Attachment 07
OFFEROR RESPONSE WORKSHEET, ACKNOWLEDGEMENTS, AND CERTIFICATIONS

Offeror must provide complete responses to each item below. Insert your responses into this worksheet directly below each question or prompt.

I. Indicate the Service Category(ies) Offeror is responding to:

- ☒ **Category 1: Risk Assessment and Mitigation Services**
- ☒ **Category 2: Incident Response Services**
- ☐ **Category 3: Breach Coach Services**
- ☐ **Category 4: Notification and Credit Monitoring Services**

II. OFFEROR INFORMATION

A. Company's Full Legal Name:
Science Systems and Applications, Inc.

B. Primary Business Address:
10210 Greenbelt Road, Suite 600, Lanham, MD 20706

C. Federal Tax Identification Number:
52-1087599

D. Entity Type:

- ☐ Sole Proprietorship
- ☐ Partnership
- ☐ Limited Liability Company
- ☒ Corporation

E. Artificial Intelligence Disclosure. Was artificial intelligence technology used in the development or completion of any portion of this proposal? (Check one of the below.)

- ☐ Yes
- ☒ No

III. BUSINESS DETAILS

A. <u>Company Website.</u> Provide a URL for your company's website.

The SSAI company website is www.ssaihq.com.

B. <u>Company History.</u> Provide a brief history of your company, including the year of its founding and any material acquisitions or mergers in which it has been involved.

Science Systems and Applications, Inc. (SSAI) is an SBA-certified, Woman-Owned Small Business (WOSB) founded in 1977 with approximately 500+ world-class employees. SSAI has no parent company. Our subsidiaries include Elucidation Concepts and Advanced Mission Partners (AMP).

SSAI has supported over 175 contracts for federal agencies, leading universities, and cutting-edge science institutes. SSAI is ISO 9001:2015 certified, has been appraised at Capability Maturity Model Integration (CMMI) Maturity level 3 (Dev), and uses Capability Level 3 rated processes. SSAI has contributed to 160 NASA space and Earth science missions requiring complex satellite data processing, information security, data management and data center management services. We also have a top secret facility clearance. Our technical, management and administrative staff excel in supporting public and private clients by using innovative techniques to process, assimilate, maintain, execute clients' changing needs.

C. <u>Company Size.</u> Identify the number of employees working for your company.

SSAI currently has over 500 world-class employees.

D. <u>Ownership Structure.</u> Describe your company's ownership structure.

SSAI is a privately held company led by a dedicated and experienced leadership team. Dr. Shilpa Bahethi - CEO of SSAI, leads with clarity and makes quick, informed decisions that help us to respond to our customers' needs. Because our program managers have a direct line to corporate leadership, we're able to stay agile and responsive, something our partners and customers value.

We also work closely with small companies that bring deep expertise in specialized areas. SSAI leads and coordinates these efforts, creating a truly collaborative, "badgeless" environment as the prime contractor, where everyone works side by side toward common goals. In perfect parallel, our corporate teams handle everything from IT security and quality assurance to finance, HR, and safety—giving our technical teams the support they need to stay focused on the mission.

SSAI's two subsidiaries, Elucidation Concepts and Advanced Mission Partners (AMP), add even more capability to our team. Elucidation is a certified Minority-Veteran Owned Small Business (VOSB) that provides cybersecurity, systems engineering, integration testing, and evaluation services—especially for Department of Defense and Intelligence Community programs. AMP focuses on designing, building, and testing high-quality electronic systems and precision-machined components. Their manufacturing team has more than 150 years of experience and a strong focus on quality, efficiency, and customer satisfaction.
Altogether, our structure and approach reflect who we are: an agile, mission-centric company that values clear leadership, efficient processes, and strong, lasting partnerships.

E. <u>Litigation.</u> List all claims of non-performance or breach from customers in excess of $5,000, including all pending litigation matters (including civil, criminal, or appellate) or criminal convictions in the past 5 years for the company and all principals. Attach an additional document if necessary.

SSAI does not have any non-performance or pending litigation matters.

IV. PROPOSAL CONTACT

(ME) The Contractor must provide a Contract Manager as the single point of contact for management of the NASPO ValuePoint Master Agreement (include: Name, Title, Email, Phone Number), administered by the state of Idaho. The Contract Manager must have experience of managing contracts for services similar to those required in this RFP. Describe in detail your proposed Contract Manager's experience managing contracts for services like those required in this RFP. Provide a detailed resume for the proposed Contract Manager. Additionally, provide the name, phone number, email address, and work hours of the person who will act as Contract Manager if you are awarded a Master Agreement. The Proposal Contact must be able to respond timely to communications from the Lead State. Offeror must, within 24 hours, notify the Lead State of any change to Offeror's Proposal Contact.

Ms. Anna Cruz will serve as SSAI's Contract Manager. She is a dynamic executive leader with 15+ years of experience managing information technology contracts across federal, state, and commercial sectors. She built and scaled technical divisions, led cross-functional global teams, and managed multimillion-dollar programs that serve mission-driven organizations like NIH, HUD, HHS, GSA, HRSA, EPA, DOT, and NASA.

At SSAI she developed digital transformation strategies, and helped shape emerging technologies that enhance IT programs. She thrives at program management, managing diverse teams, modernizing infrastructure, and ensuring innovation aligns with contract goals.

Ms. Cruz is bilingual in English and Spanish. She has a Master of Business Administration (MBA) degree and active certifications including Project Management Professional (PMP), Certified Scrum Master (CSM), Certified Professional in Supply Management (CPSM), Microsoft Azure 104 (AZ-104), Program Management Professional (PGPM), Certified Scrum Product Owner (CSPO) and Information Technology Infrastructure Library (ITIL).

Name	Anna Cruz
Contact	Phone: 301-768-6377 Email: anna.cruz@ssaihq.com
Title	Director of Business Development, IT & AI Solutions
Specializations	Government Contracts, AI/ML, Cybersecurity, Public Sector Innovation
Education	MBA – Business Administration, University of Maryland MS – Technology Management, University of Maryland BA – Psychology, University of Maryland BA – Communications, University of Maryland Graduate Certificate – Project Management, University of Maryland
Professional Experience	
Director of Business Development, IT & AI Solutions – SSAI (Current)	
• Built Health IT division • Leads federal and state AI/ML, IT and cyber program initiatives • Developed partnerships with NIH, HHS, FDA, HRSA • Oversaw technical teams and international operation	
Chief Operating Officer – Exequt (Feb 2021 – Jan 2024)	
• Managed 25-person team • Grew revenue by $7M • Led Azure and ServiceNow implementations	

• Oversaw operations, budgets, marketing, and mentorship programs
Senior Program Manager – HUD BOSS OIG (Sep 2019 – Feb 2021)
• Managed $8M+ T&M budget • Led Agile transformation • Oversaw Azure Cloud and ServiceNow rollouts
Senior Program Manager – GSA IAE Contractor (Aug 2018 – Sep 2019)
• Consolidated 10 federal websites • Led Agile SAFe (Scaled Agile Framework) processes and change management
Senior Consultant – Salmon Group (Nov 2017 – Sep 2018)
• Built PMO for GSA Innovations Division • Led process improvement and marketing campaigns
Program Director – Silver Strands Systems (Sep 2015 – Oct 2017)
• Led business development and capture for federal contracts • Focused on HUD programs
Senior Project Manager – REI Systems (Feb 2015 – Mar 2016)
• Managed HRSA and HUD projects • Implemented Salesforce and MicroStrategy
Senior Consulting Manager – Manhattan Strategy Group (May 2010 – Jan 2015)
• Managed federal projects for HUD and DOT • Developed Location Affordability Portal
Senior Program Manager – DB Consulting (Jan 2007 – May 2010)
• Provided remote support to 360+ PHAs • Led outreach and promotional strategies

V. TECHNICAL RESPONSE. This section contains technical requirements pertaining to Information Security Services. Other sections of this RFP contain additional requirements that must be met to be considered responsive. Mandatory Evaluated (ME): (ME) requires a response which is evaluated by the evaluation team. Offerors who do not provide a response to a (ME) section may be found nonresponsive.

VI. For Sections A-D, Offerors must respond to the section(s) for the Service Category(ies) Offeror is responding to.
For Section E-I, Offerors must respond to these sections.

A. Category 1 – Risk Assessment and Mitigation Services – Experience and Qualifications

- **(ME) Offeror's Experience. Describe your company's experience, demonstrating that your company has a minimum of five (5) years of experience providing services similar in scope and size to the Category 1 Risk Assessment and Mitigation Services required in Attachment 02 Scope of Work. Provide specific examples that illustrate the specific services furnished and the size, composition, etc. of the entities for whom you have provided services that you are using to demonstrate that your experience meets this minimum requirement.**

SSAI has over 45 years of experience identifying, analyzing, and addressing potential information security risks for our internal assets and external client infrastructures. The table below summarizes SSAI's three most relevant contracts with cybersecurity and information security services.

SSAI's 3 Largest Contracts	Period of Performance	Contract Value	IT Security Services
Sciences Technology and Research Support Services (STARSS III) – NASA Langley Research Center	12/1/2016 – 5/31/2023	$307M	SSAI provided science, research, and technology support services to NASA Langley Research Center's Science Directorate. We managed the Atmospheric Science Data Center which included ingesting, archiving, processing, protecting and distributing data, and providing user support for a wide range of atmospheric science data.
Support for Atmospheres Modeling and Data Assimilation (SAMDA) – NASA Goddard Space Flight Center	3/1/2017 - Present	$298M	SSAI provides comprehensive support for atmospheric sciences, modeling, and data assimilation research conducted by NASA's Earth Science Division. This includes ensuring the security, proper management, and controlled dissemination of satellite data. Accordingly, we are required to implement a robust IT security management plan and maintain compliance with NASA and DoD regulatory obligations.
Hydrosphere, Biosphere and Geophysics Support Services (HBG)	4/1/2020 - Present	$425M	SSAI provides comprehensive support services for NASA's HBG sub-division and the Terrestrial Information Systems Laboratory (TISL). This involves maintaining, enhancing, and operating several Data Centers and its secure websites that archive, distribute, and provide user services for NASA data products.

For the above-mentioned customers, SSAI constructs its team with the intentional selection of domain-specific teammates that demonstrate proven IT capabilities in Cyber Security, Penetration Testing, and Forensic Analysis. Our experts have vast industry experience and training, and a proven history of providing strong cybersecurity measures. SSAI is very confident in the team's ability to meet customer needs and exceed range security requirements.

Team SSAI approaches cyber security with holistic systems focusing on protection of networked systems. As done in compliance with other states' frameworks, Idaho's government is met through use of the industry's leading technologies for threat detection and response tailored to these services with respect for proprietary relationships legally bound compliance uphold as needed.

SSAI does not keep data sent by clients without storing it with full attention to data stewardship during all aspects of data processing and handling. All data provided to SSAI by the client retains exclusive ownership rights and is secured by our system-controls and personnel. To that end, we address the following key areas to ensure a robust security posture:

- **Network Security**: SSAI implemented a comprehensive perimeter defense strategy that includes next-generation firewalls, network segmentation policies, and intrusion detection and prevention systems (IDS/IPS). All network telemetry is encrypted mode in transit and using FIPS 140-2 trusted protocols and securing U.S.-based environments. Continuous monitoring is placed to detect anomalous behavior across network traffic flows, and network access is strictly governed by Zero Trust principles.

- **Application Security:** Our team applies a rigorous secure development lifecycle (SDLC), incorporating static and dynamic application testing (SAST/DAST) to identify and remediate vulnerabilities across web and legacy applications. SSAI ensures compliance with standards such as OWASP and integrates security reviews into CI/CD pipelines, enabling early detection and correction of coding flaws without transmitting application data beyond approved boundaries.
- **Endpoint Security:** SSAI deploys modern Endpoint Detection and Response (EDR) capabilities, fully integrated into an Extended Detection and Response (XDR) platform. This allows for centralized visibility and rapid response to threats targeting workstations, servers, and mobile assets. We strictly enforce device control policies and ensure endpoint data remains within the scope of authority defined by the Purchasing Entity.
- **Data Security:** Data entrusted to SSAI is encrypted both at rest and in transit using FIPS 140-2 compliant algorithms. We implement robust Data Loss Prevention (DLP) policies and access restrictions to ensure sensitive data is protected throughout its lifecycle. SSAI ensures that all data remains in the Purchasing Entity's exclusive property.
- **Identity & Access Management:** We apply Zero Trust principles across all IAM operations, incorporating Role-Based Access Control (RBAC), Multi-Factor Authentication (MFA), and least-privilege access models. All user and administrator access is logged, monitored, and reviewed routinely, with identity governance aligned to NIST SP 800-53 and CIS Controls.
- **Database and Infrastructure Security:** SSAI conducts in-depth configuration reviews and vulnerability assessments for databases, servers, and critical infrastructure components. We use NIST, CIS Benchmark, industry best practices, and automated compliance tools to ensure hardened baselines are enforced. All assessments and operational activities remain within the geographic and logical boundaries required under the State's data location policies.
- **Cloud Security:** SSAI offers deep expertise in secure cloud operations within FedRAMP/Government authorized platforms such as Microsoft Azure Government and AWS GovCloud. We implement Cloud Security Posture Management (CSPM), monitor for misconfigurations, and integrate native security services such as Azure Defender and AWS Security Hub to maintain continuous compliance.
- **Mobile Device Security:** Mobile access is secured through the use of Mobile Device Management (MDM) and Mobile Application Management (MAM) platforms. All mobile devices are configured for encryption, policy-based access, remote wipe, and compliance validation. Data storage on mobile endpoints is disabled unless explicitly authorized and encrypted.
- **Security Awareness and Training:** SSAI delivers targeted security training programs aligned with NIST 800-50 and 800-53 awareness requirements. Topics include phishing prevention, secure handling of sensitive information, and incident reporting. Our simulated phishing campaigns and training modules are role-based and auditable, ensuring a measurable improvement in organizational cyber hygiene.
- **Vulnerability and Threat Management**: Our vulnerability management lifecycle includes regular internal and external scans. Findings are mapped against the CVSS scoring system and MITRE ATT&CK® Framework to prioritize remediation efforts. SSAI supports the State with actionable mitigation plans, executive-level reporting, and compliance-focused dashboards.
- **Penetration Testing:** Our team of experts specializes in ethical hacking and penetration testing to identify and remediate security vulnerabilities within your systems. SSAI's penetration testing approach is conducted by certified ethical hackers and is designed to identify, exploit, and document real-world vulnerabilities in a manner that supports both risk prioritization and regulatory compliance.

Our methodology follows industry-recognized standards including NIST SP 800-115, OWASP Testing Guide, and MITRE ATT&CK® to emulate attacker behaviors and assess the effectiveness of your security controls. Testing may include (as authorized by the Purchasing Entity):

- External and internal network testing
- Web application and API testing
- Social engineering simulations (phishing, USB drops, etc.)
- Wireless security assessments
- Privilege escalation and lateral movement simulation, and
- Physical security assessments (if scoped)

All testing is conducted using pre-approved Statements of Work and is scoped in collaboration with the Purchasing Entity to ensure safety, minimize operational disruption, and meet legal and compliance boundaries. SSAI's penetration testing services specifically address the following RFP priorities:

- Proactively identify exploitable vulnerabilities across the entity's systems, applications, and infrastructure.
- Evaluate threat likelihood and severity, including real-world impact scenarios.
- Provide a detailed final report (per Section 2.2.3 of the Scope of Work) with technical findings, business-risk implications, and step-by-step remediation guidance.
- Include privacy impact insights and compliance observations (HIPAA, CJIS, FERPA, GLBA, and applicable state statutes).
- Support follow-up consultation to clarify technical findings or assist with mitigation planning
- Ensure that all evidence gathered during testing is handled securely, and reporting is compliant with the State's requirements for confidentiality and non-retention of data.

All penetration testing will be conducted by trained personnel with a minimum of five years of professional experience (per Section 2.3.1), and testing activities will be coordinated to support minimal disruption to operations.

- Forensic Analysis: In the event of security breaches, our forensic analysis services will aid in the identification, preservation, extraction, analysis, and reporting of forensic evidence of such events. This will empower customers to respond and communicate effectively to security incidents and mitigate future risks. Governance, Risk, and Compliance (GRC).
- Our GRC services are tailored to ensure the development and management of a robust security program, including:
    1. Governance - Establishing systems and processes to direct and control the cybersecurity program;
    2. Risk Management - Implementing a comprehensive risk methodology, i.e., assessment, mitigation, and establishing risk tolerance; and
    3. Compliance - Ensuring adherence to cybersecurity standards such as ISO 27001 and NIST CSF, with the development of policies, procedures, metrics, and monitoring to meet and exceed industry benchmarks.

Team SSAI is committed to performing the following functions, and any others deemed necessary, to keep customers' system optimized and protected:

- Implementing Access Control and Identity Management by employing robust access controls and identity management solutions to ensure users only access authorized areas.

- Optimizing Performance by maintaining and implementing a schedule for regular system patches and upgrades and conducting engineering assessments, including but not limited to providing trade-off analyses and assessments for improvements of overall capability and technical enhancements.
- Performing Risk Assessments to identify potential vulnerabilities, threats, and risks regarding customers' IT infrastructure and data and analyzing the impact and likelihood of identified risks to prioritize mitigation efforts.
- Continuous Monitoring/testing and providing detailed reports on incidents and vulnerabilities.
- Carrying out Incident Response and Disaster Recovery by performing risk management, investigating security breaches, and mitigating future risks; developing and regularly testing incident response and disaster recovery plans to enable a rapid and effective response to security incidents or disruptions; and establishing offsite backups and redundancy measures to enhance resilience.
- Managing Compliance by ensuring all documentation, process diagrams, and technical architectures are baselined and accurate; tracking and documenting IT security exceptions, configurations, and compliance controls; tracking key performance indicators (KPIs) and key risk indicators (KRIs), to measure the effectiveness of cybersecurity efforts; ensuring compliance with relevant regulations, standards, and legal requirements; and regularly auditing and assessing compliance to identify and address any gaps.
- Maintaining Safety and Security Policies by updating the organizational System Security Plan; ensuring compliance with customer Security procedures; and supporting annual audits
- Providing Security Awareness Training to keep employees abreast of the latest security threats, best practices, and the importance of adhering to security policies.

CYBERSAFE FRAMEWORK ™

SSAI offers the CYBERSAFE FRAMEWORK™, a comprehensive cybersecurity approach designed specifically for the public sector. This framework prioritizes resilience, compliance, and adaptability, incorporating top-tier controls, proactive risk intelligence, and a commitment to continuous improvement. More than just a security protocol, CYBERSAFE™ is a mission-aligned philosophy that SSAI customizes for states and modern government IT infrastructures.

SSAI's CYBERSAFE FRAMEWORK™ Process is a systematic, end-to-end methodology ensuring robust cybersecurity:

- "C", Critical Asset Identification: SSAI maps mission-critical assets and systems. By applying NIST RMF and Zero Trust principles, SSAI baselines the operational environment, ensuring complete visibility across the ecosystem. This step includes asset and data classification, threat modeling, and identifying external and internal vulnerability points.
- "Y", Yielding Risk Intelligence: SSAI integrates AI-enhanced threat detection and predictive analytics to generate timely and actionable risk intelligence, aiming to prevent breaches before they occur. Key components here are real-time threat detection (using SIEM and XDR), continuous risk scoring and posture evaluation, and AI-based behavioral analytics.
- "B", Building Secure Architecture: SSAI deploys modular, scalable, and encrypted-by-design architectures that strictly adhere to FedRAMP, FISMA, and HIPAA requirements. This involves cloud-native security, microsegmentation with least privilege principles, and the implementation of a Zero Trust network architecture.
- "E", Enforce Policy & Compliance: Rather than simply meeting compliance standards, SSAI streamlines and automates the process by embedding continuous controls monitoring (CCM) directly into workflows.

This includes policy orchestration, user-friendly compliance dashboards, and automated evidence generation for elements like SSP, POA&M, and ATO readiness.

- "R", Responding and Recovering swiftly: For rapid response and recovery, SSAI implements thoroughly tested incident response and disaster recovery playbooks specifically tailored to state agencies, ensuring immediate, verifiable, and secure recovery. This is supported by a 24/7 Security Operations Center (SOC), automated incident containment, and immutable backups with rollback capabilities.
- "S", Securing the Human Layer: SSAI's human-centric approach aims to train, test, and empower staff to act as the primary line of defense. This includes role-based training and phishing simulations, insider threat detection, and the development of strong governance and a robust cyber culture.
- "A", Analyzing & Improving Continuously: Through automated logging, red teaming exercises, and post-mortems, SSAI ensures that no risk goes unexamined. This stage incorporates penetration testing and ethical hacking, continuous audit and control tuning, and ML-based anomaly detection and refinement.
- "F", Forecast Emerging Threats: To stay ahead of threats, SSAI leverages federal threat exchanges like CISA and MS-ISAC, alongside SSAI's own AI lab, for predictive cybersecurity research. This involves utilizing intelligence feeds and predictive threat models, integrating secure AI for cyber defense, and comprehensive threat horizon mapping.
- "E", Engaging Stakeholders Transparently: From procurement to program management, the CYBERSAFE FRAMEWORK ™ ensures that all stakeholders are informed, involved, and aligned. This is achieved through real-time dashboards for leadership, regular briefings, reports, agency-centric Key Performance Indicators (KPIs), and shared success metrics for multi-agency missions.

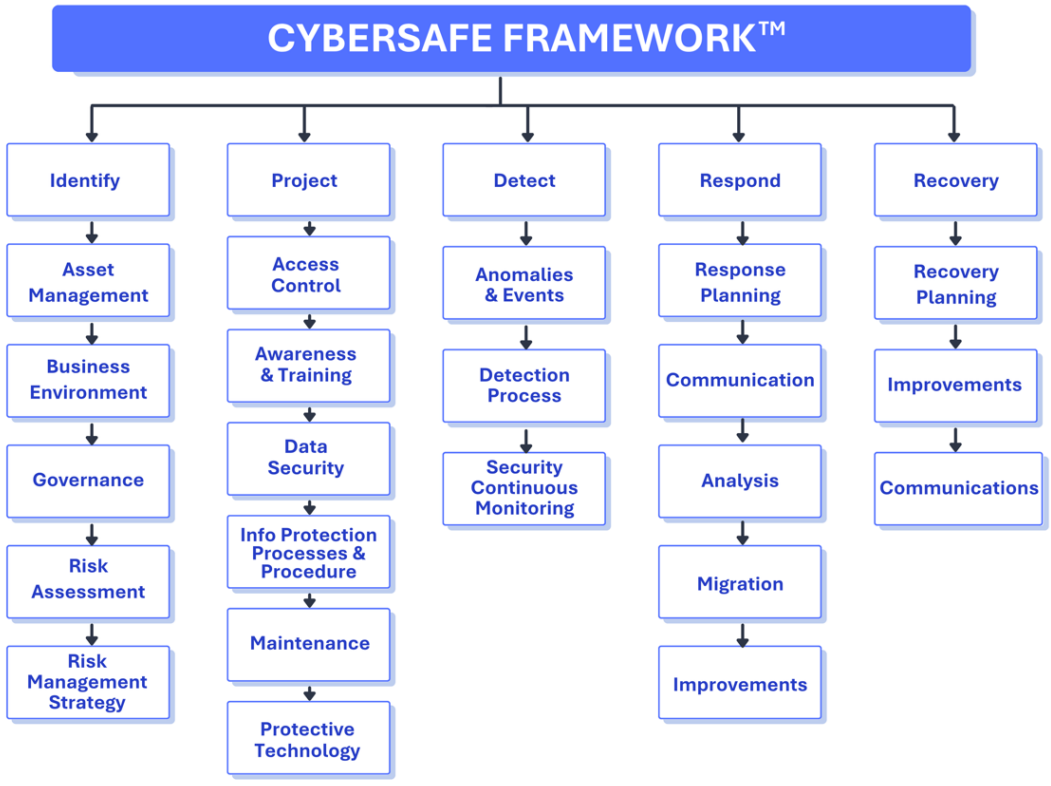


Figure 1: SSAI CYBERSAFE FRAMEWORK ™

Risk Assessment

SSAI conducts a risk assessment process that categorizes risks into qualitative, semi-qualitative, and quantitative values to evaluate potential impacts comprehensively. The process uses defined scales for financial loss, privacy breaches, and reputational damage, assigning levels such as Very High, High, Moderate, Low, and Very Low. Financial losses are quantified in ranges from over $100 million down to less than $100,000, while privacy risks consider the disclosure of sensitive or non-sensitive information affecting varying numbers of individuals. Reputation risks are assessed based on the percentage of clients affected and the extent of media coverage, ranging from widespread national news concerns to limited impact on a single client with no media attention.

By applying this structured framework, SSAI systematically measures and classifies risks to prioritize mitigation efforts effectively. The use of both qualitative descriptions and quantitative thresholds allows SSAI to capture the severity and scope of different risk types, ensuring a balanced and detailed understanding of potential threats. This approach supports informed decision-making by clearly linking risk levels to specific financial, privacy, and reputational consequences, enabling SSAI to manage and reduce organizational vulnerabilities proactively.

Figure 2: SSAI Risk Matrix

The strategic underpinnings of our risk scoring are tied to our belief that risk is dynamic and that we must manage it preemptively and proactively. In that vein, SSAI conducts a comprehensive risk assessment and mitigation process that includes several key phases. First, SSAI identifies risks by recognizing threats to operations, assets, individuals, and vulnerabilities both internal and external, including those related to software, hardware, data, and IT sectors. Next, SSAI analyzes these risks by evaluating potential outcomes and their impact on IT project goals, quantifying and qualifying the risks. Then, SSAI prioritizes risks through a thorough assessment involving stakeholder input, historical data analysis, maintaining risk registers, considering interdependencies, and ranking risks based on severity and likelihood. Following prioritization, SSAI develops mitigation strategies by choosing among risk avoidance, reduction, transfer, or acceptance approaches tailored to each risk. Finally, SSAI implements and monitors these strategies by executing mitigation actions, continuously tracking risks and their impacts, reviewing effectiveness, and adjusting plans as needed throughout the project or organizational lifecycle. Considering an increase in ransomware and phishing attacks, our process is mapped to the MITRE ATT&CK® framework, along with clear visuals that help stakeholders understand how we protect their networks.

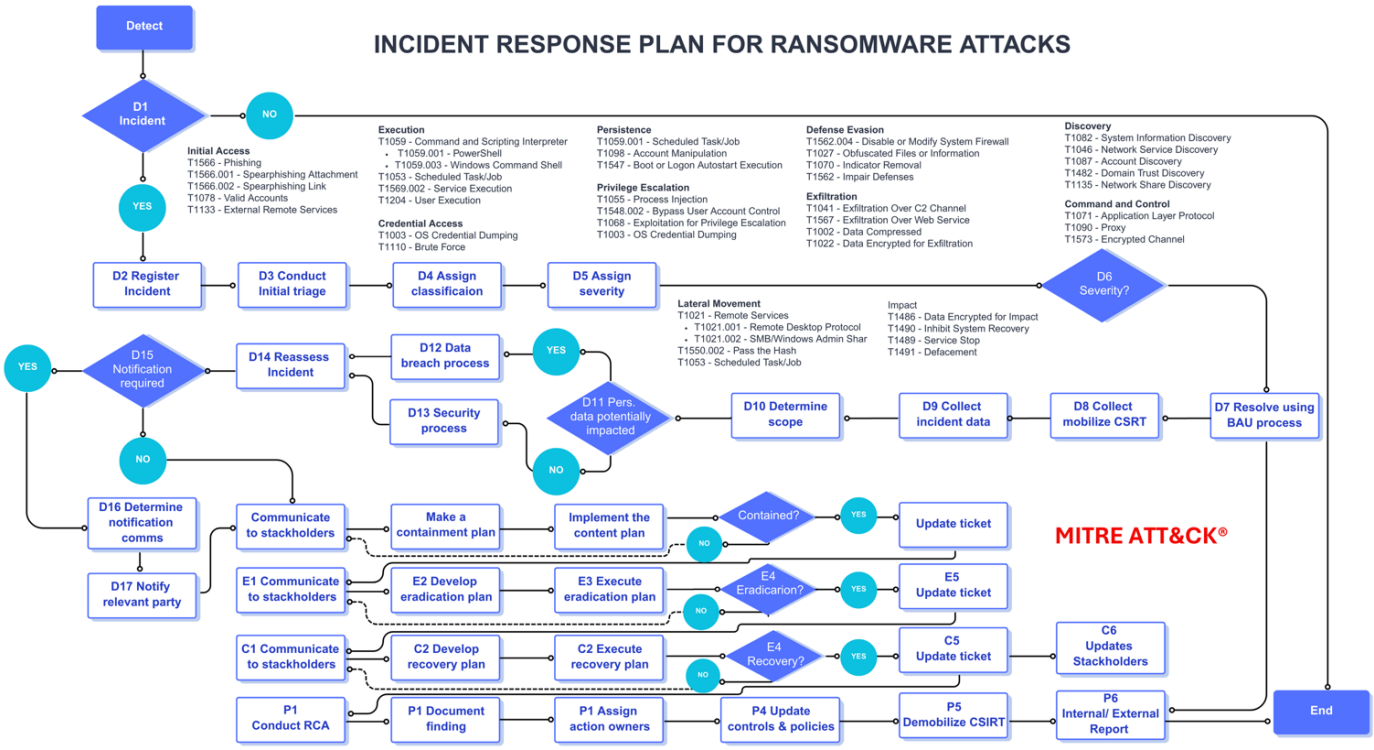


Figure 3: SSAI Incident Response Plan for Ransomware Attacks

SSAI's risk management process aligns closely with the NIST Cybersecurity Framework (CSF) 2.0 by following a structured approach to identifying, analyzing, and prioritizing risks. The initial steps—recognizing threats and vulnerabilities—correspond to the **Identify** function, particularly the **Risk Assessment (ID.RA)** and **Asset Management (ID.AM)** categories. SSAI's evaluation of potential outcomes and impacts aligns with the **Governance (ID.GV)** and **Risk Management Strategy (ID.RM)** categories, ensuring that risks are not only understood but contextualized within the organization's mission and tolerance levels. Prioritization of risks using stakeholder input and historical data further supports the **Identify** function by refining risk understanding and enabling informed decision-making.

The latter stages of SSAI's process—developing, implementing, and monitoring mitigation strategies—span multiple NIST CSF functions. Strategy development aligns with the **Protect (PR)** and **Respond (RS)** functions, particularly in selecting appropriate safeguards and response actions. Implementation and continuous monitoring reflect the **Protective Technology (PR.PT)** and **Security Continuous Monitoring (DE.CM)** categories, ensuring that mitigation efforts are active and effective. SSAI's emphasis on reviewing and adjusting strategies supports the **Respond (RS.IM)** and **Recover (RC.IM)** categories, promoting resilience and continuous improvement. This comprehensive alignment ensures that SSAI's risk management practices are robust, adaptive, and in harmony with industry-recognized cybersecurity standards.

- **(ME) Experience and Qualifications. Describe in detail the experience and qualifications that you will require for Contractor staff who will be performing Category 1 Risk Assessment and Mitigation Services, see Attachment 02, Section 2.3 for minimum qualifications. Include relevant certifications (such as, but not limited to, Certified Information Systems Auditor (CISA), Certified Information Security manager (CISM), and Certified Regulatory and Compliance Professional (CRCP) by FINRA), CISSP, GPEN, GEVA, and any areas of specialization.**

To promote best value and success in our support for the State of Idaho, SSAI will deploy a deliberate selection of specialized, value-add people who leverage proven IT capabilities in order to assess and mitigate risk. Each SSAI expert brings specific specializations and capabilities that increase our agility and responsiveness to the full range of information security requirements. Moreover, our team increases access to high-demand, low-availability subject matter expertise in a competitive marketplace. Finally, we enhance the value of our support by sharing lessons, tools, and staff, whenever beneficial. SSAI has a strong recruiting capability and the ability to retain its staff and ensure they are continuously trained as the cyber landscape evolves.

Security/Technology Senior Analyst: SSAI's Security/Technology Sr. Analyst has more than 5 years of experience with strong technical and security skills. They have contributed to system security by conducting risk assessments, putting security controls in place, and supporting compliance audits, and are also skilled at planning and coordinating technical tasks, working closely with cross-functional teams to ensure everything stays aligned with project goals. In terms of staff management, the Security/Technology Sr. Analyst ensures staff are efficiently managed by providing task direction, offering hands-on technical guidance, and reviewing performance to meet deadlines and quality expectations. They are certified with **CISSP** and **CISA**, validating deep knowledge in information systems auditing and security governance and have hands-on expertise using tools such as Nessus, Splunk, and Qualys to identify vulnerabilities and measure compliance.

Business Process/Risk Management Senior Consultant: SSAI's Senior Consultant has more than 5 years of experience with deep knowledge of frameworks related to business processes and risk management. Their skills are reinforced by their continuously updated certifications, including **CISA**, **CISM**, and the Certified Regulatory and Compliance Professional **(CRCP) – FINRA** certification. To supplement their competitive certifications, they participate in industry trainings, including webinars and courses.

They have participated in companywide process evaluations, performed operational risk assessments along with executing enterprise-wide evaluations, and assisted in formulating risk management strategies. By understanding the broader business context, they are able to prioritize issues through the combination of data analysis, stakeholder input, and industry insight. SSAI's Senior Consultants are experienced in supervising large, cross-functional teams and overseeing the delivery of complex projects.

Project Manager: SSAI's Project Manager has over 5 years of experience with an emphasis in project management and business process enhancement. They have effectively conducted multiple engagements by scoping projects, assigning roles, managing timelines and budgets while maintaining high-execution and high-quality result standards. Additionally, they manage progress to resolve early issues whilst informing stakeholders using high-level reporting that outlines accomplished milestones and impacts delivered. They manage tasks and oversee daily activities, giving equal attention to the overarching strategy and critical paths to ensure no divergence from key objectives. During technical team cross collaborations or while guiding changes to business processes they ensure provision of structure, accountability, and progress momentum to every engagement.

Supporting their ability to apply best practices, manage risk and lead with confidence, recognized project management certifications include **PMP** and **CSM**.

- **(ME) SLAs. Describe your company's SLA's surrounding Category 1 Services. Include response times, responsibilities of both the Contractor and Participating Entity, and any other relevant information surrounding the levels of service.**

SSAI has corporate-level procedures and Service Level Agreements in place that guide our information security frameworks. Our procedures are updated and refined based on compliance with industry and client requirements. Under our SLAs, response, containment, and resolution processes are time-based and tiered. For SEV1 (critical) incidents, SSAI's response commitment is under 15 minutes, containment of the issue within 1 hour, and resolution within 4 hours. For SEV2 (High) incidents, a response must be given in under half an hour, while issue containment must occur within 2 hours and full resolution in 8 hours. For SEV3 (medium) issues, SSAI aims for a 1-hour response time with issue containment within 4 hours and full resolution within a day (24 hours). Finally, for SEV4 (low) incidents, the escalation windows are longer: a 4-hour response time with issue containment taking up to 1 business day; resolution takes up to 3 business days.

In service of these timelines, SSAI adheres to a defined communication plan which varies by the severity tier. For SEV1 incidents, updates are pushed every half hour until the incident is contained and subsequently on an hourly basis until resolution. For SEV2, communications occur once every hour until containment followed by a two-hour update cadence until resolution. SEV3 incidents are managed with an initial four-hour update frequency until containment, then shift to daily updates. In the case of SEV4, communication occurs only as requested or based on completion milestones of tasks set during previous interactions. This method allows SSAI to manage incidents while providing stakeholders with the necessary communication throughout the different phases of the incident lifecycle.

SSAI Science Systems and Applications, Inc.

INCIDENT MANAGEMENT SLA

Severity Level	Description & Business Impact	Response SLA	Contain SLA	Resolution SLA	Communication Frequency
SEV1 (Critical)	Complete system outage or major data breach, significant financial loss, severe reputational damage, legal/compliance violation	< 15 minutes	< 1 hour	< 4 hours	Every 30 mins (until containment), then Hourly (until resolution)
SEV2 (High)	Major service degradation, significant data exposure, moderate financial / reputational impact.	< 30 minutes	< 2 hours	< 8 hours	Every 1 hour (until containment), then Every 2 hours (until resolution)
SEV3 (Medium)	Minor service disruption, localized data integrity issues, potential but non-critical security vulnerability.	< 1 hour	< 4 hours	< 24 hours	Every 4 hours (until containment), then Daily (until resolution)
SEV4 (Low)	Minor security alert, low-impact vulnerability, potential policy violation with no immediate business impact.	< 4 hours	< 1 business day	< 3 business days	As needed (depend upon request or completion)

Figure 4: SSAI Incident Management SLA

- **Value-Added Services. Describe any services related to Category 1 that were not included in the SOW that your company can offer. Prices for any Value-Added Services must be detailed in your response to Attachment 09.**

For Category 1, our Statement of Work (SOW) already encompasses the full scope of services we offer. We believe the comprehensive nature of our core offering provides exceptional value, addressing all key requirements within this category. Therefore, we do not have separate, additional value-added services to detail.

B. **Category 2 – Incident Response Services – Experience and Qualifications**

- **(ME) Category 2 – Offeror's Experience. Describe your company's experience, demonstrating that your company has a minimum of five (5) years of experience providing services similar in scope and size to the Category 2 Incident Response Services required in Attachment 02 Scope of Work. Provide specific examples that illustrate the specific services furnished and the size, composition, etc. of the entities for whom you have provided services that you are using to demonstrate that your experience meets this minimum requirement.**

SSAI has over 45 years of experience preparing for and responding to cybersecurity incidents for our internal assets and external client infrastructures. The following table summarizes SSAI's three most relevant contracts with cybersecurity and information security services.

SSAI's 3 Largest Contracts	Period of Performance	Contract Value	IT Security Services
Sciences Technology and Research Support Services (STARSS III) – NASA Langley Research Center	12/1/2016 – 5/31/2023	$307M	SSAI provided science, research, and technology support services to NASA Langley Research Center's Science Directorate. We managed the Atmospheric Science Data Center which included ingesting, archiving, processing, protecting and distributing data, and providing user support for a wide range of atmospheric science data.
Support for Atmospheres Modeling and Data Assimilation (SAMDA) – NASA Goddard Space Flight Center	3/1/2017 - Present	$298M	SSAI provides comprehensive support for atmospheric sciences, modeling, and data assimilation research conducted by NASA's Earth Science Division. This includes ensuring the security, proper management, and controlled dissemination of satellite data. Accordingly, we are required to implement a robust IT security management plan and maintain compliance with NASA and DoD regulatory obligations.
Hydrosphere, Biosphere and Geophysics Support Services (HBG)	4/1/2020 - Present	$425M	SSAI provides comprehensive support services for NASA's HBG sub-division and the Terrestrial Information Systems Laboratory (TISL). This involves maintaining, enhancing, and operating several Data Centers and its secure websites that archive, distribute, and provide user services for NASA data products.

For our customers, SSAI follows a comprehensive incident response process.

- In the **Preparation** phase, SSAI establishes an Incident Response Policy, forms a dedicated Incident Response Team with defined roles, develops detailed response plans and playbooks, acquires necessary tools and technologies, conducts training and awareness programs, maintains infrastructure documentation, and regularly tests their readiness through exercises.
- During **Identification**, SSAI detects potential incidents using various security tools, system logs, user reports, and external sources, then performs initial triage and analysis to confirm incidents, prioritize them by impact, document findings, and notify relevant stakeholders.
- Once an incident is confirmed, SSAI moves to **Containment** by developing strategies to limit damage, implementing short- and long-term containment measures, preserving evidence, and maintaining communication with involved parties.
- In the **Eradication** phase, SSAI identifies root causes, removes malicious components, remediates vulnerabilities, and verifies threat elimination.
- **Recovery** involves restoring systems from clean backups or rebuilding compromised assets, integrity testing, enhancing monitoring, and gradually resuming normal operations while keeping stakeholders informed.
- Finally, SSAI conducts a **Lessons Learned** review to evaluate the response effectiveness, document the incident comprehensively, assign improvement actions, update policies and training, and ensure proper evidence retention for future reference and compliance.

Figure 5 below outlines our anti-phishing blueprint implemented internally and for various federal and state government clients.

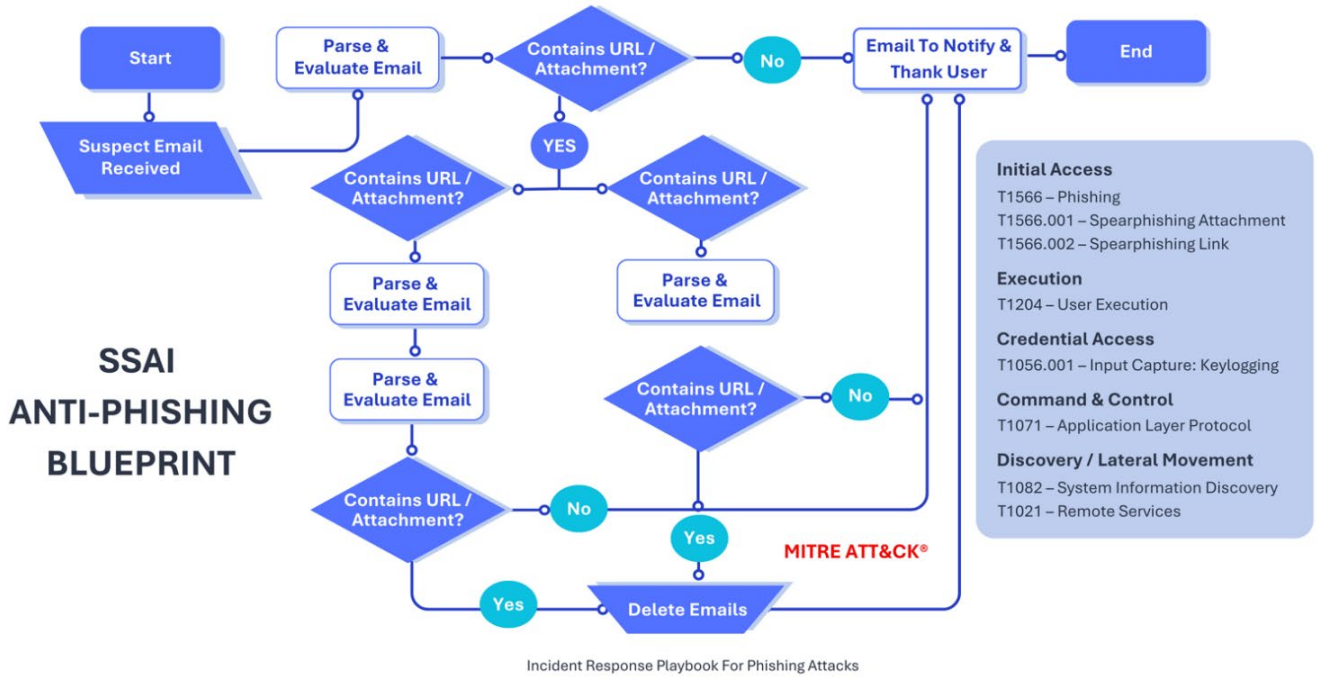


Figure 5: SSAI Anti-Phishing Blueprint

- **(ME) Category 2 Contractor Staff – Experience and Qualifications. Describe in detail the experience and qualifications that you will require for your Contractor staff who will be performing Category 2 Incident Response Services, see Attachment 02, Section 3.9 for minimum qualifications. Include relevant certifications (such as, but not limited to, SANS Certified Incident Handler (GCIH), EC-Council Incident Handler (ECIH) and ENCASE certified) and any areas of specialization.**

SSAI builds its teams by strategically selecting professionals with specialized knowledge in Cybersecurity, Penetration Testing, Forensic Analysis, and risk management. SSAI's personnel are technologists with proven track records of delivering tangible value outcomes under stringent compliance requirements. Every engagement team at SSAI comprises a certified subject matter expert holding professional credentials like CISSP, CCSP, MCT, CEH, CISA, CISM, PMP etc. These experts hold sophisticated skills associated with offensive security testing along with the identification of vulnerabilities and digital forensics which enables simulating attacker strategies through automated and adversarial manual techniques while digitally preserving evidence via legally defensible chain-of-custody methods.

Forensics Incident Investigator: SSAI's Forensics Incident Investigator has over 5 years in the field and holds the GIAC Certified Forensic Analyst and ENCASE Certified Examiner accolades. Table 1 demonstrates SSAI's focus on the identification, collection, examination, and preservation of digital evidence through controlled investigative methods. Their specialization guarantees that evidence management is conducted in such a manner that supports security investigations or legal activities if required.

Business Process/Risk Management Senior Consultant: For more than five years, SSAI's Senior Consultant has been deepening their knowledge about business processes, industry trends, fraud analytics, and risk management practices enabling them to provide value added insights for organizations. They have an uncanny ability to look beyond the immediate problem using data as mediocre inputs combined with historical reference including experience in prescriptive analytics to derive recommendations hinged on technology vis-a-vis cybersecurity enhancement and holistic organizational hardening strategies. They demonstrate highly output focused multi-disciplinary collaborative leadership integrating systems from other fields while ensuring quality control on process outcomes, serving as pre-execution core Engineering Subject Matter Expert.

Project Manager: Our Project Manager has over 5 years of experience managing complex projects, particularly in information security and incident response. They are **PMP (Project Management Professional)** and **Certified ScrumMaster (CSM)** certified. They are experts in project planning, team coordination, task scoping, budget management, and tracking progress. With a project management certification, they bring structure and reliability to every engagement, ensuring that stakeholders are kept informed and that project goals are met efficiently and effectively.

SSAI operates in full alignment with leading security frameworks and standards, including:

- **NIST SP 800-53** for federal information systems security controls.
- **FIPS 140-2** for cryptographic module compliance.
- **AICPA SOC 2 Type II**, covering Security, Availability, Confidentiality, Processing Integrity, and Privacy.
- **FedRAMP-authorized cloud environments**, ensuring standardized security controls across U.S. government infrastructure.

Our personnel also utilize the MITRE ATT&CK® Framework as a foundational model for Threat emulation, Detection gap analysis, and Adversarial behavior mapping. By aligning our assessments and red team operations with MITRE ATT&CK® tactics, techniques, and procedures (TTPs), we help clients understand how real-world threat actors operate, and how to proactively defend against them. SSAI's engagements are guided by industry best practices in cybersecurity and risk governance, and we provide end-to-end services that include:

- **Risk Assessment and Mitigation Planning** based on threat likelihood and impact.
- **Information Security Policy Development and Review**, aligned with compliance mandates.
- **Vulnerability and Threat Assessments**, including internal/external scans, social engineering, and configuration reviews.
- **Incident Response Readiness**, from playbook design to live containment and recovery.
- **Breach Notification and Credit Monitoring Compliance**, including identity theft restoration and reporting support.
- **Secure Data Handling and Storage**, with controls for encryption at rest/in transit and zero-retention protocols.

Equally critical is our strict adherence to regulatory and legal obligations applicable to the client. SSAI personnel ensures full compliance with:

- **State and Federal Privacy Laws** including HIPAA, FERPA, GLBA, and CJIS security policies.
- **Breach Notification Statutes**, such as those governed by state attorneys general and federal regulators
- **Contractor Confidentiality Agreements**, which strictly prohibit the reuse, retention, or unauthorized sharing of client data.
- **Non-Retention Policies** that guarantee the secure destruction of all client data post-engagement, in accordance with NIST SP 800-88.

Our team collaborates seamlessly with client IT teams, legal counsel, procurement offices, and executive leadership to deliver actionable outcomes that are both technically sound and aligned with enterprise objectives. Whether we're advising on cloud migration hardening, evaluating IAM policies for a statewide agency, or managing a post-breach forensic investigation, our clients know they can rely on SSAI for clarity, responsiveness, and results. With this foundation, SSAI is highly confident in the team's ability to meet and exceed the comprehensive security needs of public-sector clients across the United States, helping them manage risk, maintain compliance, and build a more secure digital future.

- **(ME) Category 2 Customer Service Representatives – Qualifications. All call center customer service representatives must have excellent customer service skills and be able to communicate clearly in English. Describe in detail the minimum qualifications and training for customer service representatives to be used in servicing the NASPO ValuePoint Master Agreement.**

The minimum qualifications for our Customer Service staff is defined below:

- Fluent in English (speaking, reading and writing)
- Strong communication and problem-solving skills (1-year or formal training preferred)
- Basic technical knowledge of required computer hardware and software
- One year of experience in customer service or helpdesk support

The training requirements for our Customer Service Representatives are outlined below for new and existing staff:

Module 1: Communication Skills

- Phone etiquette (answering calls professionally, handling difficult callers).
- Email communication (writing clear emails, email etiquette).
- Guided Troubleshooting (active listening, response and instructional protocol)
- Problem Resolution and Escalation

Module 2: Time and Task Management

- Appointment scheduling using digital calendars.
- Prioritizing and delegating IT support tasks.
- Creating and managing project task lists.

Module 3: Project Administration and Coordination

- Meeting notes (effective note-taking, summarizing discussions).
- Project planning and logistics.

Module 4: Document and Records Management

- Managing electronic and hard-copy records and tickets.
- Desktop publishing (using Microsoft Word and Publisher).
- Correspondence management.

Module 5: Technology and Collaboration Tools

- Using Microsoft Teams and applicable client collaboration tools.
- Data entry and database management.
- IT liaison and basic troubleshooting.

Module 6: Information Security and Contract Compliance

- Corporate and client security procedures
- NASPO Master Agreement compliance
- Security risk identification and reporting duties

Our staff will leverage our online training portal for onboarding and refresher training. In addition to the above-mentioned training requirements, SSAI personnel are required to complete:

- Annual refresher training covering applicable skills and responsibilities.
- Ongoing workshops and seminars related to changing client, corporate and industry requirements.
- Performance assessments including client survey ratings, peer reviews and supervisor feedback.
- Annual refresher training covering access to training materials and information security resources.

These requirements ensure that our customer service staff develop and maintain the necessary skills to perform their roles effectively in changing environments.

Our customer service representatives will prioritize articulating themselves in a friendly and universally intelligible manner. They will conduct their speech with empathy, speak slowly and clearly, and resolve customer issues based on our four escalation levels outlined in Table 1 below and covered in Problem Resolution and Escalation Training (Module 1: Communication Skills).

Level	Response Time	Escalation
Level 1: Initial Support	Within 15 minutes	If no resolution or further assistance is needed, escalate to Level 2.
Level 2: Advanced Support	Within 4 hours	If the issue persists or requires specialized expertise, escalate to Level 3.
Level 3: Expert Support	Within 8 hours	If critical business impact or executive attention is required, escalate to Level 4.
Level 4: Executive / Critical Incident	Within 2 hours (after Level 3 escalation)	The highest level of escalation focused on immediate resolution and communication.

- **(ME) SLA's. Describe your company's SLA's surrounding Category 2 Services. Include response times, responsibilities of both the Contractor and Participating Entity and any other relevant information surrounding the levels of service**.

SSAI has established a comprehensive Service Level Agreement (SLA) process to manage incidents according to their severity so that they can be responded to, contained, and resolved within specified time limits. For SEV1 (Critical) incidents, SSAI pledges to respond in under 15 minutes, contain the situation within 1 hour, and resolve it in 4 hours. SEV2 (High) incidents must be responded to within 30 minutes, contained within 2 hours, and resolved within 8 hours. SEV3 (Medium) issues, the SSAI response is within 1 hour, contains within 4 hours, and resolves within 24 hours. SEV4 (Low) incidents have the longest response windows: respond within 4 hours, contain within 1 business day, and resolve within 3 business days.

In addition to these intervals, SSAI also has a formal communications schedule specific to every level of severity. In the case of SEV1 incidents, there are updates provided every 30 minutes while contained and further hourly until resolved. SEV2 has updates every hour while contained and every two hours until resolved. SEV3 has updates every 4 hours while contained, with daily updates until resolved. For SEV4, communication is required, based on request or status of completion. The strategy helps SSAI deal with incidents in an effective way while informing stakeholders along the way.

- **Value-Added Services. Describe any services related to Category 2 that were not included in the SOW that your company can offer. Prices for any Value-Added Services must be detailed in your response to Attachment 09.**

Our approach to Category 2 is to embed maximum value directly into our core offering as outlined in the SOW. We're confident that the services already included provide significant benefits and address all anticipated needs. Consequently, we do not have supplementary value-added services for Category 2 to list separately.

C. **Category 3 – Breach Coach Services – Experience and Qualifications**

- **(ME) Category 3. Offeror's Experience. Describe your company's experience demonstrating that your company has a minimum of five (5) years of experience providing services similar in scope and size to the Category 3 Breach Coach Services required in Attachment 02, Scope of Work. Demonstrate Contractor's well-rounded knowledge of the Breach life cycle from start to finish including, but not limited to, the investigation process, regulatory requirements, and consumer and business notification rules and expectations. Provide specific examples that illustrate the specific services furnished and the size, composition, etc. of the entities for whom you have provided services that you are using to demonstrate that your experience meets this minimum requirement.**
  - N/A
- **(ME) Category 3 Breach Coach – Experience and Qualifications. If a Triggering Event occurs, Participating Entities must be able to contact a Breach Coach, see Attachment 02, Section 4.3 for minimum qualifications who can assist in determining the steps that must be taken to activate services and respond appropriately. Describe in detail the experience and qualifications that you will require for your Breach Response Specialists who will be performing Category 3 Breach Coach Services. Include any relevant certifications and areas of specialization.**
  - N/A
- **(ME) SLA's. Describe your company's SLA's surrounding Category 3 Services. Include response times, responsibilities of both the Contractor and Participating Entity and any other relevant information surrounding the levels of service.**
  - N/A
- **Value-Added Services. Describe any services related to Category 3 that were not included in the SOW that your company can offer. Prices for any Value-Added Services must be detailed in your response to Attachment 09.**
  - N/A

D. Category 4 – Notification and Credit Monitoring Services – Experience and Qualifications

- **(ME) Category 4 – Offeror's Experience. Describe your company's experience demonstrating that your company has a minimum of five (5) years of experience providing services similar in scope and size to the Category 4 Notification and Credit Monitoring Services required in section Attachment 02, Scope of Work. Provide specific examples that illustrate the specific services furnished and the size, composition, etc. of the entities for whom you have provided services that you are using to demonstrate that your experience meets this minimum requirement.**
  - N/A
- **(ME) Category 4 Identity Restoration Personnel – Experience and Qualifications. All identity restoration personnel must be highly trained, have excellent customer service skills, and be able to communicate clearly in English. Describe in detail the minimum experience, qualifications and training you will require for identity restoration representatives servicing the NASPO ValuePoint Master Agreement.**
  - N/A

- **(ME) Category 4 Call Center Customer Service Representatives – Qualifications. All call center customer service representatives must have excellent customer service skills and be able to communicate clearly in English. Describe in detail the minimum qualifications and training for call center customer service representatives to be used in servicing the NASPO ValuePoint Master Agreement.**
  - N/A
- **(ME) SLA's. Describe your company's SLA's surrounding Category 4 Services. Include response times, responsibilities of both the Contractor and Participating Entity, and any other relevant information surrounding the levels of service.**
  - N/A
- **Value-Added Services. Describe any services related to Category 4, including Identity Theft Insurance, that were not included in the SOW that your company can offer. Prices for any Value-Added Services must be detailed in your response to Attachment 09.**
  - N/A

E. (M) Subcontractors.

Offerors must identify whether or not they intend to provide all services directly or through the use of subcontractors. If you do intend to use subcontractors, describe the extent to which you intend to use subcontractors to perform contract requirements, and clearly delineate the specific Category(ies). Offerors must describe the experience and expertise of their proposed Subcontractor(s) and how they meet the minimum requirements of the Category(ies) (AMD 2).

SSAI intends to collaborate closely with Agema Technology (Agema) to supplement labor and technical solutioning for the required cybersecurity and information security services under Categories 1 and 2 of this contract. For all required services, SSAI will maintain management responsibility and accountability. Agema will serve as a key partner and subcontractor, bringing specialized expertise and resources that complement SSAI's capabilities. Through this partnership, SSAI will support both Category 1 – Risk Assessment and Mitigation Services and Category 2 – Incident Response Services by contributing skilled personnel who meet or exceed all minimum qualifications outlined in the RFP. SSAI's team includes certified cybersecurity professionals with experience in government and defense sectors, ensuring they are well-prepared to handle sensitive environments and complex security challenges. By leveraging SSAI's strengths alongside Agema's extensive virtual bench of engineers and established relationships with prime contractors, we will deliver comprehensive, scalable, and responsive cybersecurity solutions. This collaboration allows us to efficiently allocate resources, maintain high standards of service, and ensure continuity and quality across all contract requirements. Together, Agema and SSAI are committed to providing exceptional support tailored to the unique needs of each participating entity.

Agema has a proven track record of successfully providing cybersecurity services as a subcontractor to major prime contractors such as Raytheon, Leidos, and Oracle. Through these partnerships, they have supported high-profile clients including the Jet Propulsion Laboratory (JPL), the US Navy, and the US Army, demonstrating their ability to manage complex projects across both Category 1 – Risk Assessment and Mitigation Services and Category 2 – Incident Response Services.

Category 1: Agema's work under the Raytheon subcontract at Jet Propulsion Laboratory (JPL) exemplifies their expertise in risk assessment and mitigation within highly secure environments. Over an 11-year engagement valued at over $10 million, Agema provided Top Secret/SCI cleared engineers who conducted vulnerability

assessments, including evaluations of proprietary systems, privacy impact analyses, and internal control reviews critical to data protection for intelligence agencies using satellite and ISR platforms. They recommended improvements to information security policies and consulted third-party contract terms such as cloud providers, ensuring alignment with Department of Defense standards and certifications. Similarly, under Oracle's Army Enterprise Systems Integration Program (AESIP), Agema delivered comprehensive IAM services securing access to Army ERP systems handling billions in transactions annually. Their engineers implemented risk assessments and mitigation strategies consistent with mainstream information security frameworks, performed compliance assessments related to federal regulations, prioritized threats with cost evaluation, and enhanced security policies. These efforts were supported by relevant certifications including CISSP, CISA, and Oracle IAM credentials. Additionally, on the Leidos Navy NGEN-R SMIT contract, Agema contributed cybersecurity and network engineering support aligned with DoD Cyber Exchange certification requirements, performing ongoing risk assessments and compliance audits to protect critical Navy networks.

Category 2: Agema maintains a robust virtual bench of several hundred cybersecurity engineers, allowing them to quickly scale and provide personnel with the exact certifications and skills needed for each engagement. These certifications include industry-recognized credentials such as SANS Certified Incident Handler (GCIH), EC-Council Incident Handler (ECIH), ENCASE certification, CISSP, and Security+, among others. This flexibility ensures they can meet or exceed all minimum qualifications outlined in the RFP and Attachment 02.

Agema has demonstrated robust incident response capabilities across its prime contractor engagements. For Oracle's Army contract, they responded promptly to incident requests, maintained active communication channels, and managed event scope determination through log file analysis and intrusion detection systems. While specific forensic activities are not detailed for this contract, their role included coordination with law enforcement when appropriate and ensuring secure communication of incident information. On the Leidos Navy NGEN-R SMIT contract, Agema's incident response expertise is more fully developed: they executed evidence collection following strict chain-of-custody protocols, utilized forensic software to preserve system backups, and conducted legally admissible forensic analyses to identify culprits, causes, and consequences of incidents. They provided both short-term containments to limit damage while preserving evidence and long-term containment allowing affected systems to remain operational during eradication phases. Agema personnel removed malicious code, restored systems through recovery processes involving testing and validation, and produced incremental and final reports detailing findings, compromised data, trends, and post-incident recommendations. Furthermore, they offered 24x7 customer support via toll-free numbers for incident-related inquiries. Across these efforts, Agema integrated into large-scale teams, filling leadership and specialized technical roles, leveraging a virtual bench of certified cybersecurity engineers to rapidly meet client needs.

SSAI has carefully selected Agema as its primary subcontractor based not only on their technical qualifications but also on their proven experience working within government and defense environments, where security, reliability, and responsiveness are paramount. By leveraging Agema and our local network of trusted partners, we are confident in our ability to deliver high-quality, compliant, and timely cybersecurity services tailored to the specific needs of each contract under this agreement. Throughout every project phase, SSAI will maintain close oversight and coordination to ensure seamless integration between subcontractor staff and the participating entities, fostering clear communication, accountability, and exceptional service delivery.

- **Subcontractors are only permitted with written approval from the Lead State or Participating Entity and must meet or exceed all minimum requirements in this RFP. Approval by the Lead State of the Contractor's request to subcontract or acceptance of or payment for subcontracted work by a Participating Entity shall not in any way relieve the Contractor of any responsibility under the Master Agreement and Participating Entity's Participating Addendum. The Contractor shall be and remain liable for all damages to a Participating Entity caused by negligent performance or non-performance of work under the Master Agreement and Participating Entity's Participating Addendum by the Contractor's subcontractor.**

SSAI acknowledges its ultimate responsibility for all work performed by approved subcontractors, ensuring we obtain proper client approval and they meet all requirements. SSAI remains liable for their performance under the Master Agreement and Participating Entity's Participating Addendum.

- **Subcontractor(s) must maintain the same types and levels of insurance as that required of the Contractor under the Master Agreement; unless the Contractor provides proof to the Lead State's satisfaction that the subcontractor(s) are fully covered under the Contractor's insurance, or, except as otherwise authorized by the Lead State.**

SSAI acknowledges that its subcontractors maintain the same insurance coverage as required of SSAI under the Master Agreement, unless SSAI provides satisfactory proof of subcontractor coverage under its own insurance or as otherwise authorized by the Lead State.

F. **(ME) Offeror's Experience with Statewide or Large Consortium Contracts.**

- **Describe in detail your company's experience with statewide or large consortium contracts similar to the services sought in Attachment 02, Scope of Work.**

SSAI has nearly 50 years of experience supporting NASA with contract arrangements that include task orders independently supporting various NASA divisions and a consortium of federal agencies like NOAA, USDA, and various Department of Defense (DoD) and U.S Intelligence Community (IC) branches. We have a proven track record of executing information security services as part of our satellite data management and science support services contracts across diverse government missions. Table 2 below provides examples of other active consortium vehicles we have in the industry, offering quick access to our services under streamlined contract terms and conditions:

SSAI's Consortium Contract Vehicles	Contract Number	Scope
C5 (Command, Control, Communications, and Computer Technologies)	HQ00341990001	Cybersecurity, C4ISR, AI/ML, autonomy, data analysis capabilities

SSAI's Consortium Contract Vehicles	Contract Number	Scope
NSTIC (Naval Surface Technology & Innovation Consortium)	N001781990005	Naval warfare systems, remote sensing, atmospheric modeling, AI applications, communications
MSTIC (Maritime Sustainment Technology and Innovation Consortium)	N644982190001	Naval sustainment, sensing, Oceanography, remote sensing, environmental modeling, and manufacturing
RRPV (Rapid Response Partnership Vehicle)	TBD	Biomedical R&D, NIH AI research, data analysis, health security, AI analytics

- **Provide the approximate dollar value of the business's three (3) largest contracts in the last five (5) years, under which the business provided services identical or very similar to those required by this RFP.**

SSAI brings extensive IT Security experience demonstrated by our role as the prime contractor for three NASA contracts detailed in Table 3 below:

SSAI's 3 Largest Contracts	Period of Performance	Contract Value	IT Security Services
Sciences Technology and Research Support Services (STARSS III) – NASA Langley Research Center	12/1/2016 – 5/31/2023	$307M	SSAI provided science, research, and technology support services to NASA Langley Research Center's Science Directorate. We managed the Atmospheric Science Data Center which included ingesting, archiving, processing, protecting and distributing data, and providing user support for a wide range of atmospheric science data.
Support for Atmospheres Modeling and Data Assimilation (SAMDA) – NASA Goddard Space Flight Center	3/1/2017 - Present	$298M	SSAI provides comprehensive support for atmospheric sciences, modeling, and data assimilation research conducted by NASA's Earth Science Division. This includes ensuring the security, proper management, and controlled dissemination of satellite data. Accordingly, we are required to implement a robust IT security management plan and maintain compliance with NASA and DoD regulatory obligations.
Hydrosphere, Biosphere and Geophysics Support Services (HBG)	4/1/2020 - Present	$425M	SSAI provides comprehensive support services for NASA's HBG sub-division and the Terrestrial Information Systems Laboratory (TISL). This involves maintaining, enhancing, and operating several Data Centers and its secure websites that archive, distribute, and provide user services for NASA data products.

In addition to the above-mentioned NASA contracts, SSAI was recently awarded a Cybersecurity Services contract with the Los Angeles Unified School District (LAUSD), where we support the Office of the Chief Information Officer (OCIO) and other LAUSD divisions with various IT Security services.

- **Describe how you intend to market your Master Agreement and encourage participation among potential Participating Entities, including state governments.**

At SSAI, we are dedicated to making it easy and valuable for potential Participating Entities–including state governments–to join our Master Agreement. We focus on clearly communicating how the agreement simplifies procurement by offering pre-negotiated terms, competitive pricing, and strong cybersecurity protections that align with trusted industry standards like NIST CSF 2.0 and the MITRE ATT&CK® framework. By sharing these benefits, we show how participation can save time, reduce administrative headaches, and strengthen security. Our outreach is tailored to meet the unique needs of public sector organizations. We provide customized presentations, webinars, and easy-to-understand materials that address common challenges and demonstrate how we deliver on the promises outlined in the RFP or Statement of Work. We also lean on our existing relationships with government agencies and other associations to build trust and spread the word.

To make joining simple, we offer clear guidance, onboarding support, and dedicated contacts who are ready to help every step of the way. We are mindful about protecting proprietary information, so initial communications stay high-level, with more detailed processes shared only when appropriate and under confidentiality agreements. Moreover, SSAI's incident response process is flexible, allowing us to quickly escalate support based on the severity of any situation, always aligned with what the client requires. We bring our cybersecurity approach to life through real-world examples like ransomware and phishing attacks, mapped to the MITRE ATT&CK® framework, along with clear visuals that help stakeholders understand how we protect their networks. Behind this effort is a skilled, multi-disciplinary team—from Incident Response Leads and Threat Intelligence Analysts to Security Architects and Training Specialists—all working together seamlessly to keep clients safe. Finally, we believe in ongoing communication and feedback. We stay engaged with our partners to continuously improve and adapt, building long-term relationships that encourage broad participation in the Master Agreement. At SSAI, our goal is to create partnerships that deliver real value, peace of mind, and strong security for every entity we serve.

- **Describe features of the dedicated website you will be setting up for this Master Agreement, including, as applicable, customized price lists for each Participating Entity, staff contact information, and online ordering capabilities.**

All Participating Entities will have access to a website built on strong UX (User Experience) principles, accessibility, and transparency. The Landing Page will feature customized portals for each vendor. Within the portals, all services will have clear, easily accessible, and customized pricing. Furthermore, each custom portal will also include safe online ordering features for approved services and goods, enabling the Entity to monitor their service requests and access detailed historical data. The Staff page, which is prominent on the landing page, is designed to provide the user with quick access to the right expert and enable seamless coordination and support. Dedicated account managers, incident response leads, and technical support specialists are among the key SSAI staff contact details that will be clearly displayed. To ensure Participating Entities understand and adopt our Master Agreement, the website will contain interactive educational content with clear calls to action. All website features, content, and documentation provided by SSAI will be developed and maintained to meet or exceed Section 508 accessibility standards, ensuring equitable access and usability for all individuals.

- **Describe the staff and other resources that will be allocated to your Master Agreement and the training you will provide to staff to ensure their familiarity with Master Agreement terms and pricing and their compliance therewith.**

Our SSAI staff includes a diverse mix of technical, management and administrative, ranging from early-career specialists to seasoned experts with skills and credentials tailored to their specific roles. Some of our personnel possess Top Secret/SCI clearances, enabling us to effectively support sensitive government missions. In addition to technical and administrative experts, we assign skilled project and program managers who ensure seamless coordination, timely delivery, and adherence to contract requirements. We also maintain a robust virtual bench of incident response specialists ready to rapidly address any cybersecurity incidents. To ensure that all team members are fully familiar with the Master Agreement terms, pricing, and compliance obligations, SSAI provides comprehensive training upon assignment to this contract and refresher training that is accessible online and completed annually. Our Information Security and Contract Compliance training (Module 6) covers the scope of work, performance expectations, confidentiality requirements, and detailed guidance on approved hourly rates and billing procedures to guarantee accurate invoicing consistent with the contract's pricing structure. Recognizing that prime contractor flow-downs often impose additional requirements, we emphasize awareness and understanding of these provisions so our staff can meet or exceed client expectations. We prioritize ongoing professional development and certification maintenance to keep our workforce current with evolving cybersecurity standards and best practices. Our project management team conducts regular reviews of work products, timesheets, and deliverables to verify full compliance with contractual terms and pricing policies. Open communication channels between leadership and staff foster prompt resolution of questions or concerns related to the agreement. All training activities and compliance checks are thoroughly documented as part of SSAI's commitment to quality assurance and contract integrity. SSAI's combination of experienced, certified professionals and a strong focus on training and compliance ensures–along with our partnership with Agema–that our team will deliver exceptional cybersecurity services while strictly adhering to the Master Agreement's terms and pricing. Our proven track record supporting large federal clients demonstrates our ability to meet technical and administrative requirements.

- **Describe how you intend to encourage adoption and usage of your Master Agreement by Participating and Purchasing Entities.**

We will encourage adoption and usage of our Master Agreement by Participating and Purchasing Entities by removing all forms of friction that deter adoption and usage. First, we will ensure that our staff are trained to educate anyone (in the simplest terms), on specifics regarding the agreement. Second, we will develop an interactive content database (analogous to a Wiki), that allows Participating and Purchasing Entities to ask questions about the agreement and quickly obtain an answer. Third, our website will provide an actionable overview of the agreement itself with clear calls to action based on the users' needs.

- **Describe your approach to negotiation of Participating Addenda. Describe the extent to which you will provide Participating Entities flexibility in incorporating entity-specific language into their Participating Addenda. (*e.g.*, Do you require entities to provide statutory citations for their entity-specific language? Are you able to devote resources to simultaneous negotiation of multiple Participating Addenda?)**

SSAI, partnered with Agema Technology, brings extensive experience and proven capabilities in supporting large-scale government contracts and complex IT services, which uniquely positions us to effectively manage the negotiation of Participating Addenda. We understand that each Participating Entity has distinct statutory and operational requirements, and we approach these negotiations with a collaborative mindset. From the outset, we work closely with entities to fully understand their specific needs and encourage them to provide statutory

citations or references for any entity-specific language they wish to include. This practice helps our legal and contracting teams efficiently review and incorporate those provisions while ensuring compliance and mutual understanding. Leveraging SSAI's leadership and Agema's strong support—drawing on Agema's significant subcontracting experience such as cybersecurity services at Jet Propulsion Laboratory under Raytheon, Identity and Access Management engineering for the Army through Oracle, and network security support for the Navy via Leidos—we have developed robust internal processes and dedicated resources capable of managing multiple Participating Addenda negotiations simultaneously. We utilize standardized Participating Addenda templates aligned with the Master Agreement as a foundation, designed to be flexible enough to accommodate the unique language and requirements of each Participating Entity. Throughout the negotiation process, we emphasize thorough documentation and version control to keep every change transparent and traceable, minimizing misunderstandings, and supporting audit readiness. Together, SSAI and Agema balance consistency with adaptability—respecting the framework of the Master Agreement while empowering Participating Entities to include the language necessary for their compliance and operational success. By requesting statutory citations, dedicating skilled teams to manage concurrent negotiations, and fostering open, responsive collaboration, we strive to make the Participating Addenda process efficient, effective, and tailored to meet the diverse needs of all entities involved

- **Describe your ability to provide products and services immediately upon execution of a Master Agreement and Participating Addenda.**

At SSAI, we understand that once a Master Agreement and Participating Addenda are executed, our clients need products and services delivered without delay. That is why we have designed our operations to be ready to act immediately. As part of this plan, we collaborate closely with Agema Technology, whose experienced cybersecurity professionals and technical experts are prepared to mobilize quickly alongside our team. Together, we maintain a carefully managed inventory of key products and leverage strong partnerships with trusted suppliers to ensure rapid sourcing and delivery. Our combined teams work together with clients from day one, coordinating logistics, providing clear communication, and addressing any challenges promptly. With SSAI and Agema working in partnership, you can be confident that we're fully equipped and committed to meeting your needs swiftly and seamlessly, supporting your goals every step of the way.

- **Describe how you will ensure summary and detailed sales information is promptly, completely, and accurately reported to you by your dealers, partners, and resellers for aggregation and reporting to NASPO ValuePoint in compliance with the terms of your Master Agreement.**

At SSAI, we understand how important it is to have timely, complete, and accurate sales information from our dealers, partners, and resellers so that we can meet our commitments to NASPO ValuePoint under the Master Agreement. To make this happen, we focus on clear and open communication. Right from the start, we share straightforward reporting guidelines and deadlines, so everyone knows what is expected. We provide easy-to-use reporting tools and templates to simplify the process, and we're always available to offer support or answer questions along the way. We also send friendly reminders before deadlines and follow up as needed to keep things on track. To ensure accuracy, we regularly review the data submitted and work collaboratively with our partners to resolve any discrepancies quickly. By building strong relationships and maintaining transparent communication, we create a partnership where everyone feels supported and confident in meeting their reporting responsibilities, helping us all succeed together.

G. **(ME) Customer Service**

- **Identify your customer service hours of operation and when key account staff are available.**

Our standard customer service hours of operation are Monday through Friday from 8:00 AM MT to 5:00 PM MT, excluding federal holidays. Additionally, dedicated key account staff are available during these hours, with provisions for off-hours support and incident response as defined within our SLA.

- **Describe how you handle problem identification and resolution. Describe how you respond to and resolve customer complaints and service issues.**

SSAI has a structured approach to problem identification and resolution through proactive anomaly response and quality management processes. Team SSAI engages in proactive observation by analyzing historical data to detect patterns or anomalies that may indicate emerging issues, allowing preventive measures before disruptions occur. Upon detecting anomalies or incidents, security specialists follow a defined playbook to respond promptly. If discrepancies are found during project execution, they issue Deficiency Reports and select corrective actions, including stopping work (if necessary) until the issue is resolved. This approach emphasizes transparency, collaboration, clear communication, and continuous monitoring to ensure deliverables meet requirements and maintain high performance throughout the project lifecycle.

- **Describe how you will assess customer satisfaction.**

To assess customer satisfaction, Team SSAI will gather direct feedback through surveys, service call resolution rates, and customer satisfaction ratings. They will monitor key metrics such as timely completion of tasks, quality of deliverables, responsiveness to client needs, and overall service effectiveness. Our surveys prioritize the user experience, are intuitive, and are used to improve customer experience. Additionally, ongoing communication with customers and regular reviews will help identify areas for improvement, ensuring that customer expectations are met or exceeded throughout the contract period. SSAI will also consider implementing any established performance evaluation systems based on the customer's preference.

H. **(ME) Offeror must describe how they meet AICPA SOC 2 compliant covering all 5 functional areas (Security, Availability, Processing Integrity, Confidentiality, and Privacy), or a third-party assessment based on current revision of NIST 800-53 Moderate controls conducted with in the last two years, or FedRAMP authorization, or GovRAMP authorization , or equivalent. Offerors must provide documentation of their security practices. Offerors who fail to adequately demonstrate their security standards may be deemed non-responsive. (AMD 1)**

SSAI is ISO 9001:2015 certified. We will leverage our ISO certification by applying the standardized quality management principles it embodies to ensure consistent, reliable, and high-quality service delivery for Idaho. This certification supports our commitment to continuous improvement, process standardization, and customer satisfaction, enabling us to maintain rigorous quality controls across all project activities. By integrating ISO-based processes with industry best practices, Team SSAI enhances operational efficiency, reduces risks, and fosters a culture of excellence that aligns with Idaho's expectations for dependable and effective cybersecurity and information security services.

To ensure security, availability, processing integrity, confidentiality, and privacy, Team SSAI will employ a comprehensive approach that includes continual system patching and upgrades, adherence to established cybersecurity frameworks such as NIST Risk Management Framework (RMF), FISMA, FedRAMP, and government directives, and implementation of robust security controls and documentation.

We will conduct regular vulnerability scans and remediation, manage Plans of Action and Milestones (POAM), customize our IT/Cloud Security Plans, and perform Certification and Accreditation processes to maintain compliance and authorization to operate. We will further implement customized strategies based on existing priorities, automated monitoring tools, incident response playbooks, and strict access management practices to protect sensitive data and ensure operational continuity while maintaining regulatory compliance and safeguarding privacy throughout the contract lifecycle.

SSAI Security Standards (Condensed for Proposal Purposes)

SSAI maintains a comprehensive cybersecurity program designed to protect sensitive government and corporate data while enabling agile, compliant operations. This brief summarizes our current security posture, governance structure, and key controls relevant to contract performance.

1. Security Governance & Compliance

- Alignment with NIST SP 800-171 and ongoing pursuit of CMMC 2.0 Level 2 certification through a dedicated PreVeil enclave (90 of 110 practices satisfied).
- ISO 9001:2015–certified quality system with an active roadmap to achieve AS9100 for aerospace quality.
- Updated corporate cybersecurity policies, including an Incident Response Plan (IRP) in final review, and a System Security Plan (SSP) in development.

2. Identity & Access Management

- Enterprise identity is consolidated on Microsoft Entra ID.
- Multi-factor authentication enforced for 100 % of user accounts; passkey authentication with Microsoft Authenticator and Security Keys is in phased rollout.
- Zero-trust Conditional Access policies restrict access via devices' health, location, and risk signals.

3. Endpoint Security

- SentinelOne XDR delivers real-time protection, behavioral AI detection, automated remediation, and forensic rollback for all Windows, macOS, Linux endpoints and Servers.

4. Network Security & Monitoring

- Elastic SIEM; all system, application, and security logs are centralized for correlation, alerting, dashboards, and threat hunting.
- Corelight AP200 sensor with Suricata and Zeek provides deep-packet network telemetry and protocol analytics.
- Barracuda CloudGen Proxy and Email Gateway secure web traffic and email, blocking spam, phishing, and malware.

5. Threat Detection & Response

- 24×7 monitoring via Elastic SIEM with tailored detection rules (e.g., Entra sign-in anomalies, non-approved-country logins, etc.).
- Playbooks for critical events include an immediate containment path and executive notification.

6. Vulnerability & Patch Management

- Automox automates operating-system and third-party patching across on-prem and remote assets, with policy-based enforcement windows.
- Planned quarterly internal and external vulnerability scans; annual penetration testing supported by third-party assessors.

7. Data Security & Access Control

- Box is our authoritative cloud content platform with Entra ID SSO, granular permissions and DLP rules.

8. User Education & Awareness

- Mandatory cybersecurity onboarding training plus monthly security e-blasts and live awareness sessions (e.g., recent bulletin on AI-generated scams).

9. Incident Response & Reporting

- IRP defines roles, severity ratings, containment steps, and communication paths; tabletop exercises conducted bi-annually.
- Elastic SIEM and SentinelOne provide integrated incident tickets; after-action reports feed continuous improvement cycles.

10. Contact & Management Commitment

SSAI's executive leadership prioritizes continuous security investment and compliance. For additional information regarding our security practices and standards, our Chief Technology Officer, Mr. Ray Baldon, is ready to field your inquiries at ray.baldon@ssaihq.com.

I. Describe what, if any, artificial intelligence technologies you will be using in your performance of a Master Agreement resulting from this RFP and how and for what purposes such technologies would be used. Describe any safeguards, protocols, and/or interpretive reviews that have been or will be applied to the use of AI solutions.

The artificial intelligence technologies we will employ in a Master Agreement resulting from this RFP are our internal AI via the secured Box platform. We centrally use our internal AI stack in service of internal operations such as mining our performance database, visibility of our databases, and sourcing facts. Our safeguards, protocols, and interpretative reviews are tied to three values that include checklists to check the veracity of output. Second, we have a zero-tolerance policy of never using external AI tools (e.g., ChatGPT) to review or handle customer data.

VII. ACKNOWLEDGEMENTS AND CERTIFICATIONS

By signing below and submitting a response to this RFP, Offeror acknowledges and certifies the following:

A. Debarment. (Check one of the below.)

☒Neither Offeror nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in public procurement or contracting by any governmental department or agency.

☐Offeror cannot certify the statement above, and Offeror will affix a written explanation to this attachment for review by the Lead State. If after reviewing Offeror's written explanation the Lead State determines it is not in the best interest of the Lead State, Participating Entities, or Purchasing Entities to award Offeror a Master Agreement, the Lead State may reject Offeror's proposal.

B. Non-collusion.

1. This proposal has been developed independently by Offeror and has been submitted without collusion and without any agreement, understanding, or planned common course of action with any other Offeror or supplier of Deliverables in a manner designed to limit fair and open competition.
2. The contents of this proposal have not been communicated by Offeror or its employees or agents to any person not an employee or agent of Offeror and will not be communicated to any such persons prior to the RFP Close Date.

C. Data Disclosure to Foreign Governments and Prohibited Technology. (Check one of the below.)

☒Offeror is not an entity subject to laws, rules, or policies potentially requiring disclosure of, or provision of access to, customer data to foreign governments or entities controlled by foreign governments, and Offeror's offerings do not contain, include, or utilize components or services supplied by any entity subject to the same. Offeror's offerings also do not contain, include, or utilize covered technology prohibited under Section 889 of the National Defense Authorization Act, as amended.

☐Offeror cannot certify all statements above, and Offeror will affix a written explanation to this attachment for review by the Lead State. If after reviewing Offeror's written explanation the Lead State determines it is not in the best interest of the Lead State, Participating Entities, or Purchasing Entities to award Offeror a Master Agreement, the Lead State may reject Offeror's proposal.

D. Conflicts of Interest. (Check one of the below.)

☒Offeror represents that none of its officers or employees are officers or employees of the Lead State and that none of its officers or employees have a conflict of interest as defined by the laws, rules, or policies of the Lead State.

☐Offeror cannot certify the statement above, and Offeror will affix a written explanation to this attachment for review by the Lead State. If after reviewing Offeror's written explanation the Lead State determines it is not in the best interest of the Lead State, Participating Entities, or

Purchasing Entities to award Offeror a Master Agreement, the Lead State may reject Offeror's proposal.

E. **Required Insurance.** Offeror agrees to acquire insurance from an insurance carrier or carriers licensed to conduct business in each Participating Entity's state at the levels prescribed in Attachment 04, Sample Master Agreement. Offeror understands that this requirement is mandatory and will not be negotiated by the Lead State.

F. **NASPO ValuePoint Administrative Fee.** Offeror agrees to pay a 0.25% administrative fee and submit summary and detailed sales reports to NASPO ValuePoint in accordance with Attachment 04, Sample Master Agreement. All costs proposed by Offeror must be inclusive of the NASPO ValuePoint administrative fee. Offeror understands that the requirements in this section are mandatory and will not be negotiated by the Lead State.

G. **Marketing Plan.** If awarded a Master Agreement resulting from this RFP, within 30 days of execution of the Master Agreement, Offeror will meet with NASPO ValuePoint marketing personnel to review and track progress on the marketing plan described by Offeror.

H. **Confidential, Proprietary, or Protected Information.** As set forth in Attachment 01, RFP Terms and Conditions, if Offeror is claiming any portion of its proposal as confidential, proprietary, or protected, Offeror must complete the required sections of Attachment 11, Claim of Trade Secrets and Non-Public Information, and submit with Offeror's proposal a redacted copy of Offeror's proposal, which must be clearly marked as such. Offeror may not mark pricing or Offeror's entire proposal as confidential, proprietary, or protected. Submission of a Claim of Trade Secrets and Non-Public Information does not guarantee that information claimed by Offeror as confidential, proprietary, or protected will not be subject to disclosure in accordance with applicable public information laws, rules, and policies. If Offeror fails to submit a redacted copy of Offeror's proposal, or fails to claim information as confidential, proprietary, or protected in compliance with this RFP, Offeror releases the Lead State, NASPO, NASPO members, and entities represented on the Multistate Sourcing Team from any obligation to keep the information confidential and waives all claims of liability arising from disclosure of the information.

I. **Cancellation and Transfer.** Offeror understands and agrees that the Lead State may, as set forth in Attachment 01, RFP Terms and Conditions, cancel this RFP or transfer this RFP to a new Lead State if the Lead State determines that such transfer is in the best interest of the Lead State and potential Participating Entities and Purchasing Entities.

J. **Conditional Awards.** Offeror understands that awards and execution of a Master Agreement are conditional as set forth in Attachment 01, RFP Terms and Conditions, and Offeror agrees to hold the Lead State and NASPO harmless and release the Lead State and NASPO from any liability for damages arising from non-award or non-execution of a contract.

K. **Understanding of the RFP.** Offeror has read the RFP in its entirety and understands and agrees to comply with all requirements set forth therein. Any conflicts in the materials composing the RFP and any issues relating to the content of the RFP, including instructions, requirements, or specifications Offeror believes to be ambiguous, unduly restrictive, erroneous, anticompetitive, or

unlawful, have been brought to the attention of the Lead State using the process described in the RFP for asking questions or, if applicable, by filing a protest. In accordance with Attachment 01, RFP Terms and Conditions, Offeror acknowledges and understands that any protest, claim, dispute, or action based upon a conflict or issue described herein must be filed no later than the RFP Close Date, and Offeror waives the right to file any protest, claim, dispute, or action based upon a conflict or issue described herein if not filed by the RFP Close Date.

L. **IPRO Cost Submission.** When submitting your response through IPRO, you must enter your Cost in IPRO as "$0.01". If you do not enter a price in the "Per Unit Estimate" IPRO/LUMA will enter your response as a NO BID. You must also enter your proposed costs for services as instructed in Attachment 9 - Cost Proposal. (AMD 2)

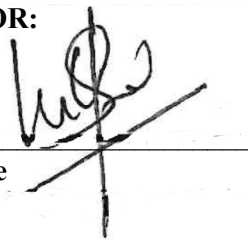
Signature

The undersigned is one of the following:

1. The Offeror, if Offeror is an individual;
2. A partner in the company, if Offeror is a partnership; or
3. An officer or employee of the responding corporation having authority to sign on its behalf, if Offeror is a corporation.

By signing below, the undersigned warrants that the representations made and the information provided in Offeror's proposal are true, correct, and reliable for purposes of evaluation for a potential contract award. The submission of inaccurate or misleading information may be grounds for disqualification from contract award and may subject the undersigned, Offeror, or both to suspension or debarment proceedings, as well as other remedies available to the Lead State by law, including termination of any Master Agreement awarded to Offeror.

OFFEROR:



Signature

6/26/2025
Date

Dr. Shilpa Bahethi
Printed Name

CEO, Science Systems and Applications, Inc.
Title

Shilpa.Bahethi@ssaihq.com
Email Address

301-867-2000
Phone Number