federal or GSA security requirements or guidelines are approved, canceled, implemented, or otherwise changed, the contractor shall comply with these policies, or provide the Government a plan to comply with the requirements and guidelines.

AGENCY MISSION

The OCISO manages the GSA IT Security Office which is responsible for the development and maintenance of the GSA IT Security Program. The OCISO provides services and expertise across the agency to implement and maintain the IT Security Program; as well as establishes and promulgates IT security policies, procedures, controls, and guidelines.

The OCISO also monitors efforts to mitigate vulnerabilities affecting the GSA Enterprise in a timely manner, manages the annual FISMA assessment process, and conducts continuous monitoring of GSA systems and the Agency Incident Response Program. In addition, OCISO provides and monitors required enterprise IT security awareness and role-based training for GSA.

SCOPE

The contractor shall provide support to the GSA OCISO security program to manage the security compliance program of GSA applications and support systems. This contract is intended to be the primary resource for OCISO IT security, A&A activities, and FISMA and OMB reporting requirements. This includes acting as a liaison, providing stakeholder communication, providing advice, and making recommendations to the various application and support system program management teams. These services are required to ensure that GSA remains compliant with current and future Federal IT security requirements.

Work performance will occur at 1800 F Street NW, Washington, D.C. 20405, and the GSA Federal Building, located at 819 Taylor Street, Fort Worth, TX 76102. Travel to other GSA locations will most likely occur on an infrequent basis.

CURRENT IT/NETWORK ENVIRONMENT

The ISSO Support Division was established within the OCISO. ISSOs possess the primary responsibility for ensuring compliance with required security requirements for GSA IT systems under ISSO jurisdiction. The ISSOs provide support to ISSMs and currently have responsibility for 120 FISMA IT systems, governed by a variety of management controls including Investment

Review Boards (IRB) and Change Control Boards (CCB). These systems are diverse and include Government-owned and operated systems, contractor-owned and operated systems, Government-owned and contractor-operated systems, and contractor-owned and Government-operated systems, and have often been tailored to meet the Government's requirements.

GSA's current environment includes approximately 9,000 servers, network devices, firewalls, appliances, and printers; 7,000 Voice over Internet Protocol (VoIP) VOIP devices; 18,000 laptops; and 13,000 tablets, phones, and other end user devices. The total number of devices requiring authenticated scans is expected to slowly increase over time, but it is not expected to exceed 50,000 devices. Additionally, there are approximately 60,000 phone numbers which require scanning.

There are approximately 90,000 Internet Protocol (IP) addresses which need analysis spread across three/16 Classless Inter-Domain Routing (CIDR) networks plus some smaller networks on a continuous basis using GSA Network Access Control (NAC) tools. These networks and devices are spread between 16 Services, Staff Offices, and Regions (S/SO/R) in nearly 2,000 buildings and locations.

PROVIDE PROGRAM MANAGEMENT

The contractor shall provide program management support under this TO. This includes the management and oversight of all activities performed by contractor personnel, including subcontractors, to satisfy the requirements identified in this Statement of Work (SOW). The contractor shall identify a Program Manager (PM) by name who shall provide management, direction, administration, quality control, cost management, and leadership of the execution of this TO.

COORDINATE A PROJECT KICK-OFF MEETING

The contractor shall schedule and coordinate a Project Kick-Off Meeting at a location approved by the Government. The meeting will provide an introduction between contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. At a minimum, the attendees shall include contractor Key Personnel, representatives from the directorates, other relevant Government personnel, and the FEDSIM COR. The contractor shall provide the following at the Kick-Off Meeting:

At least three days prior to the Kick-Off Meeting, the contractor shall provide a Kick-Off Meeting Agenda for review and approval by the FEDSIM COR and the OCISO Technical Point of Contact (TPOC) prior to finalizing. The agenda shall include, at a minimum, the following topics/deliverables:

a. Points of contact (POCs) for all parties
b. Draft Project Management Plan (PMP) and discussion including schedule, tasks, etc.
c. Personnel discussion (i.e., roles and responsibilities and lines of communication between contractor and Government)
d. Staffing Plan and status
e. Transition discussion
f. Security discussion and requirements (i.e., building access, badges, Common Access Cards (CACs))
g. Invoicing requirements
h. Quality Assurance

The Government will provide the contractor with the number of Government participants for the Kick-Off Meeting and the contractor shall provide sufficient copies of the presentation for all present.

The contractor shall draft and provide a Kick-Off Meeting Minutes Report documenting the Kick-Off Meeting discussion and capturing any action items.

PREPARE A MONTHLY STATUS REPORT (MSR)

The contractor shall develop and provide a Monthly Status Report (MSR) (Section 9 - List of Attachments, Attachment D) using Microsoft (MS) Office Suite applications, by the tenth of each month via electronic mail (email) to the OCISO TPOC and the FEDSIM COR. The MSR shall include the following:

i. Activities during reporting period, by task (include: on-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
j. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
k. Key Performance Indicator (KPIs) & OCISO operational security metrics tracking
l. Personnel gains, losses, and status (i.e., security clearance).
m. Government actions required.
n. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
o. Summary of trips taken, conferences attended, etc. (attach trip reports to this MSR for the reporting period.
p. Accumulated invoiced cost for each CLIN up to the previous month.
q. Projected cost of each CLIN for the current month.

PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The contractor shall document all support requirements in a PMP. The contractor shall provide the Government with a draft PMP on which the Government will make comments. The final PMP shall incorporate the Government's comments.

The contractor shall document all support requirements in a PMP. The PMP shall:

r. Describe the proposed management approach.
s. Contain detailed Standard Operating Procedures (SOPs) for all tasks.
t. Include milestones, tasks, and subtasks required in this TO.
u. Provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between Government organizations.
v. Include the contractor's Quality Control Plan (QCP).
w. Include a draft Integrated Master Schedule (IMS) to be further developed in conjunction with the Government to manage milestones and deliverables for all tasks in the SOW. Update the IMS as the schedule changes and once a month at minimum. Be updated on a semiannual basis at minimum or when major changes occur.

PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted. The contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and point of contact (POC) at travel location. Trip reports shall also contain Government approval authority, total cost of the trip, a detailed description of the purpose of the trip, and any knowledge gained. At a minimum, trip reports shall be prepared with the information provided in.

PROVIDE AND EXECUTE TRANSITION-IN PLAN

The contractor shall update the draft Transition-In Plan provided with its quote and provide a final Transition-In Plan. The contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition. The contractor shall implement its Transition-In Plan No Later Than (NLT) 10 calendar days after award, and all transition activities shall be completed 30 calendar days after approval of final Transition-In Plan.

The contractor shall provide a draft Transition-In Plan at the Project Kick-Off Meeting. The Transition-In Plan shall articulate:

x. The contractor’s transition approach, process, and timelines.
y. The contractor’s approach to mitigating or minimizing disruption.
z. The contractor’s staffing status.
aa. Transition risk management and mitigation strategy.
bb. Initial coordination with the incumbent contractor.
cc. Gap analysis of required skills.
dd. Training approach/knowledge transfer approach.

The contractor shall execute its Government-approved Transition-In Plan. As part of this Transition-In Plan, the contractor shall ensure that there will be minimum service disruption to vital Government business and no service degradation during and after transition.

PROVIDE AND EXECUTE TRANSITION-OUT PLAN

The contractor shall provide Transition-Out support when required by the Government. The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming contractor/Government personnel at the expiration of the TO. The contractor shall provide a draft Transition-Out Plan within six months of Project Start (PS). The Government will work with the contractor to finalize the Transition-Out Plan At a minimum, The Transition-Out Plan shall be reviewed and updated on an annual basis. Additionally, the Transition-Out Plan shall be reviewed and updated quarterly during the final Option Period.

In the Transition-Out Plan, the contractor shall identify how it will coordinate with the incoming contractor and/or Government personnel to transfer knowledge regarding the following:

ee. Project management processes
ff. Points of contact (POCs)
gg. Location of technical and project management documentation
hh. Status of ongoing technical initiatives
ii. Appropriate contractor to contractor coordination to ensure a seamless transition
jj. Transition of Key Personnel
kk. Schedules and milestones
ll. Actions required of the Government

The contractor shall also establish and maintain effective communication with the incoming contractor/Government personnel for the period of the transition via weekly status meetings or as often as necessary to ensure a seamless Transition-Out.

The contractor shall implement its Transition-Out Plan NLT six months prior to expiration of the TO. The pla

SECOPS DIVISION SUPPORT

Security Operations is configured as Product as a Service model inclusive to 4 major area of focus inc
Add Paragraph detailing Teaming model. Number of FTE resources currently supporting generally across existing functions and any expectations we have for our new vendor.

- Vulnerability & Configuration Management FTE (8)
- Incident Response FTE (4)
  - Tier 2 - 2
  - Tier 3 - 2
- SOCaaS FTE (9) Growth to (12)
  - Tier 1 - 5
  - Tier 2 - 3
  - Tier 3 - 1
- Development FTE (8)
  - DSML (3)
  - Developer (5)
- Network Security FTE (13)

VULNERABILITY AND CONFIGURATION SCANNING SERVICES

The contractor shall perform an array of holistic and integrated scanning to support maintaining a secure perimeter around the GSA Point of Presence as well as to ensure applications are secure. Vulnerability discovery is the process of testing and probing the system entry points for flaws that can be used to generate an error condition, raise an invalid response, monitor traffic or data, or control a key system process. Vulnerability and configuration scanning services will allow assessors to determine whether vulnerabilities can be exploited or exposed to violate system boundaries or controls. These vulnerabilities may manifest themselves in several ways such as business process, business logic or design flaws, development errors, or configuration flaws.

Vulnerability Management must cover all elements of Enterprise to include multi-cloud and on-prem environments and devices that are not connected to a traditional on-prem network. Additionally, vulnerability scanning must be provided to application, server, database, mobile, and workstation environments.

QUARTERLY WIRELESS SCANNING

A. The contractor shall perform quarterly wireless scans for up to four Government buildings in the Washington, D.C. metro area. These tests are to determine unauthorized and unsecured wireless access points and ad-hoc networks in these buildings. Buildings are between two and 11 stories high. Government locations may change during the performance of this TO; however, the anticipated level of scanning activities is not anticipated to change.
B. The analysis must include the type of 802.11 protocol and security features utilized including authentication protocols. Identified GSA Access Points and Peer-to-Peer networks must be checked for compliance with the GSA standard. The reviews will be

conducted using GSA- approved standalone tools or enterprise wireless network monitoring tools.

C. The contractor shall provide information monitoring support for Impersonation and man-in-the middle attack that include evil-twin attack. The contractor shall support in the reporting of weak configuration or ciphers that can compromise GSA Enterprise Wireless Infrastructure. The contractor shall work with the system owner to validate GSA Enterprise Wireless devices that include Access Point, Printers, Internet of Things (IOT) devices.

D. Access points must be cataloged and addressed in a central data repository to be provided by the GSA, known hereafter as the GSA Project Folder. The contractor shall make contact with and provide counsel, as needed, to local system administrators of these networks to determine and/or ensure compliance.

E. The contractor shall conduct quarterly wireless and vulnerability reports shall be posted in the GSA Project Folder. There will be four reviews annually to be conducted in August, November, February, and May.

F. The contractor shall be an individual(s) with at least 2 years experience in wireless technology to include wireless technology security and provide recommendations to customers on best-practice and cyber hygiene.

WAR DIALING PENETRATION TESTING

A. Conducting a War Dialing test involves testing an GSA list of phone numbers for the presence of modems. The purpose of this test is to detect unauthorized devices, such as modems or faxes, on a GSA telephone network that might provide an insecure connection into a GSA network system. GSA has approximately 60,000 phone numbers across the country.

B. The contractor shall provide quarterly War Dialing Penetration Testing. The contractor shall use the approved Enterprise solution to conduct its war dialing penetration testing and provide quarterly reports to the ISO Director. Intrusions can occur through the use of dial-up connections to controlled systems. The contractor shall provide any inventory of authorized devices to compare results in the discovery of unauthorized devices on the network.

C. All vulnerabilities discovered shall be manually verified to determine compliance with GSA guidelines (Section 5, Deliverable 13). Vulnerabilities shall be sent to the proper GSA security manager for mitigation.

VULNERABILITY AND CONFIGURATION SCANNING (GENERAL OPERATING SYSTEM (OS)/NETWORK LEVEL)

The contractor shall analyze approximately 90,000 IP addresses spread across four/16 CIDR networks plus some smaller networks on a continuous basis using GSA tools. These networks and devices are spread between 115 FISMA boundaries located across GSA, Cloud, and non-connected mobile devices. The contractor shall survey to identify any servers that are not included in existing system FISMA inventories and ensure that they are included in subsequent vulnerability review and analysis. Contractor survey techniques shall distinguish between servers, workstations, printers, network equipment, building control systems, and other devices. The contractor shall monitor sources such as the American Registry for Internet Numbers (ARIN) to identify GSA-assigned networks. These network assignments shall be cataloged and monitored for changes and reported to the Director of SecOps. The contractor shall verify that networks are indeed assigned to GSA. The contractor shall survey these networks for servers and services weekly or more frequently, and shall conduct authenticated scans against all identified servers and services. The contractor shall conduct authenticated vulnerability scanning at least every three days on approximately 12,000 servers, network devices, firewalls, appliances, and printers; 7,000 VoIP devices; 22,000 laptops; and analysis of vulnerabilities on almost 13,000 tablets, phones, and other end user devices. The total number of devices requiring authenticated scans is expected to slowly increase over time, but it is not expected to exceed 50,000 devices.

A. The contractor shall provide the various S/SO/Rs support to answer and/or resolve questions about potential false positives, and determine if the vulnerability is applicable in each situation. The contractor shall provide instructions and assistance in mitigating the vulnerabilities discovered via email, phone, or schedule meeting as needed.
B. The contractor shall manage and maintain the GSA Vulnerability Management tools including server tuning and maintenance, backups, patching, OS maintenance, and troubleshooting. Maintenance should utilize automation where possible.
C. The contractor shall develop and provide training sessions, as needed, based on the scanning process to stakeholders. This training session shall be focused towards the end users of the scan tools (primarily ISSOs,ISSMs, and System Owners) and will be held up to four times annually. The training sessions will be recorded for later playback by internal GSA end users.
D. The contractor shall, upon Government request, evaluate new scan tools and develop automated scripts and processes. This includes researching technologies using the internet and other sources of public information, as well as meeting with potential providers of tools to further explore suitability to the Government's requirements.
E. The contractor shall use the scanning process document noted above for the notification and reporting process. Reports are managed through the GSA Vulnerability Management tool and may be automated.
F. The contractor shall review and determine which vulnerabilities are applicable to the GSA environment and only forward those for mitigation and inclusion in the A&A process. False positives and non- applicable vulnerabilities must be reduced to the greatest extent possible, marked as such within the GSA Vulnerability Manager, and documented as appropriate.
G. The contractor shall provide monthly metrics on scan trending data to include vulnerability discovery and remediation time across multiple FISMA systems
H. The contractor shall support GSA IT Metrics gathering across Critical/High
I. The contractor shall support GSA IT Metrics gathering across CISA Known Exploited Vulnerabilities.
J. The contractor shall support the management and implementation of CDM AWARE drive recommendations to resolve
K. The contractor shall support in review and verification of Acceptance of Risk (AOR) provided by the ISSO/ISSM and provide the Vulnerability Product Owner recommendation
L. The contractor shall provide biweekly Executive Summary reporting of cyber hygiene
M. The contractor shall provide support toward Cyber Hygiene and reduce Moderate, High, Critical vulnerabilities from public facing devices.
N. The contractor shall scan all assets within the GSA Policy CIO-IT Security-17-80 and provide assisting in update based on current operations.
O. The contractor shall provide executive summary to the SecOps Director based on KPI

VULNERABILITY SCANNING (WEB APPLICATIONS)

GSA serves a myriad of unique stakeholders across both the private and public sector through interactive web applications. To ensure these web-based applications are secure, the Government requires scanning to ensure all potential security vulnerabilities and architectural weaknesses are remediated.

A. The contractor shall perform approximately 70-80 authenticated scans per Quarter as requested Vulnerability Product Owner and be conducted by the vulnerability management team in addition to 1,500-2,000 unauthenticated web application scans per month
B. The contractor shall support a Cyber Hygiene web scan to support parameter Firewall support.
C. The contractor shall ensure that reports are provided to the appropriate system owners, ISSMs, and ISSOs within two business days of the scans being completed (this may be automated), and conduct a monthly call with developers and system administrators from each SSO to discuss questions or concerns they may have with the scan results or process.
D. The contractor shall utilize automation when possible to maintain statistics of scans, false positives, accepted risks, and known vulnerabilities and vulnerability age in a separate spreadsheet or tools.
E. The Government will provide inventories, necessary access and permission to scan the systems,and assist as needed in mitigation of vulnerabilities found during the analysis. However, the contractor shall be responsible for identifying the applicable POCs to accomplish this.
F. The contractor shall track and report the monthly and quarterly unauthenticated and authenticated scan completion
G. The contractor shall work with the system owners, DNS, ISSO, ISSM team to verify URL inventory managed by the Enterprise GRC solution.

VULNERABILITY DISCLOSURE / BUG BOUNTY PROGRAM

GSA has an Enterprise level Vulnerability Disclosure and Bug Bounty Program that Security Research has the ability to report to GSA for free disclosure or bounty paid. The GSA VDP program consists of around 800 public facing FQDN and has around 50 FQDN in private/public bug bounty programs.

A. The contractor shall provide support on GSA Enterprise Vulnerability Disclosure and Bug Bounty programs that consist of around 1000 public facing FQDN. The total number of public facing FQDNS could increase or decrease by 15%. The average number of reports is about 10 per week with a triage SLA within 3 days of report sent to GSA.
B. The contractor shall conduct analysis of the finding to determine if finding is new or already existing from our OS, Web, or Penetration finding and replicate the finding to determine true positives.
C. The contractor shall engage with the searcher and third party vendor to validate the finding.
D. The contractor shall engage with the System Owner /technical / ISSO /ISSM team in remediation and validation effort.
E. The contractor shall provide recommendations on severity rating for all Bug Bounty programs.
F. The contractor shall provide KPI for number of finding open, closed, and remediation timeline and keep remedial effort based on 06-30.
G. The contractor shall ensure newly created external web assets are included within the scope of the VDP to maintain 100% inclusion of scope.
H. The contractor shall provide a centralized location to view vulnerabilities data between all scanner that will provide a Enterprise Risk posture of GSA

VULNERABILITY SCANNING (MOBILE DEVICES)

The contractor shall analyze approximately 12,000 Mobile devices spread across iOS and Android devices.

A. The contractor shall support the vulnerability management and scanning requirements for mobile devices and conduct analysis of finding as required.
B. The contractor shall track vulnerabilities finding and remediation and report to the System Owner/ Technical / ISSO / ISSM team and provide recommendations on remediation effort.
C. The contractor shall support review of Acceptance of Risk for mobile devices and provide recommendations for action.
D. The contractor shall provide a centralized location to view vulnerabilities data between all scanner that will provide a Enterprise Risk posture of GSA

VULNERABILITY SCANNING (CONTAINERS)

A. Maintain and manage the container vulnerability solution that support on-prem and cloud containers
B. The contractor shall scan for vulnerabilities utilizing a set of solutions provided by the Government to support the vulnerability management of containers.
C. The contractor shall map image vulnerabilities to running containers and tag to FISMA for tracking and reporting
D. The contractor shall work with Security Engineering in managing the approved image and registries.

VULNERABILITY SCANNING (CLOUD ENVIRONMENT)

GSA has an Enterprise managed cloud environment multiple . SecOps responsibilities to provide scan for misconfigurations and benchmark is required to provide a safe Cloud Environment. There are over 120 Cloud environments with a 20% growth in the next five years.

A. The contractor shall work with Security Engineering on provide support with Benchmark development for Cloud environment
B. The contractor shall support in delivery of benchmark configuration to the System Owner, Technical teams, ISSO, and ISSM
C. The contractor shall support in identifying false positive and working with technical team to address issue
D. The contractor shall support adding acception modifications based on GSA Policies and procedures
E. The contractor shall coordinate with the system team to onboard the cloud environment as required. Estimated about 5 per year.
F. The contractor shall report

ENTERPRISE PHISHING PROGRAM

A. The contractor shall conduct around 32 phishing campaigns annually utilized GSA has an enterprise saaS service, FedRAMP authorized, to facilitate this work activity. a contractor will be required to manage and deliver service.
B. The contractor shall conduct phishing campaigns against about 18000 user all GSA users (18000 users) quarterly via the approved Phishing Campaign.
C. The contractor shall provide phishing for critical end user groups as defined by SecOps Director or CISO that average to about 10 unique groups with estimated (4000 users) quarterly.
D. The contractor shall phish 7 high value groups (4000 users) 4 times a year. Using 28 different phishing attacks.

E. Contractor shall record all results and provide metrics prior months, quarters, and years based on Click-rate, Organization, Office and campaigns. Provide repeat offender and recommendation of compare the previous years and months results
F. Contractor shall work with ISP Security Training to ensure the training content provide Phishing training to all GSA Enterprise

INCIDENT RESPONSE Services (IR)

GSA OCISO has an Enterprise level Incident Response team responsible for coordination and Forensics review for all Federal Information systems. The GSA IR has responsibility for reporting and coordinating incidents based on policies and processors listed in Section (Policies and Procedure guide section). The contractors shall provide a Tier approach to support incident tracking and management throughout the year in support of around 116 FISMA systems across Government Owned Contractor Operated (GoCo) and Contracted Owned Contractor Operated (CoCo).

Incident Response Tier 2 and Tier 3 Support

A. Coordinate and evaluate around 100-120 incidents per year that include reporting and coordination with DHS/CISA, OIG, Insider Threat, or other entities as required.
B. The contractor shall report all incidents to CISA within 1 hour of identification.
C. Coordinate and lead incident response functions to the GSA Enterprise.
D. Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.
E. Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.
F. Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.
G. Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation.
H. Perform cyber defense trend analysis and reporting.
I. Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.
J. Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).
K. Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
L. Track and document cyber defense incidents from initial detection through final resolution.
M. Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies.
N. Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness).
O. Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.
P. Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.
Q. Coordinate with intelligence analysts to correlate threat assessment data.
R. Write and publish after action reviews.
S. Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus, DHS/CISA report) to maintain currency of cyber defense

threat condition and determine which security issues may have an impact on the enterprise.

T. Provide off-hour support for major incident indicated by the Director of Security Operation of Chief Information Security Officer (1-3 per year)

Incident Response Forensics Support

A. The contractor shall support estimated 7-10 per year full digital forensics in support of a Cyber Incident
B. The contractor shall support Forensics analysis from a range of different type of incident that can include cloud, mobile, laptop, server, container images services task that may be required are listed below and can change depending on the requirement of the analysis
    a. Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion.
    b. Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis.
    c. Provide technical summary of findings in accordance with established reporting procedures.
    d. Examine recovered data for information of relevance to the issue at hand.
    e. Perform file signature analysis.
    f. Perform file system forensic analysis.
    g. Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.
C. The contractor shall develop forensics playbook and maintain playbook update quarterly
D. The contractor shall keep up with technology and support forensics analysis
E. The contractor shall coordinate and support with third party contract support
F. Provide off-hour support for major incident indicated by the Director of Security Operation of Chief Information Security Officer

SECURITY OPERATION CENTER (SOC)

THREAT HUNT SUPPORT

The contractor shall provide structure and unstructured threat hunt support across multiple of environment across on prem and cloud system

A. The contractor shall provide data analytics to terabyte worth of SIEM data utilizing data science and other techniques to provide analytics to threat.
B. The contractor shall evaluate normal data vs abnormal data and structure hunts
C. The contractor shall provide Observe, Orient, Decision, and Act (OODA) methodology to threat hunt activities
D. The contractor shall conduct research on latest exploitation to develop unstructured hunt
E. The contractor shall utilize security tool and CTI data in development and execution of hunt activities

SOC TIER 1 AND TIER 2 SUPPORT

The contractor shall provide 24x7x365 SOC Tier 1 and Tier 2 Services.

A. The contractor shall validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools
B. The contractor shall provide recommend computing environment vulnerability corrections
C. The contractor shall escalate alert incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment to

the Incident Response team

D. The contractor shall provide cyber defense trend analysis utilizing the GSA Security tools and reporting
E. The contractor shall receive and analyze security alerts from various sources within the enterprise and determine possible causes of such alerts.
F. The contractor shall provide Tier 2 support addressing real security incidents. Evaluates incidents identified by tier 1 analysts. Uses threat intelligence such as updated rules and indicators of compromise (IOCs) to pinpoint affected systems and the extent of the attack. Analyzes running processes and configs on affected systems. Carries out in-depth threat intelligence analysis to find the perpetrator, the type of attack, and the data or systems impacted. Creates and implements a strategy for containment and recovery while evaluating all data point to determine entry point and risk to a system

CYBER THREAT INTEL SUPPORT AND THREAT ASSESSMENT EVALUATION SUPPORT

A. The contractor shall maintain a common intelligence picture.
B. The contractor shall provide subject matter expertise to the development of cyber operations specific indicators.
C. The contractor shall assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.
D. The contractor shall assist in the identification of intelligence collection shortfalls.
E. The contractor shall brief threat and/or target current situations to IS staff on a monthly basis
F. The contractor shall collaborate with intelligence analysts/targeting organizations involved in related areas.
G. The contractor shall conduct in-depth research and analysis.
H. Conduct nodal analysis.
I. The contractor shall evaluate threat decision-making processes.
J. The contractor shall identify threat tactics, and methodologies and identify intelligence gaps and shortfalls.
K. The contractor shall monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.
L. The contractor shall monitor and report on validated threat activities.
M. The contractor shall monitor open source websites for hostile content directed towards organizational or partner interests.
N. The contractor shall monitor the operational environment and report on adversarial activities which fulfill leadership's priority information requirements.
O. The contractor shall produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).
P. Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.
Q. The contractor shall provide current intelligence support to critical internal/external stakeholders as appropriate.
R. The contractor shall provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.
S. The contractor shall provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations.
T. The contractor shall provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.
U. The contractor shall provide timely notice of imminent or hostile intentions or activities which

may impact organization objectives, resources, or capabilities.

V. The contractor shall report intelligence-derived significant network events and intrusions.

PURPLE TEAM SUPPORT

A. The Contractor shall then assess the environment’s response to various inputs and conditions using industry standard security testing tools.
B. The Contractor shall identify and exploit vulnerabilities discovered, with the end goal of breaking out of the environment. Prior to attempting to exploit any discovered vulnerability which may cause an interruption to the GSA’s business or impact the GSA’s systems, or cause the unauthorized disclosure of GSA’s Information, the Contractor shall provide detailed information to the Government on the risk and potential consequences of any such attempted exploitation
C. The Contractor’s project management approach for engagements of this type shall include a formal kickoff meeting.
D. The kickoff meeting introduces the members of the Contractor’s team participating in the project to their Government counterparts. The meeting will serve to validate points of contact (POC), establish a formal timeline, describe the events of each phase, discuss the rules of engagement, and coordinate any administrative requirements.
E. The contractor shall perform at least 1-2 quarterly purple team exercise that involve a FISMA boundary selected by the Director of Security Operations or Chief Information Security Officer (CISO)
F. The contractor shall provide deliverable reports that explain the exercises, activities, detections, and recommendations of the test.
G. The contractor shall maintain Purple team procedural and SOP guide and update at least annually to match industry standards.

MACHINE LEARNING MODEL OPERATIONALIZATION MANAGEMENT (MLOPS) SUPPORT

A. The contractor shall support Machine Learning Model Operationalization Management (MLOps) and work with the ML team in creating custom GSA models for detection and prevention of Cyber Attack across the Enterprise.
B. The contractor shall support and provide a model Governance encompasses a set of processes and frameworks that help GSA in the deployment of ML for Cyber Threats across on prem and cloud environment.
C. The contractor shall set up automatized and reproducible data and ML pipelines reduce the amount of time required to bring models into production.
D. The contractor shall provide to the government all models in a readable and usable format
E. The contractor shall maintain current ML Model and keep them optimize to reduce drift
F. The contractor shall provide recommendations to the SecOps directors of the model to complete quarterly based on industry best practices and threats.

DEVOPS / SYSTEM ENGINEERING SUPPORT

The DevOps and System Engineer Support has the responsibility to keep the technology and solutions up and optilized for the SOC, Incident Response and Vulnerability Management team across OCISO. The team is responsible for upkeep and maintenance of the solution, implementation of the new solution, migrating from existence to new solution through the contractor. The team responsible for optimizing and automating the solution in support of the OCISO mission.

TOOL ENGINEERING AND DEVELOPMENT

A. The contractor shall provide engineering and development support for new Security tools
B. The contractor shall support in the development of documentation to new solutions and support any ATO efforts for usage
C. The contractor shall provide implementation services for any new security solutions implemented by Security Operations

AUTOMATION AND OPTIMIZATION

A. The contractor shall provide automation and optimization of the Security tools
B. The contractor shall automate and streamline processes where possible
C. The contractor shall automate and optimize the detection and remediation of issues toward the security stack and report to the government within 30 min of detecting such issues.
D. The contractor shall follow internal and external change advisory board (CABs) Process

ENDPOINT SECURITY TOOL / SIEM MANAGEMENT

The contractor shall support the Enterprise Security stack

A. The contractor shall maintain the Enterprise SIEM solution and its component
B. The contractor shall provide engineering support in the collection and automation of log information to the Enterprise SIEM Solution
C. The contractor shall review log type and collection and determine action to be taken to collect logs associated with Government requirements (OMB-21-31)

The contractor shall perform and communicate to OCISO SecOps Director via email the following routine tasks as prescribed below:

Frequency	Ta sk
Multiple Times Daily	Interact with support staff to facilitate blocking/unblocking of files
Twice Daily	Monitor for legitimate applications that are being blocked. Manage software policies
Daily	Monitor the overall health of the tool; check that backups of the system are successful
Weekly	Status of system health, block activity and interaction with support staff
Monthly	Ensure patching of the system is up to date. Monthly summary status of system health, block activity and interaction with support staff
Every 30-60 Days	Test and deploy new versions of the client software to servers and laptops

NETWORK SECURITY

FIREWALL MANAGEMENT

A. The contractor shall manage, monitor, and maintain all Enterprise firewall, next generation web application firewall, IDS/IPS, cloud based Firewall instances, and proxy servers utilized by GSA OCISO and its customers. This includes, but is not limited to, upgrades, patches, system hardening, rulesets/configuration, troubleshooting with other teams, and regular health checks. There are currently nearly 30 virtual and physical devices as well as 3000 firewall context rules that shall be maintained by the contractor.
B. The contractor shall coordinate with the vulnerability management team when creating public facing inbound firewall rules that can include around 30 tickets per week.
C. The contractor shall complete change request processing (to include assessment and implementation) for perimeter firewalls within five business days, and internal firewall requests within three business days. The contractor shall work with the system administrators and ISSMs/ISSOs to obtain necessary access to the systems, and assist in mitigation of vulnerabilities found during the analysis.
D. The contractor shall maintain and all content firewall rules and clean up unused rules annually
E. The contractor shall maintain the Secure Web Gateway (SWGs) to prevent unsecured internet traffic from entering the GSA endpoint network.
F. The contractor shall maintain the Enterprise SASE solution and its content rules. The average number of tickets is 15 per week. All Tickets shall be resolved within 24 hours of report.

DNS MANAGEMENT

A. The contractor shall managed the enterprise DNS service that include over 4,000 DNS record include A, AAAA, MX, TXT, others
B. The contractor shall provide 99% up time for Internal / External DNS Services
C. The contractor shall provide DOH/DOT, DNS service for internal and external devices across the network
D. The contractor shall maintain the CISA protective DNS services that include routing all DNS traffic
E. The contractor shall provide maintain and upkeep of the DNS Environment that include on prem and cloud DNS devices
F. The contractor shall identify and provide recommendations to the Director of Security Operations process and technology improvements DNSaaS solutions for the GSA Enterprise

MICRO SEGMENTATION AND ASSET DISCOVERY MANAGEMENT

A. The contractor shall maintain the Enterprise micro segmentation solutions to protect the Building Management System. On average there are 30-50 rules that need to be maintained and coordinated with the Building Management Team, System Owner, and ISSM/ISSO.
B. The contractor shall support the Asset Discovery solution
C. Contractor shall support the device discovery over 800 facilities,data centers, and cloud assets
D. Contractor shall manage enumeration and detection policies for asset discovery and tagging.
E. The contractor will work with the CDM PMO to verify assets tags is reflected with the CDM program
F. The contractor shall support discovery of over 22k devices with a 95% accuracy. Contractor shall ensure the audit log are sent to Kibana and configured correctly
G. The contractor shall support the Building Security Network (BSN) microsegmentation rule that includes over 800 buildings and 2 data centers.
H. The contractor shall support microsegmentation across the GSA Enterprise and Cloud

environment.

I. The contract shall manage micro segmentation rules

J. The contract shall support integration with the Enterprise SIEM solution and CDM program.

SECURITY ENGINEERING

SecEng ensures multiple software components, hardware components, communication components, and processes and integration components across a project are designed and implemented to create a single functioning system that can deliver the business functionality proposed. IT security is embedded and threaded throughout the IT architecture for a project. A multi-disciplinary approach is required to ensure appropriate IT security is implemented and that IT systems function as single units.

The vendor is expected to provide qualified FTE resources to support existing functions and any expectations across various SecEng domains.

- Technical Benchmark and Hardening Guide (1)
- Software Testing (1)
- Security Architecture and Consulting (1, ad hoc in demand)
- FedRAMP (5, ad hoc in demand)
- PCI (1)
- DevSecOps (7, in demand)
    - Project support and core ODP support (5)
    - Hardening Services (1)
    - AppSec (1)

DEVELOP AND MAINTAIN GSA HARDENING GUIDES AND APPLICATION BENCHMARKS

At present, GSA has 32 technical and hardening guides. New guides shall be developed as the GSA application standards change. For existing guides, there will be approximately one update to the hardening guides annually, and technical guides shall be refreshed per GSA policy. The contractor shall ensure the guides are kept current. The current list of guides and benchmarks (provided for reference only) which need to be developed and maintained can be found in the below table.

Web Application Security
Web Server Log Review
Key Management
SSL/TLS Implementation
Windows Server 2012 R2 Hardening
Software Security Testing
Windows 10 Hardening
Web Browser Technologies Hardening
Microsoft SQL Server 2012 Hardening
RedHat Enterprise Linux 7 Hardening
Oracle Solaris 11 Hardening
Windows Server 2016 (Member Server) Hardening
Security Engineering Architecture Reviews
Application Programming Interface (API) Security
Robotic Process Automation (RPA) Security

Ubuntu Linux 18.x LTS Server Hardening
Windows Server 2016 (Domain Controller) Hardening
OCISO DevSecOps Program
MacOS 10.15 Hardening
Drones and Unmanned Aircraft Systems
Windows Server 2019 Hardening
RedHat Enterprise Linux 8 Hardening
Mulesoft Application Programming Interface (API) Security Process
Microsoft Office Pro Plus Hardening
Amazon Web Services (AWS) Elastic Kubernetes Service (EKS) Hardening
Container Security Hardening
Amazon Linux Hardening
macOS 11.0 Hardening
Microsoft SQL Server 2016 Hardening
Ubuntu Linux 20.x LTS Server Hardening
macOS12.0 Hardening
Microsoft SQL 2019 Hardening
macOS13.0 Hardening

A. The contractor shall develop and maintain GSA technical guides and hardening guides that comply with NIST guidelines and utilize the best practices from the CIS Benchmarks (Level I) and industry based on a defined refreshing schedule and on an as-needed basis.

B. The contractor shall develop, maintain, update, test, deploy GSA hardening benchmarks to identify performance standards for compliance with the approved GSA hardening guides.

C. The benchmarks shall include the supporting automation content including, but not limited to, templates, scripts, batch jobs, Inf files, GPOs, and/or Ansible, chef, and puppet content as applicable; SCAP content (security checklists); and, testing the associated GSA images.

D. All guide automation artifacts and compliance files shall be published to the security repository. Guides and supporting SCAP content shall be compliant with GSA tools. SCAP content shall align with GSA requirements (i.e., must be modified to account for GSA exceptions and/or policy requirements that are unique to the agency). SCAP content shall map to CCE, CCE CVE, CPE, Extensible Configuration Checklist Description Format (XCCDF), and Open Vulnerability and Assessment Language (OVAL) formats.

E. The contractor shall provide O&M support of the compliance content lifecycle management. For implementation, the contractor shall deploy new compliance audit content as required by GSA hardening guides, including new CIS benchmark content, the new STIG benchmark content that is published by DISA, the new compliance audit content as required by executive mandates (e.g., OMB Memorandum; DHS Cybersecurity Directives), and new custom audit content is created in-house on an ad-hoc basis to support the resolution of security events.

F. For Testing and Integration, the contractor shall review and modify of newly deployed audit content to ensure that every check/setting that is referenced in the GSA Security Benchmark is accounted for in the associated compliance checklist in the compliance tool, missing content is created in-house where possible, and applicable agency defined checks are modified to meet the agency requirements.

G. The contractor shall also analyze and remediate Compliance false positives as reported by GSA consumers and ensure faulty content is remediated in-house where possible, otherwise the contractor shall submit enhancement tickets to the platform vendor to update the content.

H. The contractor shall also monitor announcements for CIS content updates, STIG Update emails for DISA content updates that are applicable to GSA Compliance, and also checklists associated with deprecated/EOL technology or for which there are no longer any relevant GSA endpoints are archived.
I. The contractor shall review deviation itemization(s) as entered in GSA Security Benchmarks and cross-reference them with the associated Security Deviation Request Form submission for validation. Once validated, the contractor shall proceed to define scoring exceptions and verify scoring exceptions are correctly being applied
J. The contractor shall provide Reporting for Compliance, Web Reports and Inventory and other ad-hoc reporting requests .
K. The contractor shall provide assistance to GSA ISSMs/ISSOs, OCISO SecOps Division and other GSA IT organization in the application of benchmarks, including troubleshooting the implementation of required benchmarks for information systems and making appropriate changes to the GSA benchmarks, as needed and other general support and inquiries.
L. The contractor shall participation in bi-weekly sync meetings with Server Services and sync with Client Engineering to go over items related to technical benchmark and hardening guides

WORKSTATION AND SERVER SOFTWARE TESTING

GSA has a process to review any workstation and server software, client workstation software, Chrome extensions, Chrome Add-ons, chatbots, Trello Power Ups, and mobile applications for vulnerabilities and present recommendations for usage within GSA. The process triages all requests, of which there are about 50 each month typically and takes on average 30 minutes per request, or approximately 350 hours annually. Only a few are expected to go through in-depth testing each year of approximately 50 hours annually.

A. The contractor shall test and assess new or upgraded software including, but not limited to, server software, client workstation software, Chrome extensions, Chrome Add-ons, chatbots, Trello Power Ups, and mobile applications for vulnerabilities and present recommendations for usage within GSA.
B. The contractor shall perform automated and manual security testing and analysis on these proposed software.
C. The contractor shall develop, update, and maintain workstation software testing process documents including the SOP and the Software Security Testing (CIO IT Security 16-72) that describe the workstation and server software testing process, usage of tools, development of resultant testing reports with recommendations for usage within GSA, and the roles and responsibilities of the individuals involved in the testing. This document shall be updated whenever there are major changes in the process and/or based on the refreshing policy.
D. As with all major changes, the contractor shall be required to present this documentation, as well as documentation of the impact to the agency, applicable CCB, or approving authority.

SECURITY CONSULTING AND ENGINEERING SUPPORT

The SecEng Division provides three key security engineering and consulting services that the contractor shall be required to support:

SECURITY ARCHITECTURE DESIGN, REVIEW AND APPROVAL

GSA SecEng reviews and approves security architectures prior to the commencement of the system build (architecture, infrastructure, and code) and/or the start of A&A activities. The goal of the review is to ensure that any proposed security architecture or major changes to an existing architecture comply with GSA security requirements and are generally secure by design.

Security architecture specifically reviewed by SecEng will be performed after approval by ISSOs, ISSMs with their completion of SecEng defined architecture review checklist. For system teams adopting DevOps/DevSecOps working models and developing cloud applications with SecEng pre-approved deployment models/architectures, the review will be done in an agile way in collaboration with related technical teams to ensure systems are securely designed and implemented before they go into operation.

On an average, SecEng provides around 60 reviews per fiscal year, and each review takes approximately 10-20 hours to complete. However there typically is back and forth clarification required with the system team which will sometimes prolong the review process.

A. The contractor shall maintain the Security_Engineering_Architecture_Reviews (CIO_IT_Security_19-95) guide, follow the existing process and utilize a multidisciplinary approach to perform security architecture review and approval within the SLA defined by the SOP in order to ensure all architecture components including software, hardware, communications, process, and integration across a project are designed and implemented to create a single functioning system that can securely deliver the business functionality proposed.

B. The contractor shall develop, maintain and update the GSA security architecture design patterns and be able to provide secure architecture design for system teams upon request to resolve highly complicated and evolving IT security issues faced by GSA.

SECURITY ENGINEERING CONSULTING SUPPORT

SecEng provides technical expertise and advice on the restructuring and/or re- architecting of major systems (in particular hosted in Amazon Web Services (AWS) to ensure the best secure placement and configuration of network tools and appliances in order to provide the maximum protection of various types of sensitive Government data. The estimate of this type of security engineering and consulting support is approximately 2-4 engagements per fiscal year and each engagement will require 2 to 4 months of active security engineering engagement. These projects tend to have short lead times and varying knowledge requirements.

A. The contractor shall acquire the necessary skill sets and subject matter expertise to fulfill the Government's requirements within one month of stated need.

B. The contractor shall provide subject matter expertise in security engineering, system security integration, and security consulting support in the design, implementation, and modification of GSA information systems.

C. The contractor shall support highly technical IT projects dealing in cloud security (AWS in particular), virtualization security, web application security, network architecture and active directory design/segmentation, and secure coding, and source code reviews (i.e., Python, Ruby Node, YAML, Java, VB, APEX, Go and PHP).

D. The contractor may be required to attend GSA CCB meetings, and shall review and comment on design documents, perform testing as needed, and develop security engineering plans.

E. The contractor shall ensure all GSA requirements are addressed in the development of new applications and when there are major functional and or architectural changes.

F. The SecEng Subject Matter Expert (SME) shall be available to support activities under other tasks, particularly Tier 3 incident handling/forensics staff and DevSecOps and Security Automation, when necessary.

G. The contractor shall support the following types of application/network systems which are representative, but not inclusive, of the types of support required:
   a. Building Control Systems/Physical Access Controls
   b. Mobile Device and Applications
   c. Cloud-based information systems leveraging IaaS, PaaS, and Software as a Service (SaaS)
   d. Data Integration and Analysis Systems
   e. Enterprise Single Sign On/Multi-Factor Authentication Solutions
   f. API Gateways

THREAT MODELING AND SECURITY ARCHITECTURE DESIGN PATTERN SUPPORT

Threat modeling is a structured process to identify potential security threats and vulnerabilities based on the business use cases and security requirements. Threat modeling should ideally quantify risks based on the criticality and possibility of exploration of threats and vulnerabilities, and drive the prioritization of remediation and improvement of system architecture design.

SecEng estimates around 6-8 threat modeling for highly visible projects annually and the expected exercise lasts around 2-3 weeks for each engagement.

A. The threat modeling exercise shall include the interviews with the key stakeholders, review of the architecture (conceptual architecture, candidate architecture and existing architecture), perform Threat Modeling, conduct Architecture Risk Analysis and deliver the final report.
B. The contractor shall possess the knowledge and skills to perform threat modeling and security architecture risk analysis for applications, identify the flaws and gaps, review issues with system teams and stakeholders in order to help them understand the state of technology and security, provide recommendations and advisories in the area of secure architecture design and secure system development, and work together to prioritize and remediate identified flaws and gaps.
C. The contractor shall develop relevant documentation and capabilities for threat modeling, including but not limited to identifying a tooling for performing threat model, developing a procedural guide and SOP etc.
D. The contractor shall keep abreast with the knowledge and expertise of the latest security technologies and architectures especially in cloud, and develop and maintain an enterprise repository of approved and recommended security architecture patterns and assist in the standardization of enterprise security architecture.
E. The contractor shall produce security architecture patterns as reference architecture for major GSA cloud systems identified by OCISO.

FEDRAMP SPONSORSHIP SUPPORT

SecEng is responsible for FedRAMP GSA agency sponsorship program, and is currently supporting 19 vendors for achieving FedRAMP authorization, and 20 CSPs for Continuous Monitoring (ConMon) activities. The anticipation is that SecEng will support on average 5 new agency FedRAMP ATO sponsorships annually while maintaining the ConMon activities. For FedRAMP Moderate authorization,

The contractor shall provide support developing and formalizing the GSA IT OCISO FedRAMP sponsorship program. Key activities include developing program documentation, templates, processes, and systems to facilitate cloud service providers (CSPs) through the FedRAMP authorization process. The contractor shall also participate in cross functional teams with other OCISO organizations to develop, mature, and implement new processes supporting authorization options such as GSA LiSaaS, GSA MiSaaS, and GSA Protecting CUI in Non-Federal Systems guides which interconnect with supported FedRAMP systems.

The contractor shall follow the FedRAMP program procedural guide and provide the comprehensive support throughout the complete FedRAMP authorization process of a CSP offering. The contractor shall work directly with the government and CSP to ensure all FedRAMP sponsorship program requirements are met. Inform a CSP of the GSA FedRAMP authorization process and ensure CSPs receive and understand all program, technical, and documentation requirements.

- Facilitate and participate in recurring and ad-hoc CSP meetings to ensure schedules are on track, CSP questions are answered, and review incremental CSP progress to ensure deliverables meet GSA quality and technical expectations.
- Work alongside GSA FedRAMP Lead and provide security engineering services.
- Lead and conduct architecture interviews with CSPs to ensure all critical control areas throughout the architecture are designed to meet program requirements.
- Conduct architecture reviews of CSPs authorization packages to validate secure design, alignment to FedRAMP and GSA requirements, identify gaps, and advise FedRAMP Government Lead overall risk posture and compliance.
- Develop architecture briefing documents to inform the Government FedRAMP program manager, Director of Security Engineering, and GSA CISOthe CSP compliance with FedRAMP program requirements, technical capabilities, and any concerns noted from material review.
- Complete comprehensive review and comment documents of CSPs FedRAMP documentation including but not limited to system security plans, policies and procedures, supplemental GSA guidance documents, alternative implementation and risk acceptance documents, etc. Work with CSPs to reconcile and address any documentation and technology gaps discovered during the review.
- Complete comprehensive review of CSPs assessment and package submissions after 3PAO audits and prepare a package briefing for the Government FedRAMP program manager, Director of Security Engineering, and GSA CISO. Artifacts include but are not limited to vendor security assessment plans, security assessment reports, vulnerability scans, penetration tests, etc.
- Provide support for Continuous Monitoring activities including but not limited to items such as reviewing annual and monthly package submissions, reviewing and scoping significant change proposals, and reviewing risk acceptance, risk adjustment, and false positive justification documents.

The contractor shall provide the advisory and consulting services related to FedRAMP and Government wide policy as well as security review of new and emerging technologies. The contractor shall interpret FedRAMP and other GSA requirements and provide vendors with guidance regarding expectations, technical requirements, and process. The contractor shall stay informed of updated FedRAMP guidance, industry best practices, emerging technologies, and Government cybersecurity directives and provide recommendations to FedRAMP Government lead regarding impacts. The contractor shall conduct security reviews of technologies for use base consideration within CSPs authorization boundary.

The contractor shall provide project management support related to organizing, managing, and reporting on CSP deliverables and overall authorization status. The contractor shall develop a FedRAMP program level dashboard with a high level summary of each CSP status, schedule, milestones, and risks. The contractor shall create a detailed WBS per CSP to track detailed project schedules, activities, and deliverable status.

PCI PROGRAM SUPPORT

A PCI assessment is an audit for validating compliance with the Payment Card Industry Data Security Standard (PCI DSS) for merchants who accept, process, store or transmit credit card information. Based on the transaction volume, GSA is a merchant required to be PCI Level 4 compliant. The contractor shall provide PCI program support in order to bring GSA into PCI compliance.

The contractor shall work with the GSA PCI program manager, ISSMs and ISSOs and system teams to define the business profiles, baseline and keep up-to-date the GSA merchant IDs and chain IDs, and support the annual PCI assessment activities. Currently GSA PCI applications leverage two supporting FISMA subsystems for common controls. GSA is expecting the return of the Pegasys Merchant system which will increase the PCI scope. The contractor shall assist the program to identify the applications within the scope and facilitate the annual deliverables of the PCI Report on Compliance. The contractor shall also assist the GSA to complete the annual PCI compliance activities, including but not limited to self assessment, vulnerability scanning, completing SAQs, maintaining documentation repository of PCI artifacts, and attestation of compliance etc. The contractor shall ensure all PCI findings are entered in POA&M and tracked regularly. The contractor shall consult with PCI in-scope systems to remove processing and/or storage of cardholder data in order to be descoped from the PCI compliance requirements. The ultimate goal is to bring GSA into PCI compliance.

The contractor shall maintain and update the PCI DSS Program Implementation Plan and develop, maintain and update other related program documentation, including the annual PCI training course materials delivered via GSA OLU. The contractor shall provide other PCI program support including developing and maintaining supporting documentation such as SOP, PCI Procedural Guide, ROC template, Network topology template diagram, System inventory template etc.

DEVSECOPS

OCISO DevSecOps Program (ODP) is a program designed to integrate security into workflows and practices of DevOps in order to ensure security is considered and implemented in all design and operational phases. ODP is providing embedded DevSecOps engineers to supported system and platform teams and is operating hardened AMI and image pipelines and. ODP is implementing a cross team operational model to support the Ongoing Authorization and establishing an AppSec program to ensure the application security and software supply chain security is considered and vested during the software development life cycle.

OCISO DevSecOps Program(ODP) is leading the effort of implementing and improving the DevSecOps practice in GSA in order to assist GSA system teams to transition to DevOps/DevSecOps working model and meet the requirements of the Application and Workload tier of M-22-09. ODP aims to provide full security support in areas including secure design, application security, change management, operational security and security/compliance automation. The ultimate goal is to facilitate a cultural shift, reduce silos and communication barriers, provide security product-as-a-service through an integrated engagement model, help GSA IT systems deploy immutable workloads in cloud environments, integrate with GSA security stacks and improve overall security posture.

The scope of OCISO DevSecOps Program support includes teams that are composed of differing skill sets to include but not limited to DevSecOps, AppSec, Software Supply Chain security, Cloud/infrastructure/software engineers, trainers, and consultants as defined by the Government.

The contractor shall support an Agile environment where the scope of work can and will change at any time as needed, and use Scrum to ensure all activities and backlog are properly defined, sized and delivered. The contractor shall also support the program development of GSA DevSecOps Program. Below are the critical requirements

PROGRAM SUPPORT AND DEVELOPMENT

The contractor shall establish an overarching DevSecOps program plan and processes to engage, support and build DevSecOps based working model and support model between OCISO ISE team and various IS divisions, as well as system teams and business lines across GSA.

The contractor shall establish the GSA OCISO Application Security (AppSec) program, define program maturity models, processes, SOPs, KPIs; Develop policies, guidelines and best practices for application/software security and provide training to the GSA developer community.

The contractor shall Develop a Software Supply Chain Security framework that complies with NIST Secure Software Development Framework (SSDF) and in line with the industry best practice framework such as Supply chain Levels for Software Artifact (SLSA); Develop policies, guidelines and best practices for software supply chain security

The contractor shall research, identify, procure and implement enterprise tools and technical solutions for DevSecOps, AppSec and Software Supply Chain security.

DEVSECOPS AND APPSEC SUPPORT

The contractor shall establish cross functional working groups to define and develop security processes to engage and support DevSecOps team and practices DevSecOps across GSA. Contribute and advocate for security vision and requirements on various forums, leadership meetings etc as needed.

The contractor must provide qualified manpower within ten (10) business days of Government request or of a vacancy. All labor category mixes and key personnel positions will be determined at the order level. The contractor shall identify and provide dedicated resources composed of personnel with the skill sets (and any additional skills required according to the provided requirements) set forth in performance requirements defined by the specific order.

The contractor shall actively engage and contribute to application and platform teams' agile ceremony and activities. Advocate, prioritize and track security activities and priorities in PI plans, sprint cycle and schedules across multiple GSA teams engaged in DevSecOps practices with OCISE ISE.

The contractor shall directly support secure architecture design, application security, security impact analysis during changes management process and Operational Security of GSA application and platform in coordination with cross functional application/platform teams

The contractor shall identify, procure, implement and maintain enterprise Static Application Security Testing (SAST) solution, and offer it as SAST-as-a-Service and onboard system and platform teams.

The contractor shall assist in the automated Static Application Security Testing (SAST) and perform manual code reviews. Assist in the finding triage, vulnerability remediation and rescan of application code.

The contractor shall evaluate the existing DAST solution and identify areas for improvement and potentially upgrade the enterprise solution and offer it as DAST/IAST-as-a-Service and onboard system and platform teams.

The contractor shall assist in the automated Dynamic Application Security Testing (DAST) and/or Interactive Application Security Testing (IAST) and perform manual application level pen-testing and finding verification. Assist in the finding triage, vulnerability remediation and rescan of application.

The contractor shall assist system and platform teams to practice software supply chain security best practice based on the defined software supply chain security framework.

The contractor shall perform change review in relation with security impact in platform and application teams engaged with OCISO ISE team

The contractor shall utilize various security tools, SOC dashboard , logs monitoring solution to support various security and compliance function of integrated application/platform teams

The contractor shall support and maintain system integration with IS enterprize security tools

The contractor shall coordinate with ISSM/ISSO to support compliance functions, identify opportunities for automating manual compliance functions and processes, and enhance processes where a gap exists.

SECURITY AUTOMATION

The contractor shall develop standardization, framework and notional architecture for security automation, data correlation between various security tools, workflow and process automation including continuous assessment of NIST controls.

The contractor shall develop community of practice for development , maintenance and release of security automation process and code in GSA

The contractor shall develop automation, api integration, data correlation, data integration and reporting to support security and compliance automation

The contractor shall develop, maintain and support automation content for reusable security implementation such as installation and configuration of security tools and agents.

HARDENED IMAGES

The contractor shall develop and maintain hardened AMIs and ensure the compliance score aligns with the GSA hardening benchmark requirements and baked in with required GSA enterprise security tools and agents.

The contractor shall develop, maintain and certify docker container images and ensure container images meet the GSA benchmark compliance requirements

The contractor shall operate and maintain ODP Product-as-a-Service offerings for both Hardened AMIs service and Container Images service

The contractor shall develop and maintain the processes and SOPs for ODP Hardened AMIs as-a-Service and Container Images-as-a-Service and advocate for consumption of standard OS/Container images across GSA teams

RESEARCH AND DEVELOPMENT (R&D)

The contractor shall scope the market for latest security technologies and solutions and perform research write up, Proof of Concept, pilot and deliver MVP as needed to enhance the IS security stack. Also includes API Security and Mobile App Security.

SECURITY SUPPORT SERVICES

The Government has an established ISSO Support Division within the OCISO. Information System Security Officers (ISSOs) possess the primary responsibility for ensuring compliance with required security requirements for GSA IT systems under designated ISSO jurisdiction. The ISSOs provide direct support to Information System Security Managers (ISSMs) and currently have responsibility for more than 120 distinct information systems of varying size, complexity and user base belonging to system owners across GSA. This number may increase or decrease based on agency mission, needs and potential reorganization.

The contractor shall serve in an advisory capacity to OCISO focused on assessments, architecture and design, security solutions integration, and security transformation initiatives.

The contractor shall ensure security is embedded in all aspects of IT in a standardized manner and shall improve the overall cybersecurity risk posture of GSA IT.

The contractor shall respond to multiple laws, regulations, governing bodies, and policies and shall comply with an increasing number of interactions with federal agencies.

The contractor shall obtain a full risk view of GSA and shall improve risk-based decision capabilities of OCISO.

The contractor shall enhance Governance, Risk, and Compliance (GRC) activities within GSA IT with eGRC tooling improvements and automation.

SYSTEM DEVELOPMENT LIFE CYCLE SUPPORT (SDLC)

The contractor shall participate throughout the SDLC to ensure security is an integral part of GSA business processes. The contractor shall ensure that security activities are implemented throughout the SDLC from acquisition to end of life. The ISSO shall review software releases and documentation, as assigned, to determine effects to the security posture. The contractor shall identify whether scans are required for any major, minor, patch, or data refresh releases submitted based on the documentation provided and Government policy. The contractor shall manage the configuration management and engineering change control processes (as applicable) to create security feedback loops, which help to provide the most streamlined security reviews, and to institute corrective action strategies for application release vulnerabilities prior to implementation into the production environment. Activities shall be coordinated with appropriate OCISO Security divisions.

The contractor shall support new user request processes (i.e., verification of initial/full access); and review monthly user inactivity reports and reconcile against GSA identity systems (e.g., Active Directory), as appropriate, to ensure inactive accounts are removed or disabled.

INFORMATION SYSTEM SECURITY OFFICER (ISSO) SUPPORT

The contractor shall provide support for OCISO IST. This support consists of a set of responsibilities that are universal to all GSA IT systems requiring ISSO support.

For their assigned system(s), the contractor shall assist in coordination of services provided by the SecOps, SecEng, and Policy and Compliance Divisions to ensure systems are securely implemented and comply with FISMA, OMB, CISA and GSA policies.

The contractor shall provide support for traditional IT systems, as well as Building Monitoring and Control (BMC) systems including, but not limited to, building technologies such as Advanced Metering Systems (AMS), building automation systems, lighting control systems, Physical Access Control Systems (PACS), renewable energy systems, and kiosks. These systems, while closely related to the scope of facilities management, are IT systems, and as such are subject to the same Federal and agency-specific policies and security standards as any other Federal IT system. To support these systems, the contractor shall possess highly specialized knowledge of BMC systems, understand the threats they pose to the GSA enterprise network, and be able to provide guidance on securely implementing such systems.

The contractor shall work closely with the ISSMs, and IS Divisions and GSA business lines to develop a systematic, repeatable approach to securely implement such systems. The contractor shall facilitate Assessment and Authorization (A&A) on systems for which the contractor has responsibility. The ISSO shall collaborate with system owners and business lines to remediate identified vulnerabilities, and provide recommendations based on their expertise to manufacturers, vendors, and building managers as to how to resolve vulnerabilities or mitigate threats discovered during the assessment.

These coordination activities shall also include Systems Development Life Cycle (SDLC) support, participating in cross-discipline project teams, and working with system owners and business lines in matters concerning the assigned system(s). The contractor shall evaluate assigned information systems to ensure systems are securely hardened, patched, monitored, and evaluated via available assessment services and ascertain if additional safeguards are needed.

The contractor shall ensure all systems are operated, maintained, and disposed of in accordance with documented security policies and procedures. For assigned systems that may be contractor-owned and contractor-operated, the contractor, in coordination with ISSMs, shall ensure that such vendors comply with GSA security and privacy requirements.

The contractor shall provide comprehensive documentation, development, and operational support for GSA IT Security programs for major and minor applications and GSSs. The contractor ISSOs shall act as the primary resource for all IT security documentation development and revision. Documentation requirements include:

a. System Security and Privacy Plans (SSPPs)
b. Continuous Monitoring Plans
c. Configuration Management Plans
d. Contingency Plans
e. Contingency Plan Test Reports
f. POA&M Updates
g. User Recertification
h. FISMA Assessments
i. Assessments reflecting customer responsibilities for GSA cloud systems and assessments supporting the Limited ATO process for cloud systems
j. Incident Response Plans and Reports
k. Privacy Threshold Analysis (PTA) and Privacy Impact Assessment (PIA)
l. FIPS 199 Impact Analysis
m. Business Impact Analysis

These GSA FISMA ATO package documents and supporting attachments are to be ingested and maintained in GSA's governance risk and compliance security tool. GSA OCISO is open to evaluating an eGRC tool that will natively support future Federal OSCAL initiatives.

The contractor shall advise ISSM, system owners and OCISO staff in other Security divisions of risks to assigned systems. The contractor shall research assigned IT security systems to provide insights on IT security architectures and IT security recommendations for assigned systems. The contractor shall serve as the IT Security POC for assigned Service and Staff Office systems. The contractor's activities shall be coordinated with other OCISO Security divisions, as appropriate. The contractor shall provide recommendations which identify how to improve the IT security function to reduce costs, increase quality, and improve response times.

The contractor shall assist in the coordination of services provided by other OCISO Security divisions including SecOps, SecEng, ICAM Shared Services, and Policy and Compliance as well as SDLC support, and participate in cross-discipline project teams working with system owners and business lines in a team topologies construct.

The contractor shall attend internal Federal Government IT security meetings which may be weekly divisional meetings, ISSO/ISSM meetings, project meetings, change control, engineering review, or other meetings. The contractor shall review and coordinate reporting of Security Advisory Alerts (SAA), Binding Operational Directives (BODs), Emergency Directives (EDs), Executive Orders (EOs), compliance reviews, security training, incident reports, contingency plan testing, and other IT security program issues, and prepare and report on the IT security architecture, IT security processes, and IT security posture of supported IT security systems at GSA. The contractor shall manage identification and authentication schemes used in systems as well as new user requests.

The contractor shall prepare incident reports, assist or perform in incident mitigation, and forward incident reports, as appropriate, after consultation with the ISSM, in coordination with the OCISO SecOps Division for incident management and/or US-CERT reporting.

The contractor shall provide a detailed approach that addresses the functional delivery of the specified tasks listed in the sections below for ISSO support. The contractor shall:

a. Perform as the lead IT security POC for all activities related to IT security for assigned information systems, coordinating activities and services from other OCISO Security divisions (i.e, SecOps, SecEng, ICAM Shared Services, and Policy and Compliance) to ensure systems are securely implemented and operating as intended.
b. Provide oversight and responsibility for implementation of system security and privacy requirements.
c. Coordinate and facilitate across OCISO Security divisions to ensure available services are implemented for assigned systems; evaluate assigned information systems to ensure systems are securely hardened, patched, monitored, and evaluated via available assessment services; ascertain if additional safeguards are needed; and develop and maintain system security documentation.
d. Facilitate relationships for assigned systems that may be contractor-owned and contractor-operated, ensuring vendors comply with GSA security and privacy requirements.
e. Ensure systems are operated, used, maintained, and disposed of in accordance with documented security policies and procedures. Ensure GSA information systems comply with FISMA, OMB, CISA and GSA Policies.
f. Identify risks to assigned systems to ISSM, System Owners, and OCISO staff in other Security divisions.
g. Research assigned IT security systems to provide insights on IT security architectures and IT security recommendations for assigned systems; activities shall be coordinated with other OCISO Security divisions, as appropriate.
h. Assist in identifying how to improve the IT security function to reduce costs, increase quality, and improve response times.
i. Serve as the IT Security POC for assigned S/SO systems, coordinating IT security issues with other OCISO security divisions, as appropriate.
j. Review and coordinate reporting of Security Advisory Alerts, compliance reviews, security training, incident reports, contingency plan testing, and other IT security program issues.
k. Identify, report, and respond to security incidents following GSA Information Security policy and process requirements; security incident reporting and response activities are led by the OCISO ISO Division.

The IST Division is supported by a mix of Federal and Contractor ISSOs formally designated throughout IS and GSA. The Contractor staffing plan should have a primary ISSO and backup ISSO per FISMA system assigned.

The contractor shall develop an ISSO Guide and Orientation Manual for delivery to the government within the first 60 days of the contract award. This guide will serve as a part of an ISSO's onboarding process and ISSO role-based training.

The contractor shall ensure all ISSOs, Assessors and Pentesters are NIST NICE certified (e.g, CISSP, CEH, CASP, OSCP)

CLEAN ATO SUPPORT

GSA has a dynamic FISMA ecosystem with many paths to granting proper authorizations for information systems. The OCISO Clean ATO guide provides an overall understanding of the Authorization types at GSA and provides an overview for the paths to Authorization to Operate (ATO) for GSA information systems.

GSA OCISO has provided a path for new systems to take advantage of a more flexible framework that supports rapid delivery of new services with a phased Authorization that can meet GSA business needs and security requirements via the Lightweight ATO process.

The Clean ATO phases are as follows:

- ○ Phase 1: Pre-Assessment - Assessment Preparation Procedure
- ○ Phase 2: Assessment - Assessment Procedure
- ○ Phase 3: Post- Assessment - Security Package Review and Authorization Process

The contractor shall align to the OCISO Clean ATO process and support review checklists to obtain a Full 3-Year FISMA ATO or an appropriate ATO for new FISMA systems (e.g., LiSaaS, LATO, MiSaaS).

PENETRATION TESTING

A penetration test is an authorized simulation of a cyberattack which is used to identify security weaknesses by way of technical flaws, misconfigurations, vulnerabilities, and/or business logic, with or without knowing the inner workings of the system. NIST SP 800-115 describes two primary types of penetration testing: external and internal testing.

External security testing offers the ability to view the environment's security posture as it appears outside the security perimeter, usually as seen from the Internet, with the goal of revealing vulnerabilities that could be exploited by an external attacker.

In internal security testing, assessors work within the security perimeter, assuming the identity of a trusted insider or an attacker who has penetrated the perimeter defenses. This testing can reveal exploitable vulnerabilities and demonstrates the potential risk to the organization or agency. Internal security testing also focuses on system-level security and configurations including application and service configuration, authentication, access control, and system hardening.

The Contractor shall conduct External and Internal pentesting using the one or more of the 14 types of pentesting defined in the GSA CIO-IT Security-11-51, Revision 6 Conducting

Penetration Test Exercises security guide. These penetration tests must be aligned to Penetration Testing Execution Standard (PTES) and the Open Web Application Security Project (OWASP) industry standards.

The Contractor shall conduct penetration testing on all GSA FISMA systems during their defined A&A type lifecycle and as part of normal operations and maintenance.

The Contractor shall conduct GSA annual penetration testing based on a defined schedule and CISO approved sampling and scoping methodology for all external facing URIs.

The Contractor shall conduct Ad Hoc penetration testing to support GSA security impact analysis and GSA DFIR incidents and engagements

GSA anticipates conducting approximately 100 penetration tests annually, these being a blend of FISMA system A&A and annual pentests.

SECURITY ASSESSMENT AND AUTHORIZATION (A&A) SUPPORT

Cybersecurity is the ability to protect or defend information systems from cyber-attacks. Cybersecurity is an umbrella term that incorporates different information technology (IT) strategies and security controls that protect networks (e.g., identity management, risk management, and incident management). Information Assurance employs measures that protect and defend information and information systems by ensuring their confidentiality, integrity, availability, authentication, and non-repudiation. These measures include providing for restoration of information systems by incorporating identification, protection, detection, response, and recovery capabilities. As IT evolves, so do the threats to data security, individual privacy, and the continued operation of the Federal Government’s IT assets.

GSA's Staff Offices Division (IST) requires professional technical services to expend reasonable commercial efforts to perform a Risk Management Framework (RMF) Step 4 Full Review for GSA FISMA systems These tasks will be accomplished in accordance with the A&A process described in NIST SP 800-37 Rev 2 and NIST SP 800-53 Rev 5, as well as the GSA provided Security Assessment Plan (SAP), GSA process guidance docs and templates. Assessments will be conducted natveily in GSA’s eGRC security tool.

The contractor shall provide security A&A support. Security authorization is the formal risk management decision by the Authorizing Official (AO) to accept the risk to operations, assets, and/or individuals based on the implementation of an agreed-upon set of security controls in order to authorize operation of an information system. By accrediting an information system, the AO is accepting responsibility for the security of the system and becomes fully accountable for any adverse impacts should a breach of security occur.

It is essential that the AO has the most complete, accurate, and trustworthy information possible on the security status of the information systems, in order to make timely, credible, risk-based decisions as to whether to authorize system operations. The information and supporting evidence needed for security accreditation is developed during a detailed security review of an information system, typically referred to as security certification.

RISK MANAGEMENT FRAMEWORK (RMF) STEP 4 – ASSESS SECURITY CONTROLS

DEVELOP SECURITY ASSESSMENT PLAN

Determine the initial controls to be assessed by reviewing the accepted System Security and Privacy Plans (SSPPs). Once the security controls to be assessed have been identified, the team will use NIST Special Publication 800-53A, Appendix F, to identify an appropriate assessment procedure for each security control and control enhancement. Once assessment procedures have been identified, the team will tailor the procedures by executing the following steps, as identified within SP 800-53A, Section 3.2.3:

- Selecting the appropriate assessment methods and objects needed to satisfy the stated assessment objectives;
- Selecting the appropriate depth and coverage attribute values to define the rigor and scope of the assessment;
- Identifying common controls that have been assessed by a separately-documented security assessment plan, and do not require the repeated execution of the assessment procedures;
- Developing information system/platform-specific and organization-specific assessment procedures;
- Incorporating assessment results from previous assessments where the results are deemed applicable; and
- Making appropriate adjustments in assessment procedures to be able to obtain the requisite assessment evidence from external providers.

Once the security control assessment procedures have been tailored to meet the unique characteristics of the system under evaluation, the team will finalize the Security Assessment Plan (SAP) by including everything that is located in the GSA SAP template. This includes the following information, in addition to the tailored assessment procedures:

- A summary of the security control assessment process;
- A table of personnel participating in the security control process that includes roles and contact information;
- A description of the system, the location(s) where the evaluation will occur and the security objectives of the system;
- A system diagram clearly identifying the assessment boundary;
- A table of system user roles and their descriptions;
- A table identifying the system components that will be evaluated, including hostnames, IP addresses, primary functions, operating systems and major applications;

- A description of the methodology to be used during the assessment;
- General and system-specific rules of engagement;
- A table of tools that have been approved for use within this assessment and their primary purpose(s);
- A preliminary schedule of activities; and
- A signature page that authorizes the assessment and approves of the plan.

The security control assessment plan will identify all planned assessment methods in a manner that ensures repeatability and verification of results by a third party in order to facilitate approval by both GSA staff and potential audit by external agencies.

ASSESS SECURITY CONTROLS

Following approval of the Security Assessment Plan (SAP), the team will execute the plan in accordance with the methods and preliminary schedule of activities. As the assessment is executed, engineers will conduct daily out-briefs/status calls with all interested parties and will conduct a formal out-brief at the conclusion of the assessment. This final out-brief will not be representative of the complete content of the Security Assessment Report (SAR); rather, it will provide interested parties with an understanding of the process that has been executed, significant findings to date, any remaining actions that must be taken prior to the development of the final assessment report, and an anticipated date for the delivery of the final assessment report and the plan of actions and milestones (POA&M).

DEVELOP REPORTS AND POA&MS

Following the conclusion of the security assessment, the team will fully document the results of the assessment of each control and provide verifiable evidence of each finding. Characteristics of this report will include:

- Technical control findings will be supported by screenshots or verifiable digital artifacts;
- Operational control findings will be supported by specific references to policies and procedures, documentation;
- Additionally, a plan of actions and milestones (POA&M) will be developed that identifies:
    - The tasks to be accomplished with a recommendation for completion either before or after information system implementation;
    - The resources required to accomplish the tasks;
    - Any milestones in meeting the tasks;
    - The scheduled completion dates for the milestones

Step 4b – Information System Security Manager (ISSM) Approval

All A&A deliverables will undergo a comprehensive evaluation in accordance with established peer reviews and a security checklist quality control process. Once the deliverables have been approved by the internal contractor quality assurance team, the deliverables will be sent to the GSA ISSM where any required changes by the customer will be updated before the documents are considered final. This peer review process and ATO package documentation turnaround time must fall within five business days.

We require a vendor who can adapt to our on-demand scheduling needs, conduct assessments and penetration testing on-demand, within scope as quickly as possible. The selected vendor also has to meet our quality expectations and have the required NIST NICE certifications, applicable security clearances and subject matter expertise to complete the assessments.

LOW IMPACT (LI) AND MODERATE IMPACT (MI) SAAS ASSESSMENTS

The contractor shall provide support for the assessment of commercial SaaS solutions for processing and storing of LI GSA data. These assessments shall follow GSA Procedural Guide: CIO IT Security 16-75 "Security Reviews for Low Impact SaaS Solutions." Assessment involves reviewing controls for access management, authentication, encryption, vulnerability scanning, and flaw remediation. GSA anticipates conducting approximately 30 LI SaaS assessments annually.

The contractor shall also provide support for MI SaaS assessments following GSA CIO-IT Security-18-88, Revision 1 MiSaaS Security Authorization Process guidelines. GSA anticipates processing 2 MiSaaS assessments annually.

SALESFORCE MINOR APPLICATIONS ASSESSMENTS AND UPDATES

The contractor shall provide support for the assessment and update of Salesforce applications built on Salesforce organizations for FAS, GSA IT, Office of Government-wide Policy (OGP), and PBS. These assessments shall follow GSA Procedural Guide: CIO IT Security 11-62 "GSA's Security Implementation of the Salesforce Platform." GSA anticipates reviewing approximately 100 configuration changes for ISSO approval and 100 updates to existing and creation of new Salesforce application assessment packages annually.

BUILDING MONITORING AND CONTROL (BMC) DEVICE ASSESSMENTS

The contractor shall be a designated Information Systems Security Officer (ISSO), who provides support for the security assessment and vulnerability remediation of BMC devices for the PBS business line. The BMC device approvals shall follow GSA Procedural Guide: CIO IT Security 16-76 "Building Monitoring & Control Device Security Assessment Process." GSA anticipates conducting approximately 70 device assessments annually. This BMC ISSO shall also assist in identifying security gaps in current BMC procedures, and address those gaps by creating and incorporating new procedures into the assessment process. This includes, but is not limited to, a new BMC script approval process. Any new processes or procedures shall be approved by the PBS ISSM and IST Director, and any updates to the CIO IT Security 16-76 must also be coordinated through the ISP Director.

Assessment Level of Effort and Volume

The table below provides an average year of what FISMA assessments look like for GSA along with the associated level of effort per assessment denoted in hours. The contractor staffing model would need to be able to support these differing A&As and ATO types, to include backup staffing.

Assessment Type:	Hours per Assessment:	Assessments per year:
LiSaaS	80 - 324	25
MiSaaS	324	2
LATO	162	5
Low	486	2
Moderate	648	23
High	1053	3
Ongoing Assessments	324	19
Salesforce minor apps	4 - 6	100
BMC devices	162 (small) to 648 (large)	175
A&A Penetration tests	80	50
Annual Penetration tests	80	50

VULNERABILITY AND CONFIGURATION MANAGEMENT

The contractor shall coordinate with OCISO SecOps Division to ensure that the information system to which they have been assigned responsibility has been correctly identified in vulnerability and configuration assessment and enterprise monitoring systems. Additionally, the contractor shall ensure that assessors are notified of false positives, track vulnerabilities from discovery through remediation, document risk acceptance, and maintain a history of documented changes. Vulnerabilities and mis-configurations derived from automated assessment tools are to be documented in the POA&Ms or managed in automated assessment systems. Evidence for review of scan vulnerability reports shall be recorded in the designated scan review tracking sheet.

The contractor shall utilize available GSA enterprise vulnerability, configuration, and monitoring

solutions (including SIEM) to perform log review, verify system inventory, and ensure systems are configured consistent with agency security benchmarks, patched to current patch levels, and securely maintained.

The contractor shall coordinate activities with the SecEng Division to provide basic support for the incorporation of code scanners and analysis tools into GSA's development process.

The contractor shall assess vulnerabilities to ascertain if additional safeguards are needed, ensure systems are patched and security hardened at all levels of the "stack," and monitor to see that vulnerabilities are remediated, as appropriate. The contractor shall review system security audit logs locally or via enterprise management systems to ensure security measures are implemented effectively and operating as intended. The contractor shall coordinate non-standard software/hardware through established approval processes.

The contractor shall manage the process of annual user recertification and user reauthorization for tools maintained by the contractor as in scope of this contract, and shall facilitate annual visitor access control re-certifications for data centers for systems for which they have responsibility.

The contractor shall complete the annual FISMA self-assessment for tools and processes that are in scope of this contract and support and implement continuous monitoring, as assigned.

CONTINUOUS MONITORING

The contractor shall ensure continuous monitoring of assigned information systems. The contractor shall assist in the transition from static security A&A processes and security management to continuous monitoring and ongoing authorization, and shall ensure assigned systems are compliant with continuous monitoring requirements.

The contractor shall ensure the GSA Continuous Monitoring Program is implemented for assigned systems in accordance with GSA Procedural Guide: GSA CIO IT Security 12-66 "Continuous Monitoring" and as documented in the system's security plan and Continuous Monitoring Plan. The contractor shall assist the ISSM in maintaining the overall security posture of the information system by monitoring, analyzing, and reporting on automated security controls for information systems active within the OCISO Continuous Monitoring Program.

The contractor shall ensure that for systems enrolled into the Continuous Monitoring Program, enterprise wide continuous monitoring tools and capabilities are deployed on all assets within the information security boundary. The contractor shall be responsible for monitoring and reviewing the vulnerability and configuration compliance scan results and reports generated by continuous monitoring tools. The contractor shall be responsible for documenting the review and any remedial actions taken to mitigate the vulnerabilities and mis-configurations in accordance with GSA policies. The contractor shall monitor system security audit trails and SIEM reports. The contractor shall be responsible for maintaining the periodic deliverables and maintaining compliance with automated security controls in accordance with GSA Procedural Guide: GSA CIO IT Security 12-66 "Continuous Monitoring."

REPORTING AND DOCUMENTATION REQUIREMENTS

The contractor shall support development and maintenance of security documentation including, but not limited to, the SSPP, Continuous Monitoring Plan, Configuration Management Plan, Contingency Plan, Contingency Plan Test Report, POA&M, user recertification, annual FISMA assessment, and incident reports. Incidents reports are developed, as necessary, POA&Ms are updated quarterly, and all other documents are updated at least annually or when there is a major change as defined in GSA Procedural Guide: CIO IT Security IT 06-30 “Managing Enterprise Risk.”

The contractor shall ensure PTAs/PIAs are completed for IT systems that are new, under development, or undergoing major modifications which impact Privacy Act data.

The contractor shall provide support for data calls. These data calls include OMB, CISA, IT security, FISMA Assessments, IT security metrics, annual access list review, capital planning, budgeting, and capital planning, which includes developing a risk register, operations analysis, and the IT security sections of the Exhibit 300 to support the ISSM, upon request.

The contractor shall be responsible for all users who operate on its assigned system(s). As such, the contractor shall ensure compliance with HSPD-12 requirements and processes. The contractor shall verify that system users have the required authorization, background investigations, need-to-know, and access to internal security practices before access is granted to the system(s) for which the contractor has responsibility.

OPERATIONAL SECURITY METRICS AND KEY PERFORMANCE INDICATORS

Operational Security (OpSec) metrics help an organization determine what is working effectively and what needs to be improved upon within organizational security policies, processes, and technology.

The contractor shall deliver key performance indicators (KPIs) on a monthly basis, as agreed to with GSA, and demonstrate how they’ve been met within their monthly Program Management Report (PMR). These include, but aren’t limited to the following:

a. Tracking of multi-factor authentication that conforms with NIST guidance and improves GSA FISMA systems cybersecurity: 94% of GSA FISMA systems with MFA
b. Coordinate the remediation of cybersecurity vulnerabilities for GSA systems that include outstanding high and critical risks and new risks: < 25 days average to mitigate
c. Coordinate the remediation of known exploited vulnerabilities (KEVs) for GSA systems that include the required criteria contained in the CISA Binding Operational Directive 22-01: <14 days average to mitigate
d. Ensure and track encrypted network connections in transit conform with NIST guidance and improves GSA FISMA systems cybersecurity: 90% of GSA FISMA systems
e. Ensure and track sensitive data encryption at rest that conforms with NIST guidance and improves GSA FISMA systems cybersecurity: 90% of GSA FISMA systems
f. Implement Authority to Operate (ATOs) that conforms with NIST guidance and improves GSA FISMA systems cybersecurity: 100% of GSA systems.

g. Testing of all Incident Response plans and Contingency plans on an annual basis: 100% of GSA systems

AUDIT SUPPORT

The contractor shall provide active participation as a member of the audit team for GSA information systems supported by the contractor and selected as an in-scope system for audit. This support includes, but is not limited to, providing guidance, supporting internal cyber hygiene readiness assessments; audit documentation review, and coordination with stakeholders on requests for providing supporting evidence; meetings to discuss control implementation status and providing demos of the information system functionality; and responses to notification of finding and recommendation (NFR) issued by the auditors at the end of audit; and implementing recommendations and actions as defined in the correction actions plans in a timely manner to close out the findings.

Activities cover the audit spectrum phases of pre-audit, audit, and post-audit activities. The contractor shall continue to remain an active key participant and team member throughout the entire audit cycle. The contractor shall provide necessary support in the investigation of theft of devices or incidents involving assigned systems; activities shall be coordinated with the OCISO SecOps Division that has responsibility for incident reporting and response. The contractor may be required to participate in the Office of Inspector General (OIG) investigation.

KNOWLEDGE MANAGEMENT PROGRAM SUPPORT

The contractor shall support the development of an effective knowledge management capability for the Office of the Chief Information Officer.

Tasks include but are not limited to:

a. Evaluate tools, techniques, and processes for relevance, usefulness, and adoption potential by OCISO.
b. Create and document governance procedures and metrics that lead to the achievement of a mature knowledge management program
c. Create and maintain any tool(s) exclusively used by OCISO for knowledge management.

The contractor shall support creation of easy to consume descriptions, flow-charts of GSA Assessment and Authorization (A&A) processes. The contractor shall maintain Frequently Asked Questions (FAQ). The contractor shall seek to standardize language, reduce the size and complexity of GSA security policies and procedural guides, convert to plain language, and publish in alternate formats that allow for easier searching and consumption by humans and governance systems.

GOVERNANCE SUPPORT

The contractor shall provide information assurance subject matter expertise to GSA governance boards, and assist during the business requirements gathering phase to ensure that security controls are considered during the early stages of new initiatives. The contractor shall assist in ascertaining the best solution that also enables the business to fulfill its goal to support the end customer in the most efficient manner possible.

Contractor ISSOs shall provide a detailed approach that addresses the functional delivery of the specified tasks listed in this section for ISSO support. Tasks will be prioritized and allocated by a designated Government ISSM and/or Federal POC.

Need to include financial penalties for late reporting of operational metrics and/or other security deliverables. The penalty should be of such consequence as to deter future occurrences of late or non delivery of required operational security deliverables

Governance of the A&A security process is currently provided in the following GSA Policy an NIST Guides:

a. GSA IT Security Policy GSA Order P. 2100.1
b. GSA Procedural Guide: CIO IT Security 06-30 “Managing Enterprise Cybersecurity Risk”
c. GSA Procedural Guide: CIO IT Security 06-29 “Contingency Plan Testing”
d. GSA Procedural Guide: CIO IT Security 09-44 “Plan of Action and Milestones (POA&M)”
e. GSA Procedural Guide: CIO IT Security 11-51 “Conducting Penetration Test Exercises”
f. GSA Procedural Guide: CIO IT Security 14-68 “Lightweight Security Authorization Process”
g. NIST FIPS Publication 199
h. NIST FIPS 200
i. NIST Special Publication (SP) 800-18, (Current Version)
j. NIST SP 800-34 (Current Version)
k. NIST SP 800-37, (Current Version)
l. NIST SP 800-47, (Current Version)
m. NIST SP 800-53, (Current Version)

SECURITY AUTHORIZATION PACKAGE COMPLIANCE REVIEWS

Security Authorization package compliance reviews ensure that the AO is presented with complete and reliable security authorization packages to facilitate an informed system ATO decision based on risks and controls implemented.

The guidelines for GSA security authorization packages are documented in GSA Procedural Guide: CIO IT Security 06-30 “Managing Cybersecurity Enterprise Risk.” The guidelines for the Federal Risk and Authorization management Program (FedRAMP) security authorization packages are documented on the FedRAMP site available at http://www.gsa.gov/portal/category/102371.

The contractor shall review GSA and FedRAMP cloud service provider security assessment packages to ensure compliance with documented GSA and FedRAMP processes and requirements, respectively. The contractor shall review documentation and findings in security authorization packages for adherence to GSA and FedRAMP quality and acceptability criteria.

The contractor shall follow OCISO's 'Clean ATO' process documentation and complementary security review checklists.

OCISO anticipates more than 100 GSA FISMA system security authorization packages annually.TASK 10 – POLICY AND COMPLIANCE

The contractor shall support the Policy and Compliance Division. Responsibilities of the division are described in the following paragraph:

The Policy and Compliance Division provides management and maintenance of the GSA Continuous Monitoring and Ongoing Authorization, POA&M, Audit, and Security Training programs. Further, the division develops and maintains GSA security, continuous monitoring policies and procedural guidelines, and supports security audit coordination efforts. The division is also responsible for maintaining the designations and current listing of IT Security Stakeholder or FISMA POCs, an up-to-date FISMA inventory including the FIPS PUB 199 categorization, ATO issue and renewal dates, and ATO and Decommission Letters. Further the division is responsible for FISMA compliance reporting to OMB and DHS and providing responses to other internal and external data calls and performance metrics from OMB, Government Accountability Office (GAO), and DHS.

PROCEDURAL GUIDELINE DEVELOPMENT AND COMPLIANCE

The contractor shall develop and maintain Security Policies annually and GSA IT Security Procedural guides every three years or more frequently if necessary, following changes to Legislation, Federal or GSA requirements and guidance.The contractor shall also develop and maintain templates supporting procedural guides.

Currently GSA maintains two (2) IT Security policies, 44 IT Security procedural guides, 25 Technical Security guides, and approximately 105 templates. New policies and guides may need to be developed as new Federal requirements and guidance gets issued. Also, identified guides may be replaced by different guides, as necessary.

GSA expects approximately between 20 and 30 procedural guide updates and between 20 and 30 supporting template updates every year.

The contractor shall be required to update all guides and templates supporting NIST 800-53 control families within a year of the publication of the new NIST 800-53 revision.

The current list of policies and procedural guides (provided for reference only) that need to be developed and maintained can be found

The contractor shall support GSA review and comment for all NIST Special publications and guidelines, The contractor shall assist with review and triage of requirements for any Federal cyber policies, memorandums and/or executive orders.

COMPLIANCE REVIEWS

POA&M COMPLIANCE REVIEWS

The contractor shall, as directed by OCISO, perform compliance reviews of system POA&Ms to ensure system POA&Ms are completed in accordance with GSA IT Security Procedural Guide 09-44 (Section 9 – List of Attachments, Attachment K). OCISO anticipates **115-120 system** POA&Ms to be reviewed quarterly.

The contractor shall be responsible for developing quarterly POA&M review reports for ISSO, ISSM and CISO/AO reports summarizing review results. The contractor shall be responsible for preparing a briefing deck for OCISO Directors and CISO

ASSESSMENT AND AUTHORIZATION PACKAGE REVIEWS

The contractor shall, as directed by OCISO, perform compliance reviews of system A&A packages, both for new systems and systems undergoing traditional three (3) year reauthorizations to ensure system A&A packages are completed in accordance with GSA IT Security Procedural Guide 06-30, Managing Enterprise Cybersecurity Risk and Clean ATO process guide. The contractor is responsible for completing A&A package reviews using defined checklists and timelines as published in the Clean ATO process guide.

OCISO anticipates over 100 A&A packages every year.

COMPLIANCE REPORTING AND INSPECTOR GENERAL (IG) AND GAO AUDIT SUPPORT

The contractor shall assist OCISO, as necessary with the collection, analysis, reporting, and tracking to comply with GSA and Federal legislation, mandates, and executive orders including, but not limited to, quarterly FISMA submissions, annual IG Audits, GAO Audits, OMB and other Federal Cyber Security Executive orders and memorandums, internal controls assessments, and other internal (GSA) and external data calls.

FISMA REPORTING

The contractor shall assist OCISO with preparing data collection forms (i.spreadsheets and questionnaires within Agency GRC tool) with instructions for completing the data call to assist in gathering the data throughout GSA in accordance with the required FISMA metrics. The contractor shall also support analysis/review of the metrics following the completion of collection activities, to ensure they are complete and accurate. The contractor shall be responsible to provide supporting evidence documents for FISMA metrics associated with programs and processes managed by OCISO. The contractor shall also be responsible for defining strategic and tactical actions to resolve enterprise wide and system specific gaps identified in meeting the targets defined by FISMA metrics.

INSPECTOR GENERAL (IG) AND GAO AUDIT SUPPORT

That contractor shall participate and support annual IG FISMA and Financial audits; system-specific and program audits as published in the GSA IG audit plan for the FY; and any GAO audits lead or requiring support by OCISO.

The contractor shall provide responses and supporting evidence documents to any internal cyber hygiene checklists developed to prepare for audits.

The contractor shall assist OCISO with performing self-assessment of GSA's security processes and controls against the cybersecurity security functions and capabilities defined within FISMA IG metric domains and maturity model. The contractor shall support OCISO with gathering of all required enterprise wide and system specific documents to satisfy audit requirements. The contractor shall support Government personnel in OCISO meetings with the auditors as necessary. The contractor shall support OCISO progress tracking of the mitigation of findings and shall be responsible for implementation of recommendations from the annual IG audit working with the program teams.

The contractor shall assist OCISO in providing required artifacts and preparing responses to GAO Audits. The contractor shall be required to participate with Government personnel, as necessary in any meetings supporting GAO audits.

OTHER FEDERAL AND GSA REPORTING

The contractor shall assist OCISO in performing research, determining impact, creating any data collection templates, analysis, and reviews, preparing responses, and tracking the status of any action items required as part of any ad-hoc GSA internal or Federal compliance reporting requirements including but not limited to Executive orders, OMB memorandums

TRAINING SUPPORT

ROLE BASED TRAINING PROGRAM SUPPORT

The contractor shall support managing and delivering role-based training to personnel with significant security responsibilities.

Tasks include but are not limited to:

- Creating and delivering quality training content and sessions on GSA security policies, procedural and technical guides and corresponding standard operating procedures.
- Identifying industry provided security training and certifications supporting GSA cyber workforce roles and responsibilities
- Managing the training schedule and training sessions
- Planning and executing large-scale training simulations/conferences
- Collaborating with other teams to achieve predefined training outcomes and performance metrics.

The contractor shall manage training records to support evidence-based analysis of program performance and compliance with federal requirements.

The contractor shall promote and manage OCISO training resources available to personnel holding significant security responsibilities.

The contractor shall assist in ad-hoc workforce development activities as defined by the training manager and leadership.

SECURITY AWARENESS PROGRAM SUPPORT

- The contractor shall help the government improve cyber security awareness across the agency.

  Tasks include but is not limited to:
  - Assist with developing a training plan for the Fiscal year
  - Assist with defining measurable performance metrics for awareness training.
  - Creating and maintaining awareness content for the agency's mandatory training courses. When needed, use content creation software to create engaging interactions that improve learning.
  - Evaluate technologies and processes (i.e., gamification, dashboarding) that increase engagement with content. Implement and manage these technologies and techniques.
  - Create engaging and interactive content (e.g. Cybersecurity Tips, Infographics, Quizzes) to support year-round and 'surge' awareness campaigns.
  - Support all campaigns and activities meant to improve security awareness across the agency including supporting campaigns for the Cybersecurity Awareness Month (CSAM).
  - When necessary, perform precise tracking and reporting of course completions to satisfy audit and compliance requirements.
  - Identify, evaluate, and implement novel ways to improve cyber security awareness across GSA.
  - Collaborate with ISO division to improve and operate the GSA phishing program. The contractor shall try automating the entire lifecycle of a phish (i.e. scenario identification, phish, reporting), and increasing its difficulty.

CONTINUOUS DIAGNOSTICS AND MITIGATION SUPPORT

The CDM Program Management Office supports the deployment and management of capabilities supporting prioritized risk management actions, information System continuous monitoring and leveraging these capabilities for responding to CISA emergency and binding operational directives (EDs and BODs).

The contractor shall support CDM PMO tasks including but not limited to:

- Implementation of CDM projects that may come in the form of an official Request For Service (RFS) from CISA and/or internal projects approved by OCISO leadership. In both cases, the CDM PMO focuses on delivering new or expanded capabilities related to Operational Risk Management and cyber hygiene of GSA information systems.
- Assisting with identifying and prioritizing new capabilities and data sources that improves the visibility of the cyber hygiene across GSA information systems and respond to risk-trends.
- Evaluation of new technologies to support near-real-time risk evaluation and management
- Support integration of any new technology and data sources to the existing CDM tool stack
- Identify and document use cases and governance to operationalize the use of CDM capabilities within GSA
- Customize the CDM tooling and visualizations for GSA operational use cases.
-

The contractor shall support tasking related to the compliance and governance of CDM tooling. Tasks may include but is not limited to:

- Creating and maintaining artifacts required to retain an Authorization to Operate within GSA
- Facilitate data calls from CISA or internal stakeholders that require data from CDM tools
- Design and execute procedures that maintain data quality to ensure accurate and expected reporting and operation.
- Recommend and implement automation replacing existing manual processes.

GSA GOVERNANCE, RISK AND COMPLIANCE SUPPORT

The contractor shall provide Development and Operations and Maintenance (O&M) support for GSA’s GRC enterprise management tool. The contractor shall provide development and administration support of the Assessment & Authorization (A&A), Plan of Actions Milestones Management (POA&M), and Continuous Monitoring modules of GSA’s GRC tool.

The contractor shall support GRC tool administration and O&M tasks including but are not limited to:

- Manage and maintain the installation, configuration, patching and other maintenance activities
- Support the creation and maintenance of GRC Assessment and Authorization (A&&) documentation to maintain ATO.
- Maintaining an up-to-date baseline configuration of the GRC tool
- Document and maintain standard operating procedures associated with the

maintenance of the GRC tool

- Provide support for general daytime/weekday monitoring and resolution of system or client level impacting events (operation impacts lasting longer than 25 minutes are considered an outage). General after hour support in the performance of maintenance activities during non-business hours.
- Support incident and event reporting and the restoration of system services including opening of support requests and performing communications with GRC tool vendor professional services.

The contractor shall support the development and operational adoption of the GRC system's capabilities including but not limited to:

- Creation, distribution, and maintenance of end user training materials (e.g., training manuals, Standard Operating Procedures (SOPs)).
- Support for updating of training materials as process improvements are developed per client requirements.

The contractor shall support GRC development efforts to transition GSA's A&A processes natively in the GRC tool; support creation of various compliance checklists; and data calls. Tasks include but are not limited to:

- The contractor shall support the release and adoption of newly released NIST 800-53 revisions using the GRC system's Assessment & Authorization (A&A) capabilities.
- Creation and maintenance of GSA tailored security control baselines per GSA's defined Authorization To Use (ATU) and Authorization To Operate (ATO) processes.
- Configuration, implementation, and maintenance of exportable versions of system's Authorization Package (e.g. mail merge System Security and Privacy Plan (SSPP) export).
- Design, configuration, implementation, maintenance, and monitoring of all Archer system to system integrations to include automated testing and reporting of NIST 800-53 Security Control Objectives.
- Integration with GSA's Single Sign-On (SSO) solution for authentication
- Development of REST and SOAP Application Programming Interfaces (APIs) for integrations with other enterprise security tools and CDM dashboard.
- Implementation and adoption of Open Security Controls Assessment Language (OSCAL) capabilities as the GRC tool vendor supports it.
- Implementation and customization of the GRC Continuous Monitoring module to align with GSA's ISCM processes.
- Support the configuration, implementation, and maintenance of risk dashboards with an agency, organization, and system level capabilities of reporting operational risks. Risk scoring metrics to be measured and reported per qualitative and quantitative data collection originating from within and outside of the GRC tool.
- Implementation and customization of the GRC Plan of Actions Milestones

Management (POA&M) module. This includes development, implementation, and maintenance of system level automated POA&Ms creation and closure.

- Implementation and customization of GRC Risk Based Decision module to support GSA's Acceptance of Risk (AOR) process.
- Support the custom built Agency System Inventory (ASI) application configuration, implementation, maintenance, and integration with external services. This includes maintenance of a data dictionary of defined system attributes maintained within the ASI.
- Support development of compliance checklists to support tracking of periodic activities and deliverables
- Support development of data calls to support external reporting to OMB and CISA

GRC Program Key Performance Indicators (KPIs)

- Archer Development/Enhancement SLAs: An Archer enhancement request increases or provides an improvement in quality, value, or extent to the clients GRC current deployed system capabilities.

Enhancement SLAs

- Implement a Minor enhancement/resolve an identified GRC impact per application, workflow, questionnaire, or role access. Minor enhancement development and deployment LoE will be agreed upon by the government PM and system developer prior to SLA evaluation period beginning.

  Low (20 hours), Moderate (40 hours), High (60 hours)
- Implement a Major enhancement/resolve an identified GRC impact per application, workflow, questionnaire, or role access. Minor enhancement development and deployment LoE will be agreed upon by the government PM and system developer prior to SLA evaluation period beginning.

  Low (40 hours), Moderate (80 hours), High (120 hours)

Development SLAs

- An Archer Development request is a defined client request to add/create a new capability by leveraging the GRC capabilities which requires a system development effort. That includes full client capability testing, role training, capability SOP/documentation, and release communications.

- Implement a major development release with LoE agreed upon by the government PM and system developer prior to SLA evaluation period beginning.

  - Low (260 hours (1 FTE 6.5 weeks, 2 FTEs 3.25 weeks, 3 FTEs 2.2 weeks)
  - Moderate (520 hours (1 FTE 13 weeks, 2 FTEs 6.5 weeks, 3 FTEs 4.3 weeks)
  - High (1,040 hours (1 FTE 26 weeks, 2 FTEs 13 weeks, 3 FTEs 8.5 weeks)

ONGOING AUTHORIZATION PROGRAM SUPPORT

Ongoing Authorizations is defined by NIST as the subsequent (follow-on) risk determinations and risk acceptance decisions taken at agreed-upon and documented frequencies in accordance with the organization's mission/business requirements and organizational risk tolerance. Ongoing authorization is a time-driven or event-driven authorization process. GSA has established an Ongoing Authorization (OA) Program with defined information system qualifying requirements including a full security authorization package and the results of defined continuous monitoring activities that can be used to determine changes in risk and risk acceptance determinations made by authorizing officials.
GSA is actively moving systems from traditional three year authorizations to ongoing authorizations as a fundamental pivot away from traditional compliance to more outcome oriented models focusing on operational security and automation.

Currently, there are 18 systems in the OA program with an additional 3-5 systems expected to be onboarded every year.

The contractor shall support GSA' OA team with tasks supporting GSA's ISCM and Ongoing Authorization Program. Tasks include but are not limited to:

- Maintain ISCM Strategy/OA Program Guide including corresponding checklists and templates and OA program Standard Operating Procedure (SOP)
- OA Onboarding Assessment evaluations against defined OA onboarding pre-requisites and checklists
- Support Biannual Performance Metric Review (PMRs) using defined templates and validation of the data reported by ISCM dashboard and system A&A documentation
- Supporting Annual Performance Metric Reviews.
- ISCM Dashboard Development and NIST 800-53 Security Control Objective Evaluation Automation
- Defining and maturing cloud system OA onboarding and monitoring requirements including performance metric reviews
- Supporting periodic OA Program Status meetings
- Creating monthly ISCM Dashboard Metric Reports

OA PROGRAM KEY PERFORMANCE INDICATORS (KPIs)

- Biannual Performance Metric Reviews (PMRs) - Today's OA Program supports 18 FISMA systems and each undergoes a PMR cycle at the end of Q2 and Q4 each FY. The full PMR processing cycle from system evaluations to final reporting needs to be complete within a month's time frame (April and Oct). The OA Manager and/or assessment team is responsible for completing all applicable Q2 and Q4 systems PMRs on time.

    - Q1 KPI: Reports the results from the prior FY Q4 PMR processing (Oct)
        - Reported as the % of the total # of systems completed on time as scheduled
    - Q3 KPI: Reports the results of that FY Q2 PMR processing (April)
        - Reported as the % of the total # of systems completed on time as scheduled

- Annual Performance Metric Reviews (PMRs) - Today's OA Program supports 18 FISMA systems and each undergoes an Annual PMR cycle that requires the evaluation of the system's compliance with specific Change Management (CM), Access Management (AC),and OA requirements. At the beginning of each FY systems are scheduled to perform their Annual PMR per an assigned quarter (Q1, Q2, Q3, or Q4). The OA Manager and/or assessment team is responsible for completing each system's Annual PMRs per quarter on time.
    - Q1 KPI: Reports the results of the completed Q1 Annual PMRs
        - Reported as the % of the total # of systems completed on time as scheduled
    - Q2 KPI: Reports the results of the completed Q2 Annual PMRs
        - Reported as the % of the total # of systems completed on time as scheduled
    - Q3 KPI: Reports the results of the completed Q3 Annual PMRs
        - Reported as the % of the total # of systems completed on time as scheduled
    - Q4 KPI: Reports the results of the completed Q4 Annual PMRs
        - Reported as the % of the total # of systems completed on time as scheduled
- OA Onboarding/Pre-AO Assessment Evaluations - Today's OA Program supports 18 FISMA systems with an OCISO goal of adding 3-5 systems each FY. To achieve this goal the ISCM Manager will need to identify candidate systems for the OA Assessment activities to begin. Candidate systems are identified by evaluating their compliance per the defined OA Onboarding Checklist Prerequisite Requirements. Annually the OA Manager will need to complete 8 system's Pre-AO Assessment Evaluations for systems that have completed a full 3 year A&A in the past 18 months.
    - Annual KPI: Reports the results of the total completed system Pre-AO Assessment Evaluations during the FY with the requirement of 8 systems to be completed.
        - Reported as a % of 8 systems completed (can be reported as pass/fail or met/not met)
- OA Onboarding/OA Assessments - Today's OA Program supports 18 FISMA systems with an OCISO goal of adding 3-5 systems each FY. To achieve this goal the ISCM Manager and/or assessment team will need to complete 4 systems OA Assessment activities per each FY. The OA Manager is responsible for tracking the completion of each system's OA Assessment tasks. From completing its OA Kickoff to finalizing the Onboarding Assessment Report (OAR).

  - Annual KPI: Reports the results of the total completed OA Assessments during the FY with the requirement of 4 systems to be completed.
    - Reported as a % of 4 systems completed (can be reported as pass/fail or met/not met)
- Maintain ISCM Strategy/OA Program Guide and OA Program Standard Operating Procedure (SOP) - Annually the ISCM Strategy Guide and the OA Program SOPs will need to be reviewed, updated, and disseminated as required updates are identified.
  - Annual KPI: Reports the results of the ISCM Strategy Guide and the SOP documentation being maintained by the ISCM Manager.
    - Reported as a % of completion (can be reported as pass/fail or met/not met)
- ISCM Dashboard Development and NIST 800-53 Security Control Objective Evaluation Automation -
  -
- OA Program Cloud Systems Onboarding & PMR Development - The systems supported by the OA Program
  -
- Monthly ISCM Dashboard Metrics Reports - GSA has created an ISCM Dashboard capability that provides status monitoring and reporting of information system's compliance and functional state with the IT Security Enterprise monitoring tools. Monthly the ISCM Manager will need to create a Monthly ISCM Dashboard Metrics Report. That reflects the rollup results of each defined monitored metric across all monitored assets.
  - Annual KPI: Reports the results of monthly ISCM Dashboard Metrics Reports generated, disseminated, and on time (by the 10th business day of the following month).
    - Reported as a % of 12 reports completed (can be reported as pass/fail or met/not met)

ICAM AND C-SCRM

The contractor shall support the ICAM Shared Services Division. Responsibilities of the division are described in the following paragraph:

The ICAM Shared Services Division supports consolidating and coordinating Identity Credential, and Access Management-related capabilities to focus on improving ICAM governance across GSA IT. The Division is also responsible for managing C-SCRM assurance for GSA IT and its systems, and also supports agency-wide C-SCRM activities. Additionally, the Division leads Zero Trust Architecture strategy efforts, to include leading a Program Management Office overseeing a series of Zero Trust initiatives.

C-SCRM SUPPORT

The contractor shall support the management and direction of the OCISO C-SCRM Program, which currently services for GSA IT and for GSA systems, including:

- Providing coordination, oversight, and analysis for C-SCRM events and incidents
- Establishing and maintaining C-SCRM procedures

- Facilitating supplier reviews
- Identifying potential supplier threats
- Providing continuous monitoring for cyber supply chain threats
- Defining and identifying cyber supply chain events and incidents

The contractor shall identify and establish new capabilities and shall support program activities that include, but are not limited, to three main components: Pre-award, Post-award, and Ongoing C-SCRM Program Support. The contractor shall develop standardized criteria and processes to support the OCISO C-SCRM Program that are approved by the Government.

Pre-award C-SCRM operations include reviewing original equipment manufacturers (OEM) ICT suppliers and their components prior to the award of acquisition contracts that meet established government approved criteria. This analysis focuses on the information pertinent to the supplier as well as their products. Pre-award components and tasks include, but are not limited to:

- Developing standardized criteria and processes for pre-award C-SCRM activities
- Tracking of suppliers that have already been reviewed
- Developing pre-award supplier profiles and supporting vendors questionnaires
- Working with acquisition teams to incorporate C-SCRM into their procurements

Post-award C-SCRM operations focus on activities related to continuous monitoring and review of security practices of OEM suppliers and IT service providers to ensure cyber supply chain risks are continuously mitigated, and include, but are not limited to:

- Developing standardized criteria and processes used for evaluations and monitoring
- Supporting C-SCRM event and incident handling
- Coordinating component-level testing of hardware conducted by third-party providers to identify security or compliance risk
- Identification and usage of third-party supplier illumination tools to supplement C-SCRM analyst findings

Ongoing C-SCRM Program support activities are related to providing and maintaining an effective and up-to-date C-SCRM program, and include:

- Identifying and monitoring critical risk suppliers.
- Communicating with identified suppliers to update any necessary and relevant information for the needs of the program

GSA estimates one (1) analyst for this function to support an estimated forty (40) C-SCRM supplier reviews and five (5) C-SCRM events annually. This estimate may increase in option years due to changes in GSA’s acquisition volume and processes.

ICAM SERVICE OPERATIONS AND ENGINEERING SUPPORT

The contractor shall support the on-going operations and maintenance of the current or future ICAM service applications. The contractor shall:

- Perform upgrades and patching of the applications

- Monitor and resolve alerts and Tier 2 help desk tickets
- Process access requests for GSA enterprise users as needed
- Establish new or updated environments as needed
- Work with cross-functional GSA IT and business teams to achieve prioritized improvements to continuous delivery and automated release management tasks as needed
- Support On-going authorization activities including, but not limited to:
    - Supply technical information to Information System Security Officer(s)
    - Provide updates to the architecture diagrams and documentation
    - Provide updates to the System Security and Privacy Plan(s)
    - Monitor compliance with system security controls
- Develop program guidance to further enhance capabilities, improve performance and user acceptance

The contractor shall utilize GSA provided toolsets and collaboratively work with cross-functional GSA IT teams.

The contractor shall provide service design and implementation services in order to improve the quality of new and existing services. This includes recommending and implementing when approved the changes and improvements necessary to increase or maintain value to GSA missions over the lifecycle of services, the continuity of services, achievement of service levels and service level agreements, and conformance to standards and regulations. The contractor shall:

- Design and implement features and integrations for GSA enterprise including integration with enterprise IT service management platforms
- Design and perform onboarding of additional privileged access management tools and frameworks for GSA IT assets including but not limited to:
    - Windows Servers
    - Security Appliances
    - Network Appliances
    - Databases
- Design and perform implementation of new authoritative source data connectors for GSA user accounts
- Onboard applications for access requests,provisioning and continual certifications
- Provide continued design and development of automated release management, and scalable repeatable automation
- Support updates to continuous diagnostics and mitigation (CDM) dashboard reporting initiatives

GSA estimates five (5) ICAM systems engineers and one (1) ICAM analyst for this function. This estimate may increase in option years due to changes in GSA's acquisition volume and processes.

ICAM GOVERNANCE SUPPORT

The governance of GSA’s ICAM Shared Services Portfolio, is managed by the ICAM Shared Services Division (ISI) and works collaboratively across IT and business lines. In support of this effort, the contractor shall:

- Advise and assist in developing ICAM strategies to define requirements, eliminate duplicative efforts, identify technology standards, and align ICAM shared service capabilities across the agency
- Implement ICAM strategies across GSA service offices and IT divisions
- Review the existing ICAM environment to understand capability gaps and recommend improvement opportunities for ITAB consideration
- Evaluate business requirements to chart recommendations for the future ICAM environment of GSA
- Advise and assist in developing and maintaining an ICAM roadmap to ensure that ICAM solutions and technologies are not fragmented or duplicative
- Collaborate with the Identity, Credentialing and Access Management Sub-Committee (ICAMSC) of the Federal Chief Information Security Officer Council (CISO Council) to ensure Federal mandates and policies are reviewed and implemented in accordance with the federal government roadmap as appropriate.

The contractor performance of duties shall include, but is not limited to, to the following:

- Conducting analyses and providing input into technology, process, and policy recommendations for decision-making
- Reviewing the current ICAM strategies and working collaboratively to execute the initiatives identified
- Reviewing current National Institute of Standards and Technology (NIST), Office of Management and Budget (OMB), Information Security, Personnel Security, and other Federal guidance and agency goals to provide guidance and ensure alignment
- Recommending changes to GSA policies and orders relevant to ICAM
- Engaging with customers to understand business processes to shape ICAM policies, procedures and technology needs
- Developing efficient procurement and licensing strategies for preferred technologies and services for GSA IT
- Updating the overall portfolio of ICAM solutions, systems, applications, and technology standards for GSA IT
- Working towards standardization of service offerings for GSA IT
- Evaluating new initiatives or proposed solutions prior to deployment to ensure alignment with GSA’s ICAM architecture and roadmaps, where appropriate

The ICAM Portfolio will provide product ownership support for GSA’s enterprise ICAM tools and the contractor shall provide support in these activities to include suggestions for configurations and product strategies and roadmaps.

GSA estimates one (1) analyst for this function. This estimate may increase or decrease in option years due to changes in GSA's IT and environment and support models.

ZERO TRUST ARCHITECTURE SUPPORT

The contractor shall provide on-going oversight of initiatives related to GSA's Zero Trust Architecture strategy to align with NIST SP 800-207 and M-22-09, *Federal Zero Trust Strategy*. Initiatives are based on GSA's Zero Trust Strategy, and include an award for an Advancing Zero Trust project by the Technology Modernization fund. Support for Zero Trust Architecture and initiatives may include the following to support the Advancing Zero Trust Program Management Office:

- Oversight for project teams
- Financial projections and review of acquisition requests
- Developing presentations materials, monthly and quarterly deliverables
- Responses to requests from the TMF Board and TMF PMO

GSA estimates one-quarter (0.25) analysts for this function for the base period. This task is not expected to last beyond the first option period.

CROSS DIVISIONAL

DHS CISA develops and oversees the implementation of Binding Operational Directives (BODs) ,and Emergency Directives (EDs), and Federal Cybersecurity Coordination, Assessment, and Response Protocol (C-CAR) which require action on the part of civilian Executive Branch agencies that fall under CISA's authorities. GSA is an agency that falls under CISA's authorities. GSA Security Operations support the Binding / Emergency Operational Directive maintaining and execution of all nine BOD / ten ED with the a projection increase of of 2 new ED and 1 BOD yearly

- The contractor shall support the maintenance and tracking of all BOD, ED, and C-CAR and report to the Vulnerability Management Product Owner or appropriate system owner / ISSO / ISSM of remediation action to comply with each Directive
- The contractor shall provide a monthly summary report of each Directive status and action required to comply with the directives
-

TECHNICAL WRITING

The contractor shall provide the following training and technical documentation support services to maximize IT efficiency and stakeholder satisfaction:

- Identify tasks which can be solved by the end user without help desk support;
- Assist in collecting and organizing information required for preparation and improvement of user's manuals, training materials, installation guides, proposals, and reports
- Draft communication (e.g., web pages, emails, videos) to guide users through the self-help steps
- Edits user's manuals, special reports, or any other customer deliverables and documents as requested

- Ensure that technical documents are written in clear readable format which can be understood by technical and non-technical personnel
- Ensure conformance to existing standards by revising text and making recommendations to changes in scope where necessary
- Write, in coordination with cross-functional IT teams, the on-boarding procedures for GSA IT application engineers and IT Program Managers to integrate or use systems and tools
- Provide reviews of data such as help desk tickets, web analytics, surveys etc. to determine GSA end user needs and deliver information for management to achieve strategic goals.

GSA estimates one (1) technical writer for this function in the base period of performance. The out years will be based on need.

HIGH VALUE ASSET (HVA) SUPPORT

- The contractor shall provide Certified Assessment Evaluation and Standardization (AES) assessment team members to support HVA assessment that include a Cyber Resilience Review (CRV) and Risk and Vulnerability Assessment (RVA) courses. The government will provide a certified External Dependencies Management (EDM).
- The contractor shall coordinate and conduct an HVA assessment based on CISA Assessment Evaluation and Standardization (AES) and provide a report to IS within 60 days of completion. Number of Assessments can range between 2-5 assessments per year (**Note**: Assessment may require to be completed onsite) and required to be completed within 3 years of last assessment.
- The contractor shall support and coordinate DHS/CISA assessments for Tier 1 HVA systems
- The contractor shall provide a dedicated Information System Security Officer (ISSO) support to manage GSA HVA FISMA boundaries. This include remediation/tracking of assessment findings for HVA systems as documented in the Plan of Action and Milestones (POA&M) and approved by CISO and Authorizing Official (AO)

PROJECT MANAGEMENT / SCRUM MASTER SUPPORT

- The contractor will provide cross divisional support project management
- The contractor shall have certified/trained individuals using the CISA the Assessment Evaluation and Standardization (AES) program to support Tier 2 HVA assessments for each HVA system within a three (3) year timeframe.
- The contractor support documentation and assessment of any HVA overlay controls identified as part of the baseline for HVA systems.

- GSA estimates one (1) project manager for this function in the base period of performance. The out years will be based on need

KEY PERSONNEL

The following are the minimum personnel who shall be designated as “Key.” The Government does not intend to dictate the composition of the ideal team to perform this TO.

a. Program Manager (PM)
b. Lead Security Engineering Specialist (ISE)
c. Lead FedRAMP Specialist (ISE)
d. Lead Security Operations Specialist (ISO)
e. Lead A&A Compliance Specialist (ISP)
f. Lead ICAM Specialist (ISI)
g. Lead Cyber Supply Chain Risk Management Specialist (ISI)
h. Lead Incident Commander - TS/SCI (Required) (ISO)

PROGRAM MANAGER (PM)

The PM shall be responsible for the day-to-day oversight of contractor personnel and TO performance. The PM shall have full authority to make all commitments and decisions for all elements of the TO. The PM shall proactively address all Government concerns to the best of their ability.

It is required that the PM has the following qualifications:

a. A project management certification, such as Project Management Institute (PMI) Project Management Professional.
b. Experience with designing and implementing information security plans for enterprises with diverse sets of complex applications, databases, network connections, and communications subsystems.
c. A minimum of five or more years’ experience managing client IT security systems similar in scope and complexity of this TO.
d. A minimum of three years’ experience in a supervisory capacity managing IT security systems.

It is desired that the PM has the following qualifications:

a. Experience implementing security procedures in accordance with best practice methodologies such as Carnegie Mellon’s Software Engineering Institute (SEI). Capability Maturity Model Integration (CMMI) standards, and/or the IT Information Library (ITIL).
b. Knowledge of Federal IT policy, regulations, and best practices to include NIST and FIPS guidelines.

LEAD SECURITY ENGINEERING SPECIALIST

The Lead Security Engineering Specialist shall be responsible for ensuring the quality of all performance under tasks relating to Security Engineering and DevSecOps. The Lead Security Engineering Specialist shall be responsible for all activity related to Security Engineering, DevSecOps, AppSec, Security Automation, Hardened Images and other Task 5 related activities.

It is required that the Lead Security Engineering Specialist has the following qualifications:

e. At least ten years of specialized experience in cloud development and cloud security security, and DevOps/DevSecOps. should be highly technical, have strong problem solving skills in securing large scale Kubernetes (K8s) environments and developing secure cloud and container applications. Solid development background and understanding of serverless, K8s pod security, service mesh and network policies.
f. Bachelor of Science (BS) degree or greater in Computer Engineering, Electrical Engineering, or Systems Engineering.

It is desired that the Lead DevSecOps Specialist has the following qualifications:

a. Extensive Knowledge of web application security, secure coding and source code reviews (such as Python, Java, C, C++, .NET, APEX and RoR), cloud security, virtualization security, Building/Physical Security, and MS Network architecture and design.
b. In depth knowledge of security architecture, AWS cloud infrastructure and cloud security with at least five years of experience as a cloud security architect and developing hardening benchmarks for cloud and containers.

LEAD FEDRAMP SPECIALIST

The Lead FedRAMP Specialist shall be responsible for ensuring the quality of all performance under tasks relating to FedRAMP. The Lead FedRAMP Specialist shall be responsible for all activity related to FedRAMP authorization including but not limited to architecture review and briefing, FedRAMP package and artifacts review, remediation support and continuous monitoring.

It is required that the Lead FedRAMP Specialist has the following qualifications:

g. At least ten years of specialized experience in cloud architecture and cloud security technologies including but not limited to AWS, GCP, and Azure. Have expert knowledge of FedRAMP authorization.
h. Bachelor of Science (BS) degree or greater in Computer Engineering, Electrical Engineering, or Systems Engineering.

It is desired that the Lead Security Engineering Specialist has the following qualifications:

c. Extensive Knowledge of security best practices and engineering principles such as virtualization security, web application security, network architecture, container technology, CICD pipeline, logging tools, hardening best practices, encryption, FIPS validation, vulnerability management,configuration management, and multi-factor authentication. Hands on experience in cloud architecture and cloud security.

LEAD SECURITY OPERATIONS SPECIALIST

The Lead Security Operations Specialist shall be responsible for all performance under tasks relating to security operations.

It is required that the Lead Security Operations Specialist has the following qualifications:

a. Certified Information Systems Security Profession (CISSP) designation.
b. Expert knowledge of Federal IT security standards (i.e., FISMA) and auditing standards. Expert knowledge of penetration testing tools, vulnerability management (including for containers), application white listing tool management, firewall management, server management, and command line scripting, with hands-on experience in the past three years.
c. In depth knowledge of Windows, Linux, and Unix/Solaris OSs, AWS/Cloud architecture, and network and wireless protocols.
d. Experience with managing DevOps or DevSecOps sprints.

It is desired that the Lead Security Operations Specialist has the following qualifications:

a. At least five years of experience with enterprise OS scanning, configuration scanning, container scanning, and web application scanning and testing in environments of similar size and scope, with hands-on experience in the past three years.
b. Experience with triaging vulnerabilities, writing and implementing hardening guides, penetration testing, Wi-Fi scanning, and war dialing

LEAD A&A COMPLIANCE SPECIALIST

The Lead A&A Compliance Specialist for this TO shall be responsible for ensuring all A&As are done completely, without error, and in compliance with all applicable rules and regulations.

It is required that the Lead A&A Compliance Specialist has the following qualifications:

a. Current CISSP designation.
b. At least five years of experience developing the required documents for the A&A package (e.g., SSP, CP, and SAR) including oversight and development of POA&Ms,

   and performing all continuous monitoring functions with the most recent experience occurring in the last three years.
c. In-depth knowledge in cloud/AWS architecture and security, operating systems (Windows, Linuxs, and Unix).
d. Experience with managing DevOps or DevSecOps sprints.

It is desired that the Lead A&A Compliance Specialist has the following qualifications:

a. At least five years of experience with and detailed knowledge of FedRAMP, NIST, OMB, US-CERT, and CISSP with the most recent experience in the last three years.
b. Experience in applying risk management techniques to develop and complete

risk assessments based on NIST standards to ensure system design and implementation sufficiently addresses or mitigates IA risk.

c. At least five years of experience implementing NIST SP 800-53a security controls for Federal agencies.

LEAD ICAM SPECIALIST

The Lead ICAM Specialist for this TO shall be responsible for all performance under tasks relating to ICAM.

It is required that the Lead ICAM Specialist has the following qualifications:

a. At least five years of experience with the design and documentation of ICAM workflows and standard enterprise ICAM tools, such as cloud and native directories and data stores, and Identity Governance and Administration (IGA) platforms.
b. At least five years of hands-on experience developing and implementing ICAM governance models, stakeholder engagement mechanisms and overall ICAM program operations.
c. At least 3 years managing a team performing technical and business implementations of new IT platforms.

It is desired that the Lead ICAM Specialist has the following qualifications:

a. Certifications relevant to ICAM tools in use by GSA (e.g. SailPoint Certified IdentityNow Engineer, SailPoint Certified IdentityIQ Engineer, Cyberark Level One: Trustee, Cyberark Level Two: Defender, Level Three, Sentry)
b. Experience in ICAM engineering operations in a Federal environment.
c. Experience with DHS CDM program objectives and implementations.
d. Project management experience or related certification.

LEAD C-SCRM SPECIALIST

The Lead C-SCRM Specialist for this TO shall be responsible for all performance under tasks relating to C-SCRM.

It is required that the Lead C-SCRM Specialist has the following qualifications:

d. At least five years of experience in cybersecurity operations or risk management
e. At least two years of experience with the development and management of an enterprise Cyber Supply Chain Risk Management program.
f. At least two years of experience with supplier illumination tools to highlight vendor cyber supply chain risk
g. Expert knowledge of NIST SP 800-161 guidelines for cyber supply chain risk management.

It is desired that the Lead C-SCRM Specialist has the following qualifications:

h. Experience in Cyber Supply Chain Risk management in a Federal environment or a large private sector enterprise.

LEAD Incident Commander

The Lead Incident Commander Specialist shall be responsible for all performance under tasks relating to security operations.

It is required that the Lead Security Operations Specialist has the following qualifications:

e. Certified Information Systems Security Profession (CISSP) designation.
f. Expert knowledge of Federal IT security standards (i.e., FISMA) and auditing standards. Expert knowledge of penetration testing tools, vulnerability management (including for containers), application white listing tool management, firewall management, server management, and command line scripting, with hands-on experience in the past three years.
g. In depth knowledge of Windows, Linux, and Unix/Solaris OSs, AWS/Cloud architecture, and network and wireless protocols.
h. Experience with managing DevOps or DevSecOps sprints.

It is desired that the Lead Security Operations Specialist has the following qualifications:

c. At least five years of experience with enterprise OS scanning, configuration scanning, container scanning, and web application scanning and testing in environments of similar size and scope, with hands-on experience in the past three years.
d. Experience with triaging vulnerabilities, writing and implementing hardening guides, penetration testing, Wi-Fi scanning, and war dialing

KEY PERSONNEL SUBSTITUTION

The contractor shall not replace any personnel designated as Key Personnel without the written concurrence of the FEDSIM CO. Prior to utilizing other than Key personnel specified in its quote in response to the RFQ, the contractor shall notify the FEDSIM CO and COR of the existing TO. This notification shall be NLT ten calendar days in advance of any proposed substitution and shall include justification (including resume(s) and labor category of proposed substitution(s)) in sufficient detail to permit evaluation of the impact on TO performance.

Substitute Key personnel qualifications shall be equal to, or greater than, those of the Key personnel substituted. If the FEDSIM CO and COR determine that a proposed substitute Key personnel is unacceptable, or that the reduction of effort would be so substantial as to impair the successful performance of the work under the TO, the contractor may be subject to default action.

NON-KEY PERSONNEL

The contractor shall provide non-key Personnel Security Engineers working in support of this TO. The contractor is responsible to allocate qualified staff to support requirements of this TO.

In support of this TO, Security Engineers performing Task 2.5.5.2 Subtask 5.2 – DevSecOps Support shall have the following required qualifications:

a. Understand cloud and cloud security.
b. Have experience working in a DevOps/DevSecOps model
c. Possess coding and scripting knowledge.

Security Engineers performing Task 2.5.3.3 Subtask 3.3 – Security Consulting and Engineering Support shall have the following qualifications:

a. Technical proficiency with Amazon Web Services (AWS) (AWS Solutions Architect or SysOps/DevOps Certification).
b. DevOps or DevSecOps experience; proficiency with various scripting language (such as Python, Node, Ruby, and YAML).
c. Security integration and automation experience.

It is desired that the ICAM Engineers performing Task 2.5.9.2 Subtask 9.2 – ICAM Service Operations and Engineering Support shall have the following qualifications:

a. Three (3) years experience with the design and documentation of either privileged access management, identity governance and administration, or single-sign on solutions, based on their task assignments.
b. Certifications relevant to ICAM tools based on their task assignments (e.g. SailPoint Certified IdentityNow Engineer, SailPoint Certified IdentityIQ Engineer, Cyberark Level One: Trustee, Cyberark Level Two: Defender, Level Three: Sentry)
c. Experience in ICAM engineering operations in a Federal environment

GOVERNMENT-FURNISHED PROPERTY (GFP)

The GFP is listed in Section 9 - List of Attachments, Attachment G. The GFP will be provided during transition-in and as required by the tasks in the SOW.

SECURITY REQUIREMENTS

The contractor shall comply with agency personal identity verification procedures identified in the RFQ that implement HSPD-12 FIPS PUB Number 201. The contractor shall insert this clause in all subcontracts when the subcontractor is required to have physical access to a federally controlled facility or access to a Federal Information System. Work on this project may require contractor personnel to have access to limited information to fully integrate financial, operational, procurement, and personnel data. The clearance is considered sensitive, but unclassified. All contractors issued a GSA email address shall maintain current contact information in the GSA Credential and Identity Management System (GCIMS) system.

Contractors shall comply with GSA Order P.2100.1K "IT Security Policy," GSA Order ADM 9732.1C – "Suitability and Personnel Security," and OCHCO/OCIO HSPD-12 Personal Identity Verification and Credentialing SOPs. Background investigations are required for access to GSA information systems (including contractor operations that design, operate, test, maintain, and/or monitor GSA systems). The applications in scope of this TO are categorized as “Moderate Risk” systems; therefore, contractors supporting the project shall be required to undergo a Minimum Background Investigation (MBI). The contractor shall adhere to all security-related laws, requirements, and regulations that bind the Government. The contractor shall have all staff members complete a confidentiality agreement prior to working under this contract. Contractor personnel involved in the management, operation, programming, maintenance, and/or use of IT shall be aware of these responsibilities and fulfill them. Detailed security responsibilities for the contractor are found in the GSA Orders/Handbooks listed in the RFQ.

Contractor personnel working under this TO will not be required to have a security clearance. When Government on-site meetings are required, the Government will provide personnel to ensure approved contractor personnel have access to Government facilities. Selected contractor employees may be required to complete mandatory Security Awareness and Privacy Training (this training is often provided internally by GSA via GSA Online University).

The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of the TO. The contractor shall implement procedures to ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of sensitive Government information, data, and/ or equipment. The contractor’s procedures shall be consistent with Government and GSA policies, including GSA Order 2100.1, Information Technology Security Policy (or most current version), OMB Memorandums and Circulars, FISMA, the Computer Security Act of 1987, and the Privacy Act. In addition, during all activities and operations on Government premises the contractor shall comply with the policies, rules, procedures, and regulations governing the conduct of personnel or protection of Government facilities and data as expressed by GSA, written or oral.

INFORMATION ASSURANCE

The contractor may have access to sensitive (to include privileged and confidential) data, information, and materials of the U.S. Government. These printed and electronic documents are for internal use only and remain the sole property of the U.S. Government. Some of these materials are protected by the Privacy Act of 1974 (AMENDED). Unauthorized disclosure of Privacy Act or covered materials is a criminal offense.

GSA IT SECURITY REQUIREMENTS

The contractor shall deliver an IT Security Plan within 30 calendar days of award that describes the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this order. The IT Security Plan shall comply with applicable Federal laws including, but not limited to, 40 U.S.C. 11331, the FISMA of 2002, and the E-Government Act of 2002. The IT Security Plan shall meet IT security requirements in accordance with Federal and GSA policies and procedures, including General Services Administration Acquisition Regulation (GSAR) clause 552.239-71, Security Requirements for Unclassified Information Technology Resources (Jan 2012). The contractor shall submit written proof of IT security authorization six months after award, and verify that the IT Security Plan remains valid annually.

PERIOD OF PERFORMANCE
The anticipated period of performance for this Task Order is a 12-month base period of performance and four (4) 12 month option period as detailed below:

Base Period:	August 3, 2023 - August 2, 2024
Option Period 1:	August 3, 2024 - August 2, 2025
Option Period 2:	August 3, 2025 - August 2, 2026
Option Period 3:	August 3, 2026 - August 2, 2027
Option Period 4:	August 3, 2027 - August 2, 2028

RFI RESPONSE SUBMISSION

Interested vendors are required to provide an electronic copy in Microsoft Word or Portable Document Format (PDF) of their response (Attachment A- RFI Questions) to Contract Specialist, Kenya McPherson, kenya.mcpherson@gsa.gov and Contracting Officer, Erica Pelham at erica.pelham@gsa.gov by **March 24, 2023, 11:00 AM EST.**

Cover Page should include the following:

- Business Address, Telephone
- Primary Point of Contact (POC) name, email, phone number and web address
- Business size and socio-economic classification (small, SDVOSB, WOSB, etc)
- Possible NAIC codes associated with this action
- GSA Schedule or other contracting vehicle contract number (if applicable)
- SAM UEI

Send written responses to Kenya McPherson, Contract Specialist, kenya.mcpherson@gsa.gov and cc: Erica Pelham, Contracting Officer, erica.pelham@gsa.gov, email subject header: **RFI #-47HAA023N0002 - CISCO Support III -{company name}.** No collect calls or telephone inquiries will be accepted.

Any questions regarding this RFI should be directed to the contract specialist and contracting officer. No Classified information will be included anywhere in your responses.

All proprietary information must be clearly marked in accordance with the instructions set forth below in “Marking Requirements.” Any information submitted in response to the RFI may be disclosed to GSA and other Government personnel. All information marked as proprietary information will be safeguarded by GSA to prevent unauthorized disclosures to on-government personnel and entities in accordance with applicable law and regulation. The GSA reserves the right to challenge proprietary information markings.

Notwithstanding any proprietary information marking, GSA shall be able to include any information provided by interested sources, in a subsequent Request for Quote (RFQ), should one be issued.

Marking Requirements: The header and footer of each page containing interested source proprietary information shall be marked with the legend “PROPRIETARY INFORMATION.” Further, the particular paragraph(s) section(s), etc. containing the actual proprietary information shall be clearly high-lighted or otherwise marked by the Respondent.
This is an RFI. No solicitation exists; therefore, do not request a copy of the solicitation.