Request for Information (RFI) #: 47HAA023N0002

Question for Vendors

Security Engineering and Operations Support III
(CISCO 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

Issued: March 6, 2023
Responses due: March 24, 2023, 11:00 AM EST

Questions for Vendors

Program/Contract Management

1. What is the offeror's management methodology for handling lines of authority and communication, organizational structure, and problem resolution. Discuss how contractor personnel will be held accountable for performance.
2. What is the offeror's approach to transitioning-in to TO performance, maintaining quality services, and mitigating any risk to GSA OCISO security function.

Experience and Background in Delivering Cyber Innovation and Resilience

3. Discuss Corporate Experience that reflects experience on projects that are similar in size, scope, and complexity to the requirements. Discuss the scope of work, the period during which the work occurred, the dollar value of the work performed, the client and project, the specific responsibilities of the offeror, major deliverables produced, performance measures/service levels applied, any awards that were received for superior performance (only include awards in past performance and if applicable, include any technical platforms, languages, operating systems, etc.), and any problems or issues that occurred and the corrective action taken.
4. What are your CPAR scores?

Maintaining a Leading Cybersecurity Workforce

5. What is the approach to hiring, retaining, and replacing appropriately cleared personnel throughout the life of this TO?
    a. Certifications --- NIST NICE / DoD 8140 (e.g., GIAC, OSCP, AWS, CISSP, CCSP, CISM)
    b. Existing Security Clearance (E.g., TS/SCi or MBI; depends on role)
    c. What is your mean time to recruit talent? (i.s., Engineers, DevSecOps, ISSOs, Assessors, Pentesters)

Security Engineering

6. **AppSec -** GSA is implementing a program area that focuses on Application security, API security, Mobile Application security, and Software supply chain security leveraging the Supply chain Levels for Software Artifacts (SLSA) framework. What experience (achievement, years of engagement, skill sets) do you have in delivering one or multiple of these security capabilities? What is your approach and what differentiates your approach?

7. **Agile & DevSecOps -** GSA is actively seeking to promote and transition to a DevSecOps working model, expanding the OCISO DevSecOps Program services including security tooling integration, security as code automation, hardened container images and embedding DevSecOps engineers to provide ongoing security support including vulnerability remediation assistance. What experience (achievement, years of engagement, skill sets) do you have in delivering one or multiple of these security capabilities? What is your approach and what differentiates your approach?

8. **FedRAMP -** GSA has an active FedRAMP sponsorship program and supports 35 fedRAMP vendors today. The expectation is that the OCISO FedRAMP Program will be adaptive to accommodate the potential surge support in time of need and to roll back to typical capacity which is around 5 new vendors annually. The vendor is also expected to provide Continuous Monitoring capabilities. What experience

(achievement, years of engagement, skill sets) do you have in delivering one or multiple of these security capabilities? What is your approach and what differentiates your approach?

Governance and Security Compliance

9. **eGRC tool implementation -** What is your experience(# of years, skills) with designing and implementing a full scope eGRC tool including FISMA inventory management, implementing agency specific customized Assessment and Authorization processes, development of SSPPs, performing assessment and maintenance of POA&Ms natively within the tool, creating checklists for periodic security deliverables, and supporting internal/external data calls? What approaches did you use to ensure CX/UX for any capability and feature implementation?

    a. Please articulate your skills and experience with designing workflows, implementation and training on eGRC capabilities aligned and customized to Agency processes and templates.
    b. Please articulate your experience with OSCAL and eGRC tooling to include automated control-based assessments Supporting Control-Based Risk Management with Standardized Formats

10. **Ongoing Authorization Program -** 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.

    What is your experience (# of years, skills) with supporting and managing ongoing authorization and more holistically Information Security Continuous Monitoring programs for Federal Agency including but not limited to defining and implementing Ongoing Authorization processes and metrics, defining risk indicators and creation of automated risk management dashboards available for both operational and executive teams providing near real time visibility into the security posture of the systems. What is your approach and what differentiated your approach?

Security Operations

11. **Security Delivery via a Product (vs Service) Orientation -** GSA is actively moving towards a 'Product" delivery model for key shared services including SASTaaS, FWaaS, SCANaaS, and SOCaaS. What experience do you have in delivering key security capabilities following a "product' delivery model? What is your approach and what differentiates your approach?

12. **Zero Trust Architecture Transformation -** GSA is in the process of implementing a Zero Trust Architecture aligned with CISA and NIST Special Publication 800-207 guidelines. What experience do you have in working with federal agencies in implementing Zero Trust capabilities - be specific. Provide 3-5 examples.

13. **Infrastructure- and Security-as-Code Security Operations -** GSA manages over 60 security tools that range from appliances, SaaS products, and on-premise. Please describe your experience in managing IDSs, IPSs, Next Generation Firewalls, SASE solutions, EDR, XDR, SIEM, and CASB at an enterprise level, identifying the number of users in those environments. Due to the magnitude of the O&M requirements of these tools, automation is essential:

    a. *Infrastructure as code (IaC)* - Describe your approach in managing solutions using agile methodology and IaC. Provide specific techniques and solutions to provide automated configuration, deployment and management to administer these unique environments.

    b. *Compliance as code (e.g. OSCAL)* - Describe your approach in implementation of OSCAL for a dynamic environment that consists of cloud and on-prem environments that are part of hybrid cloud ecosystems.

    c. *Security as Code (SaC) Automation* - Describe your approach in discipline of integrating security tooling for CI/CD pipeline that will save time and money toward Software development lifecycle? What will be some of the challenges that can help security "shift left" in our internal processes and support customers in multi-cloud tenants and for legacy on-premise environments.

14. **Security Operations Center & Incident Response Support -** GSA operates a petabyte scale enterprise logging platform in a SaaS solution for the GSA enterprise, provided via a SOCaaS orientation. The SOC as a Service (SOCaaS) consists of components, including: Automation, Machine Learning, Customer Dashboarding, AI; Incident Response and Forensics (on-prem, endpoint, mobile, and cloud);
    a. *Incident Response/Forensics* - Please describe your experience in managing an Incident Response team and coordinating with multiple stakeholders across the federal government. Please describe your experience in overcoming challenges an organization can receive when facing a security incident in a multi-cloud environment and how your approach to resolve this challenge.

    b. *SOCaaS* - Please describe your experience and challenges in managing a 24x7x365 remote workforce SOCaaS solution that supports a hybrid multi-cloud tenant ecosystem. What metrics and KPI have you developed to measure the effectiveness of a SOCaaS program?

    c. *Cyber Threat Intelligence and Cyber Threat Hunt* - Please describe your experience and approach in successfully conducting a Threat Hunt activities in multi-cloud and on-premise environments. Does this experience include decentralized networks?

15. **Vulnerability Management, VDP/Bug Bounty, and HVA Support -** GSA SecOps supports an enterprise vulnerability management program that includes multiple environments and devices. Additionally, support the HVA program, Vulnerability Disclosure Program (VDP) using a commercial service provider that includes Bug Bounty support and a number of systems.
    a. *VDP / Bug Bounty* - Please describe your approach around centralized vulnerability management, including aggregating findings from multiple tools.
    b. *Vulnerability Managemen*t - Please describe your experience in maintaining a

vulnerability management program that aggregates vulnerabilities from OS, Database, Web, Container, and cloud environments, including experience in providing threat based decisions on priority decisions. Vulnerabilities must be managed and reports distilled through a central hub to ensure a stream for all vulnerability management data vs individual reports per tool.

c. *HVA* - Have you managed and assessed HVAs? Do you have DHS CISA HVA Assessor certification?

Identity Credentialing and Access Management (ICAM)

16. **Identity, Credentialing and Access Management (ICAM) Architecture and Governance -** Please describe your experience developing, implementing and executing an enterprise ICAM architecture and strategy, including any specific expertise that distinguishes you from others in this area. Please describe your expertise in any specific software or product in addition to governance or program development capabilities.

17. **Privileged Access Management** - GSA currently manages a privilege access management solution for managing administrative access to endpoints. Please describe your experience in deploying privilege management solutions in an enterprise environment.

18. **Identity Governance and Administration (IGA) Solutions -** GSA is in the process of migrating and expanding usage of its enterprise IGA solution. Please describe your experience in expanding IGA solutions to enterprise applications to enhance user provisioning and lifecycle management processes.

ISSO Support and Security Assessment Services

19. **Security Assessment Services**
    1. Please articulate the importance off these NIST standards/guidance documents and detail your experience utilizing them in Federal/Civilian agency enterprise-wide environments supporting FISMA:
        - NIST 800-53/A, Revision 5
        - NIST 800-37, Revision 2
        - NIST 800-171/172, Revision 2
        - Are there other NIST SPs that we should take into consideration?
    2. Detail your experience with security orchestration automation and response (SOAR) tooling. Provide a recent example that was successfully implemented.
    3. Please articulate your penetration testing expertise and methodologies. Detail your pentest toolkit and processes followed.
    4. Please articulate how you've developed technical ISSOs geared toward devsecops and an agile, operational security model.
20. **Security Authorization Services**
    1. Detail your experience with developing and maintaining ATO package documentation to include, but not limited to:
        a. Performing Detailed Security Architecture Reviews in collaboration with Security Engineering. What should be detailed in a security architecture review and why?

b. System Security and Privacy Plans (SSPPs)
c. Plan of Actions & Milestones (POA&Ms)
d. Security Assessment Plans (SAPs)
e. Security Assessment Reports (SARs)
f. Supporting collateral documents and appendices (e.g., IR Plans, CM Plans, CP Plans, etc.)
g. Drafting and staffing of Certification memos and Authorization letters for stakeholder signatures