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: Assurit Consulting Group, LLC
B. Primary Business Address: 11325 Random Hills Road Suite 360 Fairfax, VA 22030
C. Federal Tax Identification Number: 46-2137637
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. Company Website. www.assurit.com

B. Company History. Assurit Consulting Group, LLC (Assurit) was founded on February 21, 2013, with a singular mission to protect critical data and information systems against emerging threats. Since our founding, we have maintained our focus exclusively on cybersecurity, delivering specialized expertise to government agencies and commercial clients across the United States. This focused approach has enabled us to develop in-depth expertise in our core competencies: risk assessment, incident response, and security governance. Since 2013, Assurit has expanded its service offerings to encompass the full spectrum of cybersecurity needs. Our company has no material acquisitions or mergers in its history.

C. Company Size. Assurit currently has 25+ employees across the United States.

D. Ownership Structure. Assurit is a privately held limited liability company with a single owner, Sunny Tuteja, who serves as CEO and President.

E. **Litigation.** Assurit has no claims of non-performance or breach from customers and no pending litigation matters or criminal convictions in the past 5 years for either the company or its principals.

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.*

Assurit Contract Manager

Assurit designates David Wellington as our Contract Manager and the single point of contact for the NASPO ValuePoint Master Agreement. Mr. Wellington brings more than a decade of successful program and contract management experience across both public and private sector engagements. As Assurit's Director of Programs, Mr. Wellington oversees and supports the company's portfolio of government contract vehicles, including the GSA Multiple Award Schedule (MAS), GSA 8(a) STARS III, FAA eFAST, and Maryland CATS+.

He leads all aspects of vehicle management including onboarding, compliance, modifications, and ongoing reporting. Mr. Wellington is also responsible for managing the entire lifecycle of proposals and task orders issued under these vehicles, coordinating internal technical and pricing strategies, resource alignment, and submission quality assurance.

Under his leadership, Assurit has continued to deliver high-quality cybersecurity services to a broad range of federal and state government clients. Mr. Wellington is known for his ability to build trusted client relationships, manage complex, concurrent programs, and ensure seamless contract execution. His experience in project governance, financial oversight, and risk mitigation has made him a vital part of Assurit's strategic growth.

Mr. Wellington is available during standard business hours and is committed to proactive and responsive communication with all NASPO stakeholders.

Point of Contact Information:

Name: David Wellington
Email: david.wellington@assurit.com
Phone: (703) 225-3305
Work Hours: Monday-Friday, 9:00 AM to 5:00 PM Eastern Time

Resume

David Wellington

Director of Programs, Assurit
September 2023 – Present | Fairfax, Virginia

- Leads program and contract management for Assurit's major government contract vehicles, including GSA MAS, 8(a) STARS III, FAA eFAST, and Maryland CATS+.
- Acts as the Contract Manager for Assurit's Master Agreements, serving as the primary point of contact for all contract-related matters.

- Oversees onboarding, compliance, modifications, reporting, and performance tracking across vehicles.
- Coordinates proposal responses, task order execution, and supports strategic business development initiatives.
- Resolves client billing and reporting issues efficiently, ensuring high satisfaction and contract compliance.

Finish Line

Application Development Manager
May 2023 – September 2023 | Indianapolis, Indiana

- Managed multiple critical business application development teams that managed and developed all financial applications.
- Managed a major internal project to modernize legacy financial systems from an on-prem hosted legacy system to a cloud-based modernized platform.

Capital One

Project Manager & Agile Program Lead
May 2019 – May 2023 | McLean, VA

Project Manager (Agile Delivery Lead (ADL) & Release Train Engineer) for Decisioning Platforms vertical in Card Tech organization. Worked with 8 and led 2 engineering teams to deliver best-in-class fraud detection and prevention systems in the Credit Card space. Managed multiple teams in delivery solutions and development of IT platforms technology imperatives and modernization. Member of leadership team.

- Project manager for data ingestion platform for major banking core data modernization platform: CPAL (Core Processing Abstraction Layer); led 2.5-year project from start to finish, saving $10M+ by building in-house system.
- Developed objectives and agile planning solution used by 20+ engineering teams.
- Increased team engineering velocity by 25% overall by implementing team and organizational scrum activities, including stand up, sprint planning, and retrospectives.
- Drove program increment feature completion rate 20%+ by utilizing Agile business methods to streamline and update business processes.

Deloitte Consulting

Senior Consultant
August 2015 – April 2019 | McLean, VA

Project Manager of major IT transformation project for Maryland Department of Health (MDH), leading team in designing, building, and maintaining new SaaS solution for agencies across Maryland. Led cloud migration strategy development for clients, including Freddie Mac and other smaller companies.

- Worked closely with client and Deloitte management to develop and execute project plan and ensure successful delivery and deployment of first SaaS in MDH history.
- Collaborated with client, business, and technical engineers, subcontractors, and vendors to manage projects within multiple work streams and develop software solutions from the ground up.
- Developed budget management process for personnel, services, and software to ensure adherence to budget and schedule; provided client with weekly financial/project status updates.
- Designed agile project management tool—adopted across 150+ resources—meeting specific state and client requirements using Scaled Agile Framework (SAFe).
- Effected project progress despite challenging political landscape by cultivating strong relationships with key leadership and internal stakeholders.

- Showcased project at AWS GovSummit in Washington, DC, presenting a vision, technical background, methodology, and overall success with the client.
- Publicly recognized by Deloitte to nationwide firm leadership for carrying project success.

Emagine IT

Consultant & Project Lead
January 2013 – July 2015 | Fairfax, Virginia

Supported program initiatives and led projects for client Natural Resource Conservation Service – US Department of Agriculture. Provided guidance within Enterprise Architecture team on various NRCS architecture assessments and deliverables.

- Key contributor in creating and developing the CTO Division's Strategic Plan.
- Analyzed office connectivity for 2,700 NRCS offices and identified $1M+ in service/network redundancies, helping develop centralized network architecture.
- Developed communication for CIO's Enterprise Architecture (EA) roadmap. Participated in Service-oriented architecture working groups across infrastructure work streams.
- Provided support to a major program initiative through architectural and design reviews. Increased clarity and efficiency by leading the redesign of the portal deployed across NRCS.

Tragedy Assistance Program for Survivors (TAPS)

Project Manager
January 2012 – January 2013 | Arlington, VA

IT Manager for staff of 50+ US and UK employees of a nonprofit serving families of fallen soldiers. Provided innovative technical solutions and project/purchasing management for a cloud-based work environment with email, document storage and editing, VoIP telephone service, and expense and time management.

Education

George Mason University

- **Bachelors** – Business Administration
- **Masters** – Master of Business Administration (MBA)

Certifications

- AWS Certified Solutions Architect
- AWS Certified Developer - Associate

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 non responsive.

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.

Assurit's Category 1 Experience and Qualifications

Assurit brings over twelve (12) years of experience delivering **comprehensive Risk Assessment and Mitigation Services** to federal, state, and commercial organizations. Our engagements span **healthcare, human services, financial regulation, and critical infrastructure**, aligning directly with the Category 1 requirements defined in **Attachment 02, Section 2.2** of the RFP.

We highlight three representative projects below that demonstrate our ability to scale and tailor services across environments of varying complexity and scope.

Maryland Department of Human Services (MD DHS)

Contract Value	$10,420,479
Performance Period	August 2016 - September 2025 (ongoing)
Client Scale	State agency serving 6+ million Maryland citizens through integrated healthcare and human services delivery
Systems Scope	40 Major Applications, 8 General Support Systems across 7,500 virtual cloud instances
Data Volume	Processing millions of eligibility determinations annually across SNAP, Medicaid, Child Welfare, and Temporary Cash Assistance programs
Geographic Coverage	Statewide service delivery with federal agency integration (Centers for Medicare & Medicaid Services (CMS), Social Security Administration (SSA), Internal Revenue Service (IRS))

Assurit has served as the primary cybersecurity partner for the Maryland Total Human-services Integrated Network (MD THINK), one of the most ambitious IT modernization efforts undertaken by a state agency. Our comprehensive risk assessment and mitigation services directly fulfill Category 1 requirements:

Implementation of Risk Assessments and Mitigation Strategies (Section 2.2.1)

- Developed a unified security framework through rigorous crosswalk of seven distinct security frameworks, including NIST SP 800-53 (Revisions 4 and 5), HIPAA, IRS Pub 1075, CMS MARS-E, SOC 2, ISO 27001, and CIS Top 20
- Implemented a "high-water mark" approach, ensuring the most stringent control requirements were adopted across all security domains
- Created comprehensive security policies, procedures, and templates serving as the foundation for guiding System Owners through all phases of the Risk Management Framework

Compliance Assessment and Evaluation (Section 2.2.1)

- Achieved and maintained 100% compliance with CMS, IRS, SSA, and HHS security requirements
- Conducted a thorough evaluation of threats and vulnerabilities across the entire cloud infrastructure and proprietary systems
- Performed annual compliance assessments against federal disclosure responsibilities and state regulations

Threat and Vulnerability Assessment (Section 2.2.1)

- Deployed comprehensive vulnerability assessment using Tenable Nessus for infrastructure scanning and HCL AppScan/Fortify/SonarQube for application security testing
- Integrated security scanning into CI/CD pipelines using Ansible/Terraform for automated configuration validation
- Achieved >90% security compliance across 7,500 cloud assets through "Deny-by-Default" principles
- Conducted annual penetration tests using methodologies based on OSINT, MITRE ATT&CK, and OWASP frameworks

Policy Review and Recommendations (Section 2.2.1)

- Developed essential Security Authorization templates including System Security Plans (SSP), Privacy Impact Assessments (PIA), and POA&M workbooks with embedded control language
- Created security policies aligned with mainstream information security frameworks and standards

Business Process Design and Development (Section 2.2.2)

- Designed and implemented business processes and procedures in direct response to risk assessment findings
- Developed technical solutions and business applications to address identified security gaps.

Federal Election Commission (FEC)

Contract Value	$3,665,841
Performance Period	March 2021 - March 2029 (ongoing)
Client Scale	Independent regulatory agency with approximately 330 employees overseeing campaign finance for federal elections
Systems Scope	Mission-critical systems supporting disclosure of campaign finance data, enforcement, and public transparency
Data Volume	High-volume transactional and disclosure data related to millions of financial records across election cycles
Geographic Coverage	Nationwide oversight of federal campaign finance activity across all U.S. states and territories

At the Federal Election Commission, Assurit implemented comprehensive risk assessment and mitigation services that directly address Category 1 requirements:

Risk Assessment Implementation (Section 2.2.1)

- Developed and implemented a risk-based vulnerability assessment model evaluating severity, exploitability, and mission impact of vulnerabilities across election-related systems
- Created structured Plans of Action and Milestones (POA&M) tracking protocols enhancing transparency and audit readiness
- Implemented rigorous testing and validation protocols ensuring effectiveness of remediation efforts

High Value Asset Program Development

- Designed and deployed a formal HVA governance program fully aligned with OMB M-19-03 and DHS CISA mandates

- Developed HVA identification framework through collaboration with system owners and in-depth FISMA system inventory reviews
- Created HVA Program Strategy and Plan defining governance roles, measurable objectives, and repeatable processes

Technical Risk Assessment Methodology

- Utilized Tenable Security Center for vulnerability management and Qualys for cloud security posture monitoring
- Implemented risk prioritization using CVSS scoring to focus on high-impact vulnerabilities
- Conducted penetration testing of election systems using industry-standard tools and MITRE ATT&CK methodology

U.S. Commodity Futures Trading Commission (CFTC)
Office of Inspector General

Contract Value	$591,256
Performance Period	July 2019 - July 2023
Client Scale	Independent regulatory agency with 736 employees overseeing U.S. derivatives markets
Systems Scope	Critical trading systems and market oversight infrastructure
Data Volume	Real-time processing of derivatives market data worth trillions in notional value
Geographic Coverage	Nationwide regulation of futures and swaps markets

Assurit supported the CFTC OIG's annual FISMA audit and cybersecurity oversight through comprehensive risk assessment services, fulfilling Category 1 requirements:

Control Assessment and Evaluation (Section 2.2.1)

- Evaluated design and operational effectiveness of cybersecurity controls across critical systems and programs
- Conducted detailed reviews of cybersecurity documentation, including system security plans, policies, POA&M workbooks, and architectural diagrams
- Developed control-based questionnaires aligned with NIST SP 800-53A and conducted stakeholder interviews

Compliance Verification and Assessment

- Assessed Zero Trust implementation against Executive Order 14028 and OMB M-22-09 requirements
- Created structured work papers mapping findings to federal and organizational requirements
- Developed Notices of Finding and Recommendation (NFRs) with prioritized remediation strategies

Advanced Technical Assessment

- Employed white-box testing methodology with documentation-informed attack vectors
- Conducted multi-platform testing across network infrastructure, web applications, and Azure cloud components
- Provided evidence-based validation with detailed capture of commands, screenshots, and reproducible steps

Comprehensive Final Reporting (Section 2.2.3)

Across all engagements, Assurit consistently delivers comprehensive final written reports within one week of the engagement conclusion, which include detailed risk statements, explanations, and actionable recommendations for mitigating identified risks. Our reports provide clear prioritization of threats and cost evaluation of remediation strategies.

Alignment with Category 1 Requirements

These engagements demonstrate Assurit's extensive experience providing all services required under Category 1 Risk Assessment and Mitigation Services. Our proven methodology encompasses:

- ☑ **Framework-Aligned Risk Strategy Implementation:** Implementation of risk assessments and mitigation strategies aligned with published, mainstream information security frameworks and standards
- ☑ **Regulatory Compliance Assessment:** Compliance assessment of disclosure responsibilities and applicable federal, state, and local regulations
- ☑ **Comprehensive Threat and Vulnerability Analysis:** Evaluation of threats and vulnerabilities in current environments, including proprietary systems
- ☑ **Risk-Based Prioritization and Cost Analysis:** Prioritization of threats and weaknesses with comprehensive cost evaluation
- ☑ **Security Policy Development and Enhancement:** Review and recommendations for improvement and creation of information security policies
- ☑ **Business Process and Application Design:** Design and development of business processes and applications in response to risk assessments

Our team has successfully scaled these services across organizations ranging from state agencies serving millions of citizens to federal regulatory bodies overseeing trillion-dollar markets. This proven track record positions Assurit to deliver exceptional Category 1 services to NASPO ValuePoint participating entities, bringing our comprehensive risk assessment methodology and commitment to regulatory excellence to support their cybersecurity objectives.

(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.

Experience and Qualifications

Assurit's Category 1 Risk Assessment and Mitigation Services are built upon highly qualified cybersecurity professionals who significantly exceed the minimum requirements outlined in Attachment 02, Section 2.3. Our current team leadership establishes the methodology, quality standards, and technical approach for all risk assessment activities.

Foundation of Excellence Through Current Team Leadership

Our Category 1 services are led by senior professionals with extensive experience and advanced certifications, ensuring exceptional deliverables. Mr. Thang Pham, our CTO and Vice President, brings 20+ years of information

security experience with a Master's degree in Applied Information Technology (Cyber Security). His certifications include CISSP, CISM, CISA, CGRC, PMP, OSCE3, OSCP, GPEN, and GWAPT, having led over 150 risk assessment engagements across federal and commercial sectors.

Mr. Jonathan Perez, Director of Cybersecurity Services, brings 10 years of experience in governance, risk, and compliance, complemented by a Master's degree in Cybersecurity. His certifications include CISSP, CGRC, CEH, and AWS Solutions Architect, with expertise in risk assessment methodologies and compliance frameworks. He has led comprehensive assessments for the Federal Election Commission, Maryland Department of Human Services, and U.S. Patent and Trademark Office.

Mr. Andy Lien, Cloud Security Engineer, provides 10 years of cloud governance experience with certifications including CISSP, CGRC, CCSK, and AWS Solutions Architect, specializing in cloud security architecture and NIST 800-53 assessments.

Staff Qualification Requirements

Security/Technology Senior Analyst Role

Assurit requires personnel with five or more years of information security experience, demonstrated expertise in risk assessments using mainstream frameworks (NIST, ISO 27001, COBIT), and hands-on experience with vulnerability assessment tools and security control testing. Technical capabilities must include proficiency with vulnerability scanning tools (such as Tenable Nessus, Qualys, and Rapid7), experience with NIST SP 800-53A assessment methodologies, knowledge of cloud security frameworks, and the ability to analyze and prioritize security findings based on their business impact.

Required certifications include one advanced security certification, such as CISSP, CISA, CISM, GPEN, or GSEC. Preferred additional certifications include CGRC, CCSK, cloud platform security certifications, and CompTIA Security+ or Network+. Areas of specialization include risk management frameworks (NIST RMF, ISO 27005), compliance frameworks (FedRAMP, FISMA, SOC 2, HIPAA), cloud security assessment, and vulnerability management.

Business Process/Risk Management Senior Consultant Role

Personnel must possess five or more years of experience in risk management, compliance, or business process analysis, with a deep understanding of industry-specific risk practices. Required capabilities include translating technical findings into business risk language, developing risk mitigation strategies, a comprehensive knowledge of regulatory compliance requirements, and experience with risk assessment methodologies and quantitative analysis.

Required certifications include CISA, CISM, CGRC, or CRISC. Preferred certifications include CIA, CRCP by FINRA, and PMP. Specialization areas encompass enterprise risk management, regulatory compliance across multiple sectors, privacy frameworks (including GDPR, CCPA, and HIPAA), and third-party risk management.

Project Manager Role

Project Managers must have five or more years of experience in project management, preferably in cybersecurity, with demonstrated expertise in managing complex security assessments, budget management, and resource allocation. Technical understanding must include cybersecurity project lifecycles, risk assessment methodologies, and security frameworks. PMP certification is mandatory, with additional security awareness certification preferred. Specialized expertise includes security assessment, project management, and client relationship management in regulated environments.

Professional Development and Quality Assurance

Assurit maintains rigorous standards requiring all Category 1 staff to maintain professional certifications through continuing education and complete 40 hours of annual cybersecurity professional development. Our team actively

participates in industry conferences and training programs, staying current with emerging threats, evolving regulations, and advancing security frameworks.

Our quality assurance process includes a technical review by senior, certified staff; peer review of findings and recommendations; and final approval by team leaders with 10+ years of experience. We maintain standardized assessment procedures based on industry best practices, with regular methodology updates that reflect evolving threats and ensure continuous alignment with NIST, ISO, and other recognized frameworks. This comprehensive approach ensures consistent delivery of Category 1 services that exceed client expectations while maintaining the highest professional standards.

(ME) SLA's. 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.

Service Level Agreements

Assurit is committed to delivering Category 1 Risk Assessment and Mitigation Services with clearly defined service levels that ensure timely, high-quality deliverables while maintaining transparent communication with Participating Entities. Our Service Level Agreements (SLAs) are designed to meet the specific requirements outlined in the Scope of Work while providing flexibility to accommodate the unique needs of each engagement.

Service Initiation and Response Times

Initial Response and Project Kickoff

Upon receipt of a Statement of Work from a Participating Entity, Assurit will provide initial acknowledgment within two (2) business hours during standard business hours (8:00 AM to 6:00 PM ET, Monday through Friday, excluding federal holidays). Our Contract Manager will conduct an initial scoping call within five (5) business days to review requirements, clarify deliverables, establish timelines, and address any questions regarding the engagement scope.

- **Standard Requests:** For standard risk assessment engagements, Assurit will provide a detailed project plan, including resource allocation, timeline milestones, and deliverable schedules, within ten (10) business days of executing the Statement of Work.
- **Urgent Requests:** For urgent or time-sensitive assessments, we will expedite this process and provide project plans within five (5) business days, with the ability to begin preliminary work within two (2) business days when circumstances require immediate attention.

Resource Deployment and Team Assignment

Assurit will assign qualified personnel meeting the requirements specified in Section 2.3 within five (5) business days of project plan approval. For on-site engagements, our team will be available to deploy within ten (10) business days of receiving final approval and any required security clearances or access authorizations from the Participating Entity. In cases where expedited deployment is needed, we will make our best efforts to accommodate compressed timelines while ensuring all personnel meet the specified qualifications and security requirements.

Service	Commitment	Responsible Party
Initial acknowledgment of Statement of Work	2 business hours	Assurit
Initial scoping call with client	5 business days	Assurit

Service	Commitment	Responsible Party
Project plan delivery (standard engagements)	10 business days	Assurit
Project plan delivery (urgent engagements)	5 business days	Assurit
Qualified personnel assignment	5 business days	Assurit
On-site team deployment	10 business days	Assurit

Assessment Execution and Progress Reporting

Regular Communication and Status Updates

Throughout the engagement, Assurit will provide weekly status reports detailing progress against established milestones, any identified issues or risks, preliminary findings of significance, and upcoming activities scheduled for the following week. These reports will be delivered every Friday by 5:00 PM ET via email to the designated points of contact of Participating Entities, with additional ad-hoc updates provided as circumstances warrant.

For engagements extending beyond 30 days, Assurit will conduct bi-weekly progress calls with Participating Entity stakeholders to discuss findings, address questions, and ensure alignment with expectations. These calls will be scheduled at mutually convenient times and will include technical team members, project management, and client representatives as appropriate.

Issue Escalation and Resolution

Any issues that may impact the project timeline, scope, or deliverable quality will be escalated to the Participating Entity within 24 hours of identification. Assurit will propose resolution strategies and work collaboratively with the Participating Entity to minimize any impact on project objectives. For critical issues that could significantly affect the assessment or require immediate attention, notification will be provided within four (4) hours during business hours or by 9:00 AM ET the following business day for issues identified outside standard hours.

Service	Commitment	Responsible Party
Weekly status reports	Friday by 5:00 PM ET	Assurit
Bi-weekly progress calls (projects >30 days)	As scheduled	Both Parties
Project plan delivery (standard engagements)	24 Hours	Assurit
Critical issue escalation	4 hours during business hours	Assurit

Deliverable Standards and Timeline Commitments

Interim Deliverables and Draft Reports

For assessments requiring interim deliverables or progress reports, Assurit will provide these materials according to the timeline specified in the Statement of Work, with a standard commitment to deliver interim products within five (5) business days of completing the associated assessment activities. Draft reports and preliminary findings will be delivered for Participating Entity review within ten (10) business days of completing field work or assessment activities.

Final Report Delivery

In accordance with the Scope of Work requirements, Assurit will deliver comprehensive final written reports within five (5) business days of engagement conclusion, or as otherwise specified in the Statement of Work. These

reports will include detailed risk statements, explanations, and actionable recommendations for mitigating identified risks, with clear prioritization based on severity and business impact.

Report Quality and Revision Process

All deliverables undergo rigorous quality assurance review by senior staff before delivery to ensure accuracy, completeness, and alignment with engagement objectives. Should the Participating Entity request revisions or clarifications, Assurit will provide revised materials within five (5) business days of receiving detailed feedback. Minor clarifications and corrections will be addressed within two (2) business days.

Service	Commitment	Responsible Party
Interim deliverables	5 business days after completion	Assurit
Draft reports	10 business days after field work	Assurit
Final comprehensive reports	5 business days after conclusion	Assurit
Major report revisions	5 business days	Assurit
Minor report clarifications	2 business days	Assurit

Contractor Responsibilities and Commitments

Personnel and Expertise Standards

Assurit commits to providing only qualified personnel who meet or exceed the minimum qualifications specified in Section 2.3 for their respective roles. All assigned personnel will maintain current certifications and demonstrate relevant experience in the specific assessment methodologies and frameworks required for the engagement. We guarantee that Security/Technology Senior Analysts and Business Process/Risk Management Senior Consultants will possess appropriate industry certifications, and Project Managers will maintain current PMP certification.

Methodology and Framework Compliance

Our risk assessments will be conducted using established, mainstream information security frameworks and standards, as specified in the Statement of Work, including, but not limited to, NIST SP 800-53, ISO 27001, COBIT, and other relevant frameworks. All assessment activities will comply with current federal guidelines and regulations applicable to the Participating Entity's environment and mission requirements.

Data Security and Confidentiality

Assurit will maintain the highest standards of data security and confidentiality throughout the engagement, implementing appropriate safeguards for sensitive information following the security requirements specified in Section 1 of the Scope of Work. All personnel will execute appropriate non-disclosure agreements and comply with security protocols established by the Participating Entity.

Responsibility	Commitment	Standard
Qualified personnel provision	Meet or exceed Section 2.3 requirements	100% compliance
Certification maintenance	Current industry certifications	Ongoing requirement
Framework compliance	NIST, ISO 27001, COBIT, other relevant standards	Per Statement of Work
Data security and confidentiality	Highest security standards per Section 1	Continuous compliance

Responsibility	Commitment	Standard
Quality assurance	Senior staff review of all deliverables	100% of deliverables

Participating Entity Responsibilities

Access and Coordination Support

The Participating Entity is responsible for providing timely access to systems, personnel, and documentation necessary for assessment activities as outlined in the Statement of Work. This includes coordinating interviews with key stakeholders, providing system access credentials or arranging for Assurit personnel to receive appropriate access, and ensuring availability of technical subject matter experts during assessment periods.

Review and Feedback Timeliness

To maintain project schedules, the Participating Entity agrees to review interim deliverables and provide feedback within ten (10) business days of receipt. Critical items will be reviewed within five (5) business days when specifically identified. Final reports should be reviewed within fifteen (15) business days to allow for any necessary revisions while meeting overall project timelines.

Information Provision and Accuracy

The Participating Entity will provide accurate and complete information regarding system configurations, policies, procedures, and organizational structure relevant to the scope of the assessment. Any significant changes to systems or environments that occur during the assessment period should be communicated promptly to avoid any impact on findings and recommendations.

Responsibility	Commitment	Timeframe
System and personnel access	Provide timely access per Statement of Work	As specified in SOW
Stakeholder interview coordination	Coordinate the availability of key personnel	As mutually scheduled
Documentation provision	Provide accurate system/policy information	Ongoing
Interim deliverable review	Review and provide feedback	10 business days
Critical item review	Review urgent deliverables	5 business days
Final report review	Complete review and feedback	15 business days
Change notification	Communicate system/environment changes	Promptly upon occurrence

Performance Metrics and Continuous Improvement

Quality Metrics and Client Satisfaction

Assurit tracks performance metrics including on-time delivery rates, client satisfaction scores, and finding accuracy to ensure continuous improvement in service delivery. We maintain a target of 95% on-time delivery for all commitments and conduct post-engagement client satisfaction surveys to identify opportunities for improvement.

Flexibility and Accommodation

While maintaining firm commitments to quality and timeliness, Assurit recognizes that the needs of Participating Entities may evolve during engagements. We will work collaboratively to accommodate reasonable scope

adjustments, timeline modifications, or changing priorities while maintaining the integrity of the assessment process and ensuring all deliverables meet established quality standards.

Metric	Target/Commitment	Measurement
On-time delivery rate	95% minimum	All project commitments
Client satisfaction	Post-engagement survey	Each completed engagement
Quality metrics tracking	Continuous monitoring	Finding accuracy and completeness
Scope flexibility	Collaborative accommodation	Reasonable adjustments as needed
Continuous improvement	Ongoing process enhancement	Based on lessons learned and feedback

These Service Level Agreements reflect Assurit's commitment to excellence in Category 1 Risk Assessment and Mitigation Services while establishing clear expectations and responsibilities for successful engagement outcomes. We view these SLAs as the foundation for productive partnerships with NASPO ValuePoint Participating Entities and remain committed to exceeding these standards whenever possible.

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.

Assurit's Category 1 Value-Added Services

Assurit offers specialized value-added services that extend beyond traditional risk assessment and mitigation activities to address the complex cybersecurity challenges facing modern organizations. These advanced services leverage our proven expertise in government cybersecurity programs, cloud security architecture, and multi-framework compliance to deliver targeted solutions that enhance security posture and operational resilience. Each service is designed to address specific gaps that standard risk assessments may not fully cover, providing organizations with comprehensive protection strategies, regulatory alignment, and implementation roadmaps tailored to their unique operational requirements and threat landscape.

Service Name	Description
Zero Trust Architecture Assessment & Implementation Planning	Comprehensive Zero Trust security model assessment including network segmentation analysis, identity and access management evaluation, endpoint security review, and data protection strategy development with phased implementation roadmap and technology recommendations.
Cloud Security Architecture Risk Review	Comprehensive risk assessment of cloud environments covering shared responsibility models, container security, serverless architectures, and cloud-native applications with security architecture recommendations.
Supply Chain Risk Assessment	Third-party vendor security posture evaluation, supply chain attack vector analysis, and vendor risk scoring methodology development with ongoing monitoring recommendations.
High Value Asset (HVA) Program Development	Complete HVA program creation from identification and classification through protection strategy development, including CISA assessor training and annual assessment planning.

Service Name	Description
Application Security Risk Assessment Program	Comprehensive application security evaluation including static/dynamic code analysis integration, API security assessment, and DevSecOps implementation guidance beyond standard vulnerability scanning.
Security Governance Program Maturity Assessment	Evaluation of security governance structures, policy effectiveness, risk management processes, and organizational security maturity with improvement roadmap and metrics development.

Cloud Security Architecture Risk Review

This service offers a comprehensive risk assessment of cloud environments, encompassing shared responsibility models, container security, serverless architectures, and cloud-native applications. We evaluate cloud security configurations, assess risks in multi-cloud and hybrid environments, and analyze security controls of cloud service providers. The assessment includes cloud workload protection evaluation, data sovereignty analysis, and cloud-specific threat modeling. We provide detailed security architecture recommendations for secure cloud adoption, migration strategies, and ongoing cloud security monitoring.

Previous Experience

- **MD THINK**: Comprehensive cloud security architecture design and risk assessment for $200M state modernization initiative
- **FEC:** Cloud environment security evaluation and AWS configuration assessment
- **CFTC:** Azure cloud infrastructure security review and compliance validation

Supply Chain Risk Assessment

This service provides a comprehensive evaluation of vendor and supply chain security risks that could impact the organization. We assess third-party security postures through questionnaires, on-site evaluations, and technical assessments. The service includes development of vendor risk scoring methodologies, contract language recommendations, ongoing monitoring processes, and incident response procedures for supply chain compromises. We evaluate cloud service providers, software vendors, hardware suppliers, and service providers to identify potential attack vectors and concentration risks.

Previous Experience

- **USPTO:** Conducted security assessments of third-party cloud vendors seeking provisional Authority to Operate
- **MD THINK:** Evaluated and assessed cloud service providers and integration partners for federal compliance
- **FEC:** Assessed vendor security capabilities as part of vulnerability management modernization

High Value Asset (HVA) Program Development

This service establishes a comprehensive program for identifying, classifying, and protecting an organization's most critical digital assets. We develop HVA identification criteria based on mission impact, data sensitivity, and operational criticality. The program includes governance structure creation, policy development, assessment methodologies, and ongoing monitoring processes. We provide training for internal staff to become certified HVA assessors, establish automated asset tagging and tracking systems, and integrate HVA considerations into incident response and business continuity planning.

Previous Experience

- **FEC**: Built the agency's first enterprise-wide HVA program from scratch, resulting in a CISA-certified HVA designation
- **MD THINK**: Identified and classified high-value assets across cloud infrastructure serving critical state programs
- **CFTC**: Evaluated critical trading systems and market data assets for enhanced protection

Application Security Risk Assessment Program

This service offers an in-depth security evaluation of applications, extending beyond standard vulnerability scanning. We conduct static application security testing (SAST), dynamic application security testing (DAST), interactive application security testing (IAST), and manual code review to identify complex security flaws. The assessment includes an API security evaluation, a review of authentication and authorization mechanisms, data flow analysis, and integration security testing. We provide guidance on DevSecOps implementation, security testing automation recommendations, and developer training on secure coding practices.

Previous Experience

- **MD THINK:** Implemented comprehensive application security testing using HCL AppScan, MicroFocus Fortify, and SonarQube integrated into CI/CD pipeline
- **SEC:** Performed static and dynamic application testing across multiple programming languages and platforms
- **CFTC:** Conducted advanced web application penetration testing using OWASP methodologies

Security Governance Program Maturity Assessment

This service provides evaluation of security governance structures, policy effectiveness, risk management processes, and organizational security maturity. We assess the alignment of our governance framework with industry standards, evaluate the effectiveness of policy implementation, and analyze security program metrics and reporting structures. The assessment includes a board-level cybersecurity governance review, security awareness program evaluation, and organizational risk culture analysis. We provide improvement roadmaps, governance structure recommendations, and metrics development to enhance overall security program maturity.

Previous Experience

- **MD THINK:** Developed a comprehensive security governance framework integrating multiple federal and state requirements
- **FEC:** Established governance processes for vulnerability management and HVA programs
- **CFTC:** Evaluated and enhanced cybersecurity governance structures for regulatory compliance

Additional Labor Categories

Our Category 1 value-added services will be supported by specialized labor categories that bring focused expertise to complex cybersecurity challenges. These roles are specifically designed to deliver the advanced technical, architectural, and governance capabilities required for our enhanced service offerings. Each labor category includes both analyst and senior levels to provide appropriate expertise scaling based on project complexity and organizational needs. The following labor categories have been developed with specific qualifications and experience requirements to ensure the highest quality service delivery across all value-added service areas.

Labor Category	Role Description	Requirements
Security Assessment Consultant	Conducts technical security evaluations including vulnerability assessments, compliance testing, vendor security reviews, and application security analysis	• 3+ years cybersecurity experience • Security+ or equivalent certification • Experience with vulnerability scanning tools • Knowledge of NIST frameworks • Basic scripting abilities
Security Assessment Senior Consultant	Leads complex security evaluations, develops assessment methodologies, and provides technical guidance on security testing and validation activities	• 7+ years cybersecurity experience • CISSP, CISA, or equivalent advanced certification • Expert-level knowledge of assessment methodologies • Experience leading assessment teams • Advanced technical writing and reporting skills
Cybersecurity Architect Consultant	Performs security architecture analysis, technology evaluations, and supports design of security solutions and implementation planning	• 4+ years in security architecture or engineering • Cloud security certification (AWS, Azure, or CCSP) • Knowledge of network security and identity management • Understanding of enterprise security technologies • Basic system design experience
Cybersecurity Architect Senior Consultant	Leads security architecture design, develops comprehensive security strategies, and provides expert guidance on complex security technology implementations	• 8+ years in security architecture and design • Multiple advanced certifications (CISSP, SABSA, TOGAF) • Proven experience designing enterprise security solutions • Expert knowledge of Zero Trust and cloud architectures • Experience with security technology integration
Compliance and Governance Consultant	Supports regulatory compliance analysis, policy development, framework mapping, and governance structure assessment activities	• 3+ years in compliance or risk management • Knowledge of major security frameworks (NIST, ISO 27001) • Experience with compliance documentation • Understanding of regulatory requirements • Strong analytical and documentation skills
Compliance and Governance Senior Consultant	Leads complex compliance harmonization efforts, develops governance frameworks, and provides expert guidance on regulatory and risk management strategies	• 7+ years in compliance, risk, or governance • CISA, CISM, or equivalent governance certification • Expert knowledge of multiple compliance frameworks • Experience developing enterprise governance programs • Proven ability to lead compliance initiatives

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.

Assurit has provided comprehensive incident response services to federal agencies and state entities, consistently demonstrating our capability to deliver critical Category 2 services outlined in Attachment 02. Our experience encompasses essential incident response capabilities, including event and incident management, containment, eradication, recovery, and forensic analysis across diverse technology environments and complex cybersecurity scenarios.

Maryland Department of Human Services (MD DHS)

Contract Value	$10,420,479
Performance Period	August 2016 - September 2025 (ongoing)
Client Scale	State agency serving 6+ million Maryland citizens through integrated healthcare and human services delivery
Systems Scope	40 Major Applications, 8 General Support Systems across 7,500 virtual cloud instances
Data Volume	Processing millions of eligibility determinations annually across SNAP, Medicaid, Child Welfare, and Temporary Cash Assistance programs
Geographic Coverage	Statewide service delivery with federal agency integration (Centers for Medicare & Medicaid Services (CMS), Social Security Administration (SSA), Internal Revenue Service (IRS))

Assurit's nine-year engagement with Maryland THINK provided extensive hands-on experience in proactive threat management and incident response capabilities across a complex, multi-stakeholder cloud environment serving millions of Marylanders.

Threat Management & Response (Category 2 Core)

- Implemented comprehensive vulnerability management using Tenable Nessus with automated scanning and remediation tracking
- Conducted annual penetration testing covering cloud, network, and application components using MITRE ATT&CK and OWASP methodologies
- Performed containment simulation through penetration testing with 3-month testing windows, including scoping, reconnaissance, execution, and remediation validation

Forensic Analysis Capabilities (Section 3.6)

- Deployed sophisticated testing arsenal including Kali Linux, Sliver C2, Metasploit, Impacket, GhostPack, PowerShell, and Burp Suite Pro
- Conducted forensic-quality evidence collection with detailed documentation, including command syntax and screenshots
- Mapped all findings to NIST SP 800-53 controls and assigned CVSS risk ratings for POA&M integration

Maryland Department of Technology (DoIT)

Contract Value	$90,000
Performance Period	August 2019 – August 2019
Client Scale	State-level IT department serving multiple Maryland government agencies
Systems Scope	Statewide government information systems and data repositories
Data Volume	Analysis of Dark Web and Deep Web data sets for Maryland state agency information exposure
Geographic Coverage	Maryland state government entities and associated data exposure risks

Assurit provided cybersecurity incident investigation and threat analysis services that directly align with Category 2 requirements.

Event and Incident Management (Section 3.2)

- Conducted comprehensive collection, processing, and analysis of data gathered from the World Wide Web and the Dark Web to determine the actual scope of potential data exposure incidents
- Gathered evidence from various sources, including Dark Web forums, public information repositories, and anonymous communication channels
- Documented all investigative actions and findings following proper Chain of Custody protocols for potential law enforcement coordination
- Performed threat actor analysis to identify methods used for selling or exposing Maryland state agency data

Forensic Analysis Capabilities (Section 3.6)

- Conducted in-depth analysis and investigation using legally admissible methodologies to identify potential data compromises
- Performed a comprehensive examination of Dark Web marketplaces and communication channels to discover Maryland state agency information exposure
- Analyzed file structures, data posting patterns, and threat actor behavior to determine the scope and impact of potential breaches
- Created detailed technical reports documenting overall analysis, discovered data exposure, and recommended remediation strategies

Threat Detection and Investigation

- Utilized advanced reconnaissance techniques including VPN services and Onion Router networks for secure investigation
- Implemented Natural Language Processing (NLP) and machine learning algorithms for automated threat detection and data analysis
- Performed passive reconnaissance using publicly available information and social media analysis
- Conducted link analysis to map potential attack vectors and data exposure points affecting Maryland government entities

This engagement demonstrates Assurit's proven expertise in critical incident response investigation capabilities, including comprehensive threat analysis, forensic examination of compromised data, and detailed incident documentation that forms the foundation of effective cybersecurity incident response services.

Federal Election Commission (FEC)

Contract Value	$3,665,841
Performance Period	March 2021 - March 2029 (ongoing)
Client Scale	Independent regulatory agency with approximately 330 employees overseeing campaign finance for federal elections
Systems Scope	Mission-critical systems supporting disclosure of campaign finance data, enforcement, and public transparency
Data Volume	High-volume transactional and disclosure data related to millions of financial records across election cycles
Geographic Coverage	Nationwide oversight of federal campaign finance activity across all U.S. states and territories

Through our ongoing partnership with the FEC since 2021, Assurit has modernized its vulnerability management program and developed enterprise-wide incident response capabilities that directly support election security infrastructure.

Event and Incident Management (Section 3.2)

- Developed automated, intelligence-driven vulnerability assessment models that evaluate severity, exploitability, and mission impact
- Implemented structured Plans of Action and Milestones (POA&M) tracking for incident documentation and accountability
- Created enterprise-wide visibility and monitoring systems for threat detection and response

Recovery and Validation Services (Sections 3.5-3.6)

- Implemented rigorous testing and validation protocols to ensure remediation effectiveness
- Developed verification procedures that confirm vulnerabilities are eliminated before marking as resolved
- Established automated patch deployment and configuration management for rapid recovery

U.S. Commodity Futures Trading Commission (CFTC)
Office of Inspector General

Contract Value	$591,256
Performance Period	July 2019 - July 2023
Client Scale	Independent regulatory agency with 736 employees overseeing U.S. derivatives markets
Systems Scope	Critical trading systems and market oversight infrastructure
Data Volume	Real-time processing of derivatives market data worth trillions in notional value
Geographic Coverage	Nationwide regulation of futures and swaps markets

Assurit's comprehensive cybersecurity assessment for the CFTC OIG demonstrated advanced incident response methodologies and forensic capabilities essential for protecting critical financial market infrastructure.

Advanced Forensic Analysis (Section 3.6)

- Conducted comprehensive penetration testing across network infrastructure, web applications, and cloud environments (Microsoft Azure)
- Performed practical exploitation demonstrations with detailed evidence capture and documentation
- Validated vulnerabilities through hands-on testing using White-Box methodology and architectural analysis

Comprehensive Reporting (Section 3.7)

- Delivered technical reports, executive summaries, and formal attestation letters
- Provided expert consultation services for remediation strategies
- Created comprehensive documentation mapping findings to federal standards and organizational requirements

Alignment with Category 2 Requirements

These engagements demonstrate Assurit's extensive experience providing all services required under Category 2 Incident Response Services. Our proven methodology encompasses:

- ☑ **Rapid Emergency Response:** Timely incident response with Incident Manager contact within four hours and on-site presence within one business day
- ☑ **Event Investigation and Evidence Management:** Comprehensive event and incident management, including scope determination and evidence collection
- ☑ **Threat Containment Solutions:** Full-spectrum containment services, including short-term and long-term containment strategies
- ☑ **System Restoration and Cleanup:** Complete eradication services with malicious code removal and system restoration
- ☑ **Production Environment Recovery:** Thorough recovery services, including production environment reinstatement with testing and validation
- ☑ **Expert Forensic Capabilities:** Advanced forensic analysis using legally admissible methodologies with expert consultation capabilities
- ☑ **Comprehensive Documentation and Analysis**: Detailed reporting and post-incident analysis with systemic improvement recommendations

Our team has successfully delivered incident response services to organizations ranging from state agencies that process millions of transactions daily to federal regulatory bodies overseeing critical market infrastructure. This proven track record positions Assurit to deliver exceptional Category 2 services to NASPO ValuePoint participating entities, bringing our comprehensive incident response methodology and commitment to rapid, effective incident resolution to support their cybersecurity resilience objectives.

(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.

Experience and Qualifications

Assurit's Category 2 Incident Response Services are delivered by highly qualified cybersecurity professionals who meet and exceed the minimum requirements outlined in Attachment 02, Section 3.9. Our current team leadership establishes the methodology, quality standards, and technical approach for all incident response activities.

Foundation of Excellence Through Current Team Leadership

Our Category 2 services are led by senior professionals with extensive incident response experience and advanced certifications, ensuring exceptional deliverables. Mr. Thang Pham, our CTO and Vice President, brings over 20 years of experience in information security, including specialized incident response management for the Bureau of Alcohol, Tobacco, Firearms, and Explosives (ATF). His advanced certifications include CISSP, CISM, CISA, OSCE3, OSED, OSWE, OSEP, OSCP, GPEN, and GWAPT. His experience as Cyber Incident Response Manager involved leading a six-member Computer Security Incident Response Team (CSIRT), managing cyber intrusion investigations using enterprise tools such as FireEye, Fidelis, NetWitness, and Splunk.

Staff Qualification Requirements

Forensics Incident Investigator Role

Assurit requires personnel with five or more years of experience in digital forensics and incident investigation, demonstrating expertise in identifying, collecting, examining, and preserving digital evidence using controlled and documented analytical techniques. Technical capabilities must include proficiency with forensic tools (such as EnCase, FTK, Cellebrite, and DISA IRRT), experience with NIST SP 800-61 incident response methodologies, knowledge of various operating systems and file systems, and the ability to conduct legally admissible forensic examinations while maintaining Chain of Custody protocols.

Required certifications include advanced forensic certifications such as GCFA (GIAC Certified Forensic Analyst), GCFE (GIAC Certified Forensic Examiner), EnCE (EnCase Certified Examiner), or CCE (Certified Computer Examiner). Preferred additional certifications include GCIH (SANS Certified Incident Handler), ECIH (EC-Council Incident Handler), CHFI (Computer Hacking Forensic Investigator), and CISSP. Areas of specialization include digital forensics across multiple platforms (Windows, Linux, macOS, mobile devices), network forensics and packet analysis, memory forensics and malware analysis, and cloud forensics in AWS, Azure, and hybrid environments.

Business Process/Risk Management Senior Consultant Role

Personnel must possess five or more years of experience in risk management, business continuity, or incident management, with a deep understanding of how security incidents impact business operations. Required capabilities include translating technical incident findings into business impact assessments, developing incident response strategies aligned with business objectives, comprehensive knowledge of regulatory notification requirements, and experience with post-incident recovery planning and business continuity.

Required certifications include CISA, CISM, CGRC, or CRISC. Preferred certifications include CBCP (Certified Business Continuity Professional), MBCI (Member of Business Continuity Institute), and PMP. Specialization areas encompass business impact analysis, regulatory compliance notification requirements across multiple sectors, crisis management and communication, and third-party incident coordination.

Project Manager Role

Project Managers must have five or more years of experience in project management, preferably in cybersecurity incident response, with demonstrated expertise in managing time-sensitive security incidents, coordinating multi-disciplinary response teams, and maintaining stakeholder communication during crises. Technical understanding must include incident response lifecycles, forensic investigation processes, and regulatory notification timelines. PMP certification is mandatory, with additional incident response training preferred. Specialized expertise includes incident response project management, crisis communication, and coordination with law enforcement and regulatory bodies.

Professional Development and Quality Assurance

Assurit maintains rigorous standards requiring all Category 2 staff to maintain professional certifications through continuing education, incident response, and forensic training. Our team actively participates in industry conferences, SANS training programs, and stays current with emerging attack vectors, evolving investigation techniques, and advancing incident response frameworks.

Our quality assurance process includes a technical review by senior, certified incident response professionals; peer review of forensic findings and incident analysis; and final approval by team leaders with over 10 years of incident response experience. We maintain standardized incident response procedures based on NIST SP 800-61 and industry best practices, with regular updates to our methodology that reflect evolving threats and ensure continuous alignment with federal law enforcement and regulatory requirements.

This comprehensive approach ensures consistent delivery of Category 2 services that exceed client expectations while maintaining the highest professional standards for incident response, forensic analysis, and customer support throughout the incident lifecycle.

(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.

Category 2 Customer Service Representatives – Qualifications

Assurit maintains rigorous standards for all customer service representatives supporting incident response operations, ensuring they possess both technical competency and exceptional communication skills essential for high-stress cybersecurity incidents.

Responsibility	Commitment	Standard
Education and experience provision	Bachelor's degree + 2-3 years of technical customer service	100% compliance
Technical certification maintenance	CompTIA Security+, ITIL Foundation	Current industry certifications
Communication proficiency	Native/near-native English, technical translation skills	Per Section 3.8.3 requirements
Specialized training completion	Incident response workflows, crisis communication	Ongoing requirement
Call response performance	Answer all calls within 5 minutes	100% adherence to RFP standard

Responsibility	Commitment	Standard
Incident triage accuracy	Correctly route incidents to technical specialists	95% accuracy rate
Professional service delivery	Consistent communication standards across all interactions	Continuous compliance
Quality assurance monitoring	Regular performance evaluations and improvement	100% of representatives

Minimum Education and Experience Requirements (Section 3.8.3)

- Bachelor's degree in Information Technology, Cybersecurity, Communications, or related field, or equivalent combination of education and experience
- Minimum 2-3 years of experience in technical customer service, help desk operations, or cybersecurity support roles
- Demonstrated experience in incident coordination, escalation procedures, and multi-stakeholder communication
- Previous experience supporting government or regulated industry clients preferred

Essential Technical Qualifications (Sections 3.1.5 & 3.8)

- CompTIA Security+ certification or equivalent cybersecurity fundamentals certification
- ITIL Foundation certification for incident management and service delivery best practices
- Understanding of basic networking concepts, system administration, and cybersecurity terminology
- Proficiency with incident tracking systems, ticketing platforms, and customer relationship management (CRM) tools
- Familiarity with federal compliance requirements and government communication protocols

Communication and Customer Service Standards (Section 3.8.3)

- Excellent verbal and written communication skills with the ability to explain technical concepts to non-technical stakeholders
- Native or near-native English proficiency with precise articulation and professional phone presence
- Active listening skills and empathy for handling stressed clients during security incidents
- Cultural sensitivity and professional demeanor when working with diverse government entities across multiple states

Specialized Training Requirements (Sections 3.1.5 & 3.8.2)

- Comprehensive incident response workflow training covering all Category 2 service processes
- Customer service excellence training focused on crisis communication and de-escalation techniques
- Security awareness training covering data handling, confidentiality, and federal privacy requirements
- Regular continuing education on emerging threats, incident response best practices, and regulatory updates

Performance Standards and Metrics (Section 3.8.3)

- Adherence to 1-minute call answer time requirement as specified in the RFP
- Demonstrated ability to triage incidents and route to appropriate technical specialists accurately
- Consistent professional communication standards across all client interactions
- Continuous performance monitoring and quality assurance evaluations to maintain service excellence

(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.

Service Level Agreements

Assurit is committed to delivering Category 2 Incident Response Services with clearly defined service levels that ensure rapid response, comprehensive technical expertise, and transparent communication during critical cybersecurity incidents. Our Service Level Agreements (SLAs) are designed to meet the specific requirements outlined in the Scope of Work while providing the flexibility and urgency required for effective incident response operations.

Service Initiation and Response Times

Emergency Incident Response (Section 3.1.3)

Upon notification of a cybersecurity incident by a Participating Entity, Assurit's Incident Manager will provide initial response by telephone or email within four (4) hours of receiving the notification, regardless of time of day or week. This initial response will include acknowledgment of the incident, preliminary assessment questions, and activation of our incident response team. Our 24x7 monitored email system ensures that all priority communications are received and escalated immediately to appropriate response personnel.

- **Critical Incidents:** For incidents involving active breaches, data exfiltration, or system compromises, Assurit will initiate immediate response protocols and can have qualified personnel on-site within one (1) business day of the request, as specified in Section 3.1.4.
- **Standard Incidents:** For routine security events requiring investigation or analysis, we will provide a comprehensive response plan and resource allocation within eight (8) hours of initial contact, with engagement activities beginning within two (2) business days.

Team Deployment and Resource Assignment

Assurit will deploy qualified incident response personnel meeting the requirements specified in Section 3.9 immediately upon incident activation. For on-site engagements requiring physical presence, our team will coordinate travel and arrive at the Participating Entity's location within one (1) business day, or as mutually agreed upon in the Work Order per Section 3.1.4.

Service	Commitment	Responsible Party
Initial incident acknowledgment	4 hours	Assurit
Incident Manager response	4 hours (24x7)	Assurit
Comprehensive response plan delivery	8 hours (standard incidents)	Assurit
Emergency response plan delivery	2 hours (critical incidents)	Assurit
Qualified personnel assignment	Immediate upon activation	Assurit
On-site team deployment	1 business day	Assurit
Initial incident acknowledgment	4 hours	Assurit

Ongoing Service Delivery and Communication

Incident Documentation and Reporting (Section 3.7.2)

Throughout active incident response engagements, Assurit will provide structured communication and documentation to ensure Participating Entities maintain complete visibility into response activities and progress. Written status reports detailing activities completed, current findings, and planned next steps will be delivered no less frequently than weekly, or as otherwise specified by the Participating Entity's requirements.

Forensic Analysis and Evidence Management (Section 3.6)

All forensic activities will be conducted using legally admissible methodologies with strict adherence to Chain of Custody protocols as outlined in Section 3.2.2. Assurit will maintain detailed documentation of all evidence collection, analysis procedures, and findings, with comprehensive final reports delivered within one (1) week of engagement conclusion, or as otherwise determined by the Participating Entity.

Participating Entity Responsibilities

Access and Authorization Requirements

The Participating Entity is responsible for providing timely access to affected systems, network segments, and relevant personnel necessary for effective incident response. This includes provisioning appropriate user accounts, security clearances, and physical access to facilities where incident response activities will be conducted.

Communication and Coordination Support

The Participating Entity will designate a primary point of contact who can provide rapid decision-making authority and coordinate with internal stakeholders, legal counsel, and external partners as needed throughout the incident response process. This includes facilitating communication with law enforcement when incidents require external reporting or investigation support.

Customer Support and Escalation (Section 3.8)

24x7 Availability and Response

Assurit's customer support framework is designed to provide 24x7 accessibility via toll-free number every day of the year, ensuring qualified customer service representatives can answer all calls within five (5) minute of being placed, as required by Section 3.8.3. Our support staff training program ensures representatives can clearly identify the appropriate method for accessing services for each distinct triggering event and immediately escalate critical incidents to our technical response teams.

Quality Assurance and Service Excellence

All customer interactions are subject to quality monitoring and continuous improvement processes to ensure consistent, professional service delivery that meets the high standards required for government cybersecurity incident response operations.

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.

Category 2 Value-Added Services

Assurit offers specialized value-added services that extend beyond traditional incident response capabilities to address sophisticated cybersecurity threats and enhance organizational incident response maturity. These advanced services leverage our proven expertise in threat hunting, malware analysis, and security operations optimization to deliver targeted solutions that strengthen detection capabilities, improve response times, and build organizational resilience. Each service is designed to address complex threat scenarios that standard incident response may not fully cover, providing organizations with proactive threat detection, automated response capabilities, and enhanced security operations tailored to their unique threat landscape and operational requirements.

Service Name	Description
Threat Hunting & Advanced Persistent Threat (APT) Detection	Proactive threat identification using MITRE ATT&CK framework, custom threat hunting playbooks, behavioral analysis, and advanced malware reverse engineering to identify sophisticated threats.
Tabletop Exercise Design & Facilitation	Custom incident response scenario development based on organization's threat landscape, crisis simulation exercises, and post-exercise improvement planning with lessons learned integration.
Security Operations Center (SOC) Assessment & Optimization	SOC maturity assessment, SIEM tuning and optimization, incident response workflow automation, and performance metrics development to enhance detection and response capabilities.
Advanced Malware Analysis & Reverse Engineering	In-depth malware analysis including behavioral analysis, code reverse engineering, custom signature development, and attribution analysis for sophisticated threats.
Incident Response Automation & Orchestration	Development of automated incident response workflows, playbook automation, and security orchestration platform integration to reduce response times and improve consistency.

Threat Hunting & Advanced Persistent Threat (APT) Detection

Proactive threat identification using MITRE ATT&CK framework, custom threat hunting playbooks, behavioral analysis, and advanced malware reverse engineering to identify sophisticated threats that may evade traditional security controls. This service includes development of custom hunting queries, threat intelligence integration, and continuous monitoring for indicators of compromise specific to the organization's environment and threat profile.

Previous Experience

- **MD THINK:** Implemented advanced threat detection capabilities using sophisticated toolsets, including Sliver C2, Metasploit, and custom PowerShell scripts
- **CFTC:** Conducted comprehensive threat simulation using MITRE ATT&CK framework across network, web applications, and cloud environments
- **FEC:** Developed risk-based vulnerability assessment models focusing on threat severity and mission impact analysis

Tabletop Exercise Design & Facilitation

Custom incident response scenario development based on the organization's threat landscape, crisis simulation exercises, and post-exercise improvement planning with lessons learned integration. This service creates realistic incident scenarios tailored to the organization's specific systems, processes, and threat environment, testing and improving incident response capabilities.

Previous Experience

- **CFTC**: Designed and facilitated cybersecurity assessment exercises aligned with regulatory oversight requirements
- **FEC**: Conducted testing and validation protocols for incident response procedures and vulnerability remediation
- **MD THINK**: Developed comprehensive testing methodologies for incident response validation across complex cloud environments

Security Operations Center (SOC) Assessment & Optimization

SOC maturity assessment, SIEM tuning and optimization, incident response workflow automation, and performance metrics development to enhance detection and response capabilities. This service evaluates current SOC effectiveness, identifies optimization opportunities, and implements improvements to increase operational efficiency and threat detection accuracy.

Previous Experience

- **MD THINK**: Implemented and configured enterprise security monitoring using Splunk, Nessus, TrendMicro, and Wiz for continuous monitoring
- **FEC**: Modernized vulnerability management program with automated intelligence-driven capabilities and enterprise-wide visibility
- **CFTC**: Developed comprehensive monitoring and assessment capabilities for critical trading systems infrastructure

Advanced Malware Analysis & Reverse Engineering

In-depth malware analysis including behavioral analysis, code reverse engineering, custom signature development, and attribution analysis for sophisticated threats. This service provides deep technical analysis of malicious code to understand attack methods, develop custom detection signatures, and provide attribution intelligence for advanced threats.

Previous Experience

- **USMC MCTSSA:** Serving as a critical cybersecurity partner to the Marine Corps Tactical Systems Support Activity (MCTSSA), Assurit provides advanced adversarial testing, reverse engineering, and vulnerability analysis in support of the Advanced Persistent Threat Team (APT2). Our analysts conduct detailed architectural reviews, security boundary assessments, and static/dynamic analysis using advanced tools like Ghidra, GDB, and Immunity. We develop custom exploit frameworks, validate attack vectors through proof-of-concept development, and deliver actionable mitigation guidance tailored to complex Program of Record (PoR) and System of Systems (SoS) environments. Our efforts directly strengthen the cyber resilience of key Marine Corps systems under real-world threat conditions.
- **MD THINK:** Conducted comprehensive forensic analysis using advanced toolsets including Kali Linux, GhostPack, PowerShell, and Burp Suite Pro to identify malicious behaviors and validate exploitability in cloud-hosted infrastructure.

- **Maryland DoIT:** Monitored and analyzed sophisticated threats using open-source intelligence (OSINT), Dark Web reconnaissance, and advanced malware identification to detect indicators of compromise and strengthen statewide cyber defenses.

Incident Response Automation & Orchestration

Development of automated incident response workflows, playbook automation, and security orchestration platform integration to reduce response times and improve consistency. This service creates automated response capabilities that can rapidly contain threats, collect evidence, and coordinate response activities across multiple systems and teams.

Previous Experience

- **FEC**: Implemented automated patch deployment and configuration management for rapid response and remediation
- **MD THINK**: Developed automated security scanning and remediation workflows integrated into CI/CD pipelines
- **CFTC**: Created automated documentation and evidence collection procedures for incident response activities

Additional Labor Categories

Our Category 2 value-added services are supported by specialized labor categories that bring focused expertise in advanced threat detection, security operations optimization, and sophisticated malware analysis. These roles are specifically designed to deliver the enhanced technical, analytical, and operational capabilities required for our advanced incident response service offerings. Each labor category includes both specialist and senior consultant levels to provide appropriate expertise scaling based on threat complexity, organizational maturity, and incident severity. The following labor categories have been developed with specific qualifications and experience requirements to ensure the highest quality service delivery across all value-added incident response areas, enabling organizations to detect, analyze, and respond to the most sophisticated cybersecurity threats.

Labor Category	Role Description	Requirements
Threat Hunter Consultant	Conducts proactive threat hunting activities, develops custom hunting queries, and performs behavioral analysis to identify advanced threats and APTs	• 4+ years cybersecurity experience • SANS GIAC certifications (GCTI, GCFA, or GNFA) • Experience with MITRE ATT&CK framework • Knowledge of threat intelligence platforms • Advanced scripting abilities (Python, PowerShell)
Threat Hunter Senior Consultant	Leads threat hunting operations, develops advanced hunting methodologies, and provides expert guidance on APT detection and attribution analysis	• 7+ years cybersecurity experience • CISSP, CISA, or equivalent advanced certification • Expert-level knowledge of threat hunting methodologies • Experience leading threat hunting teams • Advanced malware analysis and reverse engineering skills
SOC Operations Consultant	Performs SOC assessments, SIEM optimization, workflow automation, and security operations performance analysis	• 5+ years security operations experience • Security+ or equivalent certification • Experience with SIEM platforms (Splunk, QRadar, etc.) • Knowledge of security orchestration tools • Understanding of SOC metrics and KPIs
SOC Operations Senior Consultant	Leads SOC optimization initiatives, develops comprehensive security operations strategies, and provides	• 8+ years security operations experience • CISSP, GCIH, or equivalent advanced certification • Proven experience designing enterprise SOC operations

Labor Category	Role Description	Requirements
	expert guidance on security operations maturity	• Expert knowledge of security automation platforms • Experience with SOC maturity frameworks
Malware Analysis Specialist	Conducts advanced malware analysis, reverse engineering, and signature development for sophisticated threats	• 5+ years malware analysis experience • SANS GIAC certifications (GREM, GNFA) • Advanced reverse engineering skills • Experience with malware analysis tools • Knowledge of multiple programming languages
Malware Analysis Senior Specialist	Leads complex malware analysis efforts, provides attribution analysis, and develops advanced analysis methodologies for APT investigations	• 8+ years malware analysis experience • Multiple advanced certifications (OSCE, OSEE) • Expert-level reverse engineering capabilities • Experience with nation-state threat analysis • Advanced forensic and attribution analysis skills

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.

Federal Election Commission (FEC)

Contract Value	$3,665,841
Performance Period	March 2021 - March 2029 (ongoing)
Client Scale	Independent regulatory agency with approximately 330 employees overseeing campaign finance for federal elections
Systems Scope	Mission-critical systems supporting disclosure of campaign finance data, enforcement, and public transparency
Data Volume	High-volume transactional and disclosure data related to millions of financial records across election cycles
Geographic Coverage	Nationwide oversight of federal campaign finance activity across all U.S. states and territories

Assurit serves as the primary breach coach and incident response coordinator for the Federal Election Commission, providing comprehensive breach response services for one of the nation's most politically sensitive regulatory environments. Our breach coaching services directly fulfill Category 3 requirements:

Crisis Management and Stakeholder Coordination (Section 4.2.1)

- Collaborate with FEC's internal incident response team, legal counsel, and federal law enforcement agencies
- Coordinate breach response activities with external partners, including the DOJ, the FBI, and Congressional oversight committees

- Facilitate crisis management for election-related data breaches during critical election periods
- Engage with public relations firms and media representatives to manage reputation during high-profile incidents

Regulatory Compliance and Notification Determination (Section 4.2.3)

- Determine notification requirements under federal security breach laws specific to election data
- Navigate complex regulatory landscape including FISMA, Privacy Act, and election-specific disclosure requirements
- Coordinate with the Office of Inspector General and the Government Accountability Office reporting requirements
- Ensure compliance with Congressional notification protocols for election infrastructure incidents

Communication Strategy and Notification Support (Section 4.2.4)

- Prepare breach communications for affected individuals, federal regulators, Congress, and media stakeholders
- Develop specialized notification procedures for politically sensitive campaign finance data
- Support crisis communications regarding election integrity and public confidence preservation
- Coordinate with federal partners on unified messaging for election-related security incidents

Maryland Department of Human Services (MD DHS)

Contract Value	$10,420,479
Performance Period	August 2016 - September 2025 (ongoing)
Client Scale	State agency serving 6+ million Maryland citizens through integrated healthcare and human services delivery
Systems Scope	40 Major Applications, 8 General Support Systems across 7,500 virtual cloud instances
Data Volume	Processing millions of eligibility determinations annually across SNAP, Medicaid, Child Welfare, and Temporary Cash Assistance programs
Geographic Coverage:	Statewide service delivery with federal agency integration (Centers for Medicare & Medicaid Services (CMS), Social Security Administration (SSA), Internal Revenue Service (IRS))

Assurit provides comprehensive breach coaching services for the Maryland Total Human-services Integrated Network (MD THINK), managing breach response for one of the nation's largest integrated human services platforms. Our breach coaching services directly fulfill Category 3 requirements:

Multi-Agency Breach Response Coordination (Section 4.2.1)

- Coordinate breach response across federal partners, including CMS, IRS, SSA, and HHS with complex Authority-to-Connect (ATC) requirements
- Manage stakeholder engagement with internal teams, including legal counsel, risk management, IT security, and executive leadership
- Facilitate crisis management for healthcare and human services data affecting vulnerable populations
- Coordinate with external forensic accountants, credit monitoring providers, and specialized healthcare breach response vendors

Healthcare and Human Services Regulatory Navigation (Section 4.2.3 & 4.2.6)

- Determine breach notification requirements under HIPAA Security Rule for protected health information (PHI)
- Navigate federal and state breach notification laws for multiple program types (SNAP, Medicaid, Child Welfare)
- Ensure compliance with IRS Publication 1075 and CMS MARS-E security breach reporting requirements
- Advise on legal consequences under federal healthcare privacy laws and state human services regulations

Vulnerable Population Communication Strategy (Section 4.2.4)

- Develop culturally sensitive breach notifications for diverse populations including non-English speakers
- Create accessible communication materials for individuals with disabilities receiving human services
- Coordinate notification strategies for vulnerable populations including children in state custody and elderly recipients
- Support community outreach through local social services offices and healthcare providers
- These engagements demonstrate Assurit's foundational experience in incident response coordination and crisis management that directly supports Category 3 Breach Coach Services. Our proven methodology encompasses:

Alignment with Category 3 Requirements

- ☑ **Crisis Management and Multi-Stakeholder Coordination:** Demonstrated ability to coordinate breach response across federal agencies, legal counsel, and executive leadership during high-stakes security incidents
- ☑ **Incident Response Team Leadership:** Proven experience leading Computer Security Incident Response Teams (CSIRT) and managing breach response activities for federal law enforcement agencies
- ☑ **Federal Regulatory Compliance Navigation:** Extensive experience working with federal oversight bodies including Department of Justice, Office of Inspector General, and Congressional reporting requirements
- ☑ **Post-Incident Analysis and Improvement Planning:** Comprehensive post-incident review capabilities including root-cause analysis, lessons learned documentation, and organizational improvement recommendations
- ☑ **Risk Communication and Executive Reporting:** Demonstrated ability to translate complex technical incidents into executive-level reports and manage communications with senior leadership during crisis situations
- ☑ **Legal and Regulatory Coordination:** Experience coordinating with federal legal counsel, regulatory bodies, and law enforcement during sensitive security incidents affecting government operations

While Assurit's documented breach coaching experience is primarily from our federal law enforcement engagement, our comprehensive incident response expertise, regulatory compliance knowledge, and crisis management capabilities provide a strong foundation for Category 3 services. Our team's proven ability to coordinate complex stakeholder responses, navigate federal regulatory requirements, and manage high-stakes incidents positions us to effectively support NASPO ValuePoint participating entities in developing and implementing comprehensive breach response strategies that meet all legal and regulatory requirements.

(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.

Experience and Qualifications

Assurit's Category 3 Breach Coach Services are built upon highly qualified cybersecurity and legal professionals who significantly exceed the minimum requirements outlined in Attachment 02, Section 4.3. Our current team leadership establishes the methodology, quality standards, and technical approach for all breach response activities.

Foundation of Excellence Through Current Team Leadership

Our Category 3 services are led by senior professionals with extensive experience and advanced certifications, ensuring exceptional deliverables. Mr. Thang Pham, our CTO and Vice President, brings 20+ years of information security experience with a Master's degree in Applied Information Technology (Cyber Security). His certifications include CISSP, CISM, CISA, CGRC, PMP, OSCE3, OSCP, GPEN, and GWAPT. Critically, Mr. Pham served as Cyber Incident Response Manager for the Bureau of Alcohol, Tobacco, Firearms & Explosives (ATF), where he led the bureau's Computer Security Incident Response Team (CSIRT) and managed breach response coordination across federal law enforcement agencies.

Mr. Andy Lien, Cloud Security Engineer, provides 10 years of cybersecurity experience with certifications including CISSP, CGRC, CCSK, and AWS Solutions Architect, specializing in security governance, incident response coordination, and regulatory compliance frameworks essential for breach coach services.

Staff Qualification Requirements

Breach Coach Role

Assurit requires personnel with five or more years of professional experience in cybersecurity incident response, legal compliance, or breach management, with demonstrated expertise in coordinating multi-stakeholder breach response activities. Our Breach Response Specialists must possess comprehensive knowledge of federal and state breach notification laws, privacy regulations, and crisis management protocols. Technical capabilities must include subject matter expertise in assisting organizations navigate cyber response and recovery processes, experience isolating affected data and determining breach scope, comprehensive knowledge of incident breach reporting requirements, expertise in customer notification strategies, experience retaining and coordinating with forensics professionals, and demonstrated ability in managing crisis communications during high-stakes security incidents.

Required certifications include one advanced security certification such as CISSP, CISM, CISA, or CGRC, plus incident response certification such as GCIH or GCFA. Preferred additional certifications include CIPP/US, CIPM, PMP, and privacy law certifications. Areas of specialization include incident response planning and cyber security awareness program development, regulatory compliance across federal and state breach notification requirements, crisis communication and reputation management, legal coordination with counsel and regulatory bodies, and risk mitigation strategies to prevent future incidents.

Professional Development and Quality Assurance

Assurit maintains rigorous standards requiring all Category 3 staff to maintain professional certifications through continuing education and complete 40 hours of annual breach response and legal compliance training. Our team actively participates in industry conferences, legal seminars, and privacy law updates, staying current with

evolving breach notification requirements, emerging privacy regulations, and advancing crisis management practices.

Our quality assurance process includes a legal review by qualified privacy law professionals, technical validation by certified incident response professionals, regulatory compliance verification against current federal and state requirements, and final approval by team leaders with over 10 years of experience in breach management. We maintain standardized breach response procedures based on NIST SP 800-61 and industry best practices, with regular updates to our methodology reflecting the evolving legal landscape and regulatory changes. This comprehensive approach ensures consistent delivery of Category 3 services that exceed client expectations while maintaining the highest professional and legal standards for breach response coordination and crisis management.

(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.

Category 3 Service Level Agreements

Assurit is committed to delivering Category 3 Breach Coach Services with clearly defined service levels that ensure rapid response, expert guidance, and transparent communication during critical security incidents. Our Service Level Agreements (SLAs) are designed to meet the specific requirements outlined in the Scope of Work while providing the urgent response capabilities essential for effective breach management.

Service Initiation and Response Times

Initial Response and Breach Assessment

Upon notification by a Participating Entity of a potential triggering event, Assurit will provide initial acknowledgment within two (2) hours during standard business hours (8:00 AM to 6:00 PM ET, Monday through Friday) or within four (4) hours for notifications received outside standard hours. Our Breach Coach will conduct an initial assessment call within four (4) hours as specified in Section 4.1.3 of the Scope of Work to evaluate the situation, determine preliminary scope, and provide initial guidance on next steps.

- **Standard Breach Events**: For typical data security incidents, Assurit will provide a comprehensive breach response plan, including stakeholder coordination strategy, notification timelines, and resource requirements, within eight (8) hours of confirming a triggering event has occurred.
- **Critical/High-Profile Events**: For incidents involving high-visibility data, election systems, healthcare information, or those requiring immediate public response, we will expedite this process and provide initial breach response strategies within **four (4) hours**, with continuous support available as needed.

Resource Deployment and Team Assignment

Assurit will assign qualified Breach Response Specialists meeting the requirements specified in Section 4.3 within four (4) hours of breach confirmation. For on-site breach response support, our team will be available to deploy within one (1) business day as specified in Section 4.1.4, or as mutually agreed in the Order. In cases where immediate deployment is required, we will make our best efforts to accommodate same-day response while ensuring all personnel meet the specified qualifications.

Service	Commitment	Responsible Party
Initial acknowledgment of the triggering event	2 hours (business) / 4 hours (after hours)	Assurit
Initial assessment call with client	4 hours	Assurit
Breach response plan (standard events)	8 hours	Assurit
Breach response plan (critical events)	4 hours	Assurit
Qualified Breach Coach assignment	4 hours	Assurit
On-site team deployment	1 business day	Assurit

Breach Response Execution and Coordination

Continuous Communication and Stakeholder Management

Throughout the breach response, Assurit will provide daily status updates during active incident periods, detailing response progress, coordination activities with external partners, regulatory compliance status, and upcoming critical milestones. These updates will be delivered by 6:00 PM ET via secure communication channels to designated Participating Entity contacts, with additional real-time updates provided as circumstances warrant.

For complex breach incidents extending beyond 72 hours, Assurit will conduct twice-daily coordination calls with Participating Entity stakeholders to discuss findings, address emerging issues, and ensure alignment with legal and regulatory requirements. These calls will include breach response specialists, legal coordination staff, and client representatives as appropriate.

Crisis Management and Escalation

Any critical developments that may impact notification timelines, legal compliance, or public response will be escalated to the Participating Entity immediately upon identification. Assurit will provide recommended response strategies and work collaboratively with internal legal counsel, executive leadership, and external partners to ensure optimal incident management. For issues requiring immediate legal or regulatory action, notification will be provided within one (1) hour during business hours or immediately for after-hours critical situations.

Service	Commitment	Responsible Party
Daily status updates (active incidents)	Daily by 6:00 PM ET	Assurit
Coordination calls (complex incidents >72 hours)	Twice daily as scheduled	Both Parties
Critical development escalation	Immediate	Assurit
Legal/regulatory issue notification	1 hour (business) / Immediate (critical)	Assurit
Daily status updates (active incidents)	Daily by 6:00 PM ET	Assurit
Coordination calls (complex incidents >72 hours)	Twice daily as scheduled	Both Parties

Deliverable Standards and Timeline Commitments

Notification Strategy and Legal Compliance

For incidents requiring breach notifications, Assurit will provide preliminary notification strategies and legal compliance assessments within 12 hours of breach scope determination. Final notification templates, regulatory filing requirements, and communication timelines will be delivered within 24 hours of completing impact assessment, ensuring compliance with all applicable federal and state notification deadlines.

Documentation and Reporting

Assurit will maintain continuous documentation of all breach response activities, stakeholder communications, and decision points throughout the incident lifecycle. Interim summary reports will be provided within 24 hours of key milestones, including breach scope confirmation, notification decisions, and regulatory filings. Comprehensive post-incident reports, including lessons learned and improvement recommendations, will be delivered within five (5) business days of incident closure.

Legal Coordination and Regulatory Support

All legal strategies and regulatory compliance recommendations undergo review by qualified legal professionals before delivery to ensure accuracy and compliance with current requirements. Should the Participating Entity request revisions to notification strategies or legal assessments, Assurit will provide revised materials within four (4) hours for time-sensitive items or 24 hours for comprehensive strategy updates.

Service	Commitment	Responsible Party
Preliminary notification strategy	12 hours after scope determination	Assurit
Final notification templates and compliance	24 hours after impact assessment	Assurit
Interim milestone reports	24 hours after key milestones	Assurit
Comprehensive post-incident reports	5 business days after closure	Assurit
Time-sensitive strategy revisions	4 hours	Assurit
Comprehensive strategy updates	24 hours	Assurit

Contractor Responsibilities and Commitments

Personnel and Expertise Standards

Assurit commits to providing only qualified Breach Response Specialists who meet or exceed the minimum qualifications specified in Section 4.3. All assigned personnel will maintain current certifications in incident response, legal compliance, and crisis management, with demonstrated experience in breach notification laws and regulatory requirements. We guarantee that all Breach Coaches will possess appropriate legal knowledge and incident response certifications.

Legal and Regulatory Compliance

Our breach response activities will be conducted in accordance with all applicable federal and state breach notification laws, privacy regulations, and sector-specific requirements as specified in the Statement of Work. All response strategies will comply with current legal standards including HIPAA, Privacy Act, state breach notification statutes, and other relevant regulatory frameworks.

Confidentiality and Crisis Management

Assurit will maintain the highest standards of confidentiality throughout the breach response, implementing appropriate safeguards for sensitive incident information following the security requirements specified in Section 1 of the Scope of Work. All personnel will execute appropriate non-disclosure agreements and comply with crisis communication protocols established by the Participating Entity.

Service	Commitment	Standard
Qualified personnel provision	Meet or exceed Section 4.3 requirements	100% compliance
Legal certification maintenance	Current incident response and legal certifications	Ongoing requirement
Regulatory compliance	Federal and state breach notification laws	Per applicable regulations
Confidentiality and crisis management	Highest security standards per Section 1	Continuous compliance
Quality assurance	Legal review of all breach strategies	100% of deliverables
Qualified personnel provision	Meet or exceed Section 4.3 requirements	100% compliance

Participating Entity Responsibilities

Access and Information Provision

The Participating Entity is responsible for providing immediate access to incident information, affected systems, and key personnel necessary for breach assessment activities. This includes coordinating with legal counsel, executive leadership, and technical teams, providing incident details and system logs as available, and ensuring the availability of decision-makers during critical response periods.

Decision-Making and Approval Authority

To maintain rapid response capabilities, the Participating Entity agrees to provide decision authority or designated representatives who can approve notification strategies, legal filings, and public communications within established timeframes. Critical breach response decisions should be made within four (4) hours when specifically identified, with routine approvals provided within 12 hours of recommendation delivery.

Communication and Coordination Support

The Participating Entity will coordinate with internal stakeholders including legal counsel, public relations teams, and executive leadership to ensure unified breach response. Any significant changes to incident scope, legal requirements, or organizational priorities should be communicated immediately to avoid impact on response strategies and compliance timelines.

Service	Commitment	Timeframe
Incident information and system access	Provide immediate access per breach scope	As required for response
Key personnel coordination	Ensure availability of decision-makers	During critical response periods
Critical decision approval	Approve time-sensitive strategies	4 hours
Routine decision approval	Approve standard recommendations	12 hours
Internal stakeholder coordination	Coordinate legal, PR, and executive teams	Ongoing

Service	Commitment	Timeframe
Scope/priority change notification	Communicate changes immediately	Upon occurrence

Performance Metrics and Continuous Improvement

Quality Metrics and Response Effectiveness

Assurit tracks performance metrics including response time compliance, legal accuracy, stakeholder satisfaction, and incident resolution effectiveness to ensure continuous improvement in breach response delivery. We maintain a target of 100% compliance with all response time commitments and conduct post-incident client satisfaction surveys to identify opportunities for improvement.

Flexibility and Crisis Adaptation

While maintaining firm commitments to rapid response and legal compliance, Assurit recognizes that breach incidents are dynamic situations requiring adaptive strategies. We will work collaboratively to accommodate evolving incident scope, changing legal requirements, or emerging stakeholder needs while maintaining the integrity of the breach response process and ensuring all deliverables meet established quality and legal standards.

Service	Target/Commitment	Measurement
Response time compliance	100% compliance	All SLA commitments
Legal accuracy	Post-incident review	Each completed engagement
Stakeholder satisfaction	Post-incident survey	Each breach response
Incident resolution effectiveness	Comprehensive assessment	Resolution success and compliance
Crisis adaptation capability	Collaborative flexibility	Reasonable adjustments as needed

These Service Level Agreements reflect Assurit's commitment to excellence in Category 3 Breach Coach Services while establishing clear expectations and responsibilities for successful incident response outcomes. We view these SLAs as critical for protecting Participating Entities during their most vulnerable moments and remain committed to exceeding these standards whenever possible.

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.

Category 3 Value-Added Services

Assurit offers specialized value-added services that extend beyond traditional breach coaching activities to address the complex crisis management and regulatory challenges facing modern organizations during and after security incidents. These advanced services leverage our proven expertise in federal incident response, multi-stakeholder coordination, and regulatory compliance to deliver targeted solutions that enhance breach response capabilities and organizational resilience. Each service is designed to address specific gaps that standard breach coaching may not fully cover, providing organizations with comprehensive crisis management strategies, regulatory alignment, and recovery roadmaps tailored to their unique operational requirements and threat landscape.

Service	Commitment
Multi-Jurisdiction Regulatory Notification Strategy	Comprehensive breach notification planning across federal, state, and international jurisdictions with regulatory timeline coordination, notification template development, and compliance verification.
Third-Party Breach Impact Assessment	Supply chain breach impact analysis, vendor breach notification coordination, customer/partner communication strategy, and business relationship preservation planning.
Executive Leadership Coaching During Crisis	C-suite crisis leadership development, decision-making frameworks during breach events, board communication strategies, and stakeholder confidence maintenance.
Post-Breach Security Program Redesign	Comprehensive security program enhancement based on breach lessons learned, policy revision, control implementation, and organizational culture change management.
Business Continuity & Recovery Planning	Post-breach business operations restoration, customer trust rebuilding strategies, revenue recovery planning, and long-term reputation management.

Multi-Jurisdiction Regulatory Notification Strategy

This service provides comprehensive breach notification planning across complex regulatory landscapes involving federal, state, and international jurisdictions. We develop coordinated notification strategies that address varying timeline requirements, content specifications, and regulatory expectations across multiple jurisdictions. The service includes regulatory timeline mapping, notification template development for different jurisdictions, compliance verification processes, and coordination with international data protection authorities. We provide detailed regulatory analysis for cross-border data incidents and develop unified notification strategies that satisfy all applicable requirements.

Previous Experience

- **MD THINK**: Coordinated breach notification requirements across federal partners including CMS, IRS, SSA, and HHS with varying compliance standards
- **FEC**: Developed notification strategies for politically sensitive data with federal regulatory and Congressional reporting requirements
- **CFTC**: Managed regulatory compliance verification for federal cybersecurity oversight requirements

Third-Party Breach Impact Assessment

This service provides a comprehensive evaluation of breach impacts on vendor relationships, supply chain operations, and business partnerships. We assess third-party notification obligations, evaluate vendor security postures following supply chain incidents, and develop customer/partner communication strategies to preserve business relationships. The service includes vendor breach coordination protocols, business relationship impact analysis, supply chain risk reassessment, and ongoing monitoring processes for affected partnerships.

Previous Experience

- **MD THINK**: Evaluated breach impact across federal agency partnerships and state vendor relationships for integrated human services platform
- **FEC**: Assessed vendor security capabilities and breach notification requirements as part of vulnerability management modernization
- **CFTC**: Conducted compliance verification activities involving multiple regulatory oversight bodies

Executive Leadership Coaching During Crisis

This service provides specialized coaching for C-suite executives and senior leadership during high-stakes breach events. We develop decision-making frameworks for crisis situations, provide board communication strategies, and offer guidance on maintaining stakeholder confidence during incidents. The coaching includes crisis leadership development, media engagement preparation, investor/stakeholder communication, and organizational confidence maintenance strategies. We provide real-time advisory support during active incidents and post-incident leadership assessment.

Previous Experience

- **MD THINK**: Coordinated with state executive leadership and federal partners during security incidents affecting critical public services
- **FEC**: Provided strategic recommendations and governance support for federal cybersecurity program management
- **CFTC**: Delivered executive briefings and strategic recommendations for regulatory oversight bodies during cybersecurity assessments

Post-Breach Security Program Redesign

This service offers comprehensive security program enhancement based on breach lessons learned and incident analysis. We evaluate existing security controls, policies, and procedures in light of incident findings and develop enhanced security frameworks to prevent similar incidents. The service includes security policy revision, control implementation planning, organizational culture change management, and ongoing security program maturity assessment. We provide implementation roadmaps, training programs, and continuous improvement processes based on incident learnings.

Previous Experience

- **MD THINK**: Implemented comprehensive security control enhancements and policy revisions based on continuous monitoring findings
- **FEC**: Established enhanced vulnerability management and HVA programs based on security assessment recommendations
- **CFTC**: Provided strategic advisory services for cybersecurity program improvements and federal compliance alignment

Business Continuity & Recovery Planning

This service provides comprehensive planning for business operations restoration, customer trust rebuilding, and long-term reputation management following security incidents. We develop recovery strategies that address operational continuity, revenue recovery planning, customer communication, and brand reputation restoration. The service includes business impact analysis, recovery timeline development, customer retention strategies, and ongoing reputation monitoring. We provide stakeholder communication frameworks, competitive positioning strategies, and long-term trust rebuilding initiatives.

Previous Experience

- **MD THINK**: Supported continuous operations for critical human services affecting millions of Maryland citizens during security incidents and system modifications
- **FEC**: Maintained election integrity operations and public confidence during cybersecurity program modernization and assessment activities
- **CFTC**: Ensured regulatory oversight continuity during cybersecurity assessments and compliance verification activities

Additional Labor Categories

Our Category 3 value-added services will be supported by specialized labor categories that bring focused expertise to complex crisis management and breach response challenges. These roles are specifically designed to deliver the advanced legal, communication, and organizational capabilities required for our enhanced service offerings. Each labor category includes both consultant and senior levels to provide appropriate expertise scaling based on incident complexity and organizational needs.

Labor Category	Role Description	Requirements
Crisis Communication Consultant	Supports crisis communication strategy development, stakeholder messaging, media response coordination, and reputation management activities during security incidents	• 3+ years in crisis communication or public relations • Experience with cybersecurity incident communication • Knowledge of media relations and stakeholder management • Strong written and verbal communication skills • Understanding of regulatory communication requirements
Crisis Communication Senior Consultant	Leads complex crisis communication strategies, develops comprehensive messaging frameworks, and provides expert guidance on high-stakes incident communication and reputation management	• 7+ years in crisis communication and reputation management • Expert knowledge of cybersecurity incident communication • Proven experience managing high-profile crises • Advanced media relations and stakeholder engagement skills • Experience with regulatory and legal communication requirements
Legal Compliance Consultant	Supports breach notification analysis, regulatory requirement interpretation, legal risk assessment, and compliance documentation activities	• 3+ years in legal compliance or privacy law • Knowledge of breach notification laws and privacy regulations • Experience with regulatory compliance documentation • Understanding of cybersecurity legal frameworks • Strong analytical and legal research skills
Legal Compliance Senior Consultant	Leads complex multi-jurisdiction compliance analysis, develops comprehensive legal strategies, and provides expert guidance on regulatory requirements and legal risk management	• 7+ years in privacy law, cybersecurity law, or regulatory compliance • CIPP/US, CIPM, or equivalent privacy certification • Expert knowledge of breach notification laws across jurisdictions • Experience with complex regulatory compliance strategies • Proven ability to lead legal compliance initiatives
Business Recovery Consultant	Supports business continuity planning, operational recovery strategies, stakeholder relationship management, and organizational resilience activities	• 3+ years in business continuity or crisis management • Knowledge of business recovery methodologies • Experience with operational continuity planning • Understanding of stakeholder management principles • Strong project management and coordination skills
Business Recovery Senior Consultant	Leads comprehensive business recovery strategies, develops organizational resilience frameworks, and provides expert guidance on long-term recovery and reputation restoration	• 7+ years in business continuity, crisis management, or organizational recovery • CBCP, MBCP, or equivalent business continuity certification • Expert knowledge of crisis recovery and reputation management • Experience developing enterprise resilience programs • Proven ability to lead complex recovery initiatives

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.
- **(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.
- **(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.
- **(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.
- **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.

Assurit does not intend to pursue Category 4 – Notification and Credit Monitoring Services under this solicitation. We are focusing our capabilities and proposal on Categories 1 through 3, where our experience and service offerings align most closely with the scope and requirements outlined in the RFP.

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).

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.

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.

Assurit does not intend to use subcontractors for any services under this Master Agreement. We will provide all cybersecurity and information security services directly through our own expert staff and resources. This direct service delivery model ensures consistent quality, unified accountability, and seamless integration across all service categories.

Our decision to provide all services directly is supported by our robust internal capabilities, including a team of nationwide cybersecurity professionals with relevant federal experience and comprehensive certifications (CISSP, CISM, CISA, GPEN, OSCP, and other specialized credentials). We maintain a robust recruitment division and a national talent network that enables us to scale resources rapidly and deploy specialized expertise to meet the varying project demands of our participating entities. This approach ensures that Participating Entities receive the full benefit of Assurit's expertise and accountability while maintaining direct oversight and quality control over all service delivery.

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. Provide the approximate dollar value of the business' 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.

Experience with Large Contract Vehicles and Consortium Agreements

Assurit has extensive experience working with large contract vehicles and consortium agreements that serve multiple entities across state and federal jurisdictions. We are currently positioned on several major contract vehicles including GSA Multiple Award Schedule (MAS), SBA 8(a) STARS III, and Navy Seaport Next Generation (NxG). Additionally, we maintain active contracts on the Baltimore, MD ITCATS contract vehicle, GSA eFAST, and hold a position on the Georgia Technology Authority IT Cybersecurity Blanket Purchase Agreement (BPA). This diverse portfolio of contract vehicles demonstrates our proven ability to navigate complex procurement processes, meet stringent qualification requirements, and deliver consistent value across multiple jurisdictions and entity types.

Our experience spans the full lifecycle of large consortium contracts, from initial proposal development and award through ongoing contract management and performance. We have successfully competed for and won multiple contracts exceeding $1 million in value, demonstrating our capability to scale operations and deliver comprehensive cybersecurity services to large-scale initiatives. Our contract management approach emphasizes flexibility, responsiveness, and collaborative partnerships with contracting entities to ensure mission success.

Largest Contracts in the Last Five Years

Maryland Department of Human Services - MD THINK

- **Contract Value:** $10,420,479
- **Period of Performance:** August 2016 - September 2025
- **Services:** Comprehensive cybersecurity program including risk assessment and mitigation, incident response capabilities, vulnerability management, and security assessment and authorization services across a $200M cloud modernization initiative serving millions of Marylanders

Federal Election Commission - Vulnerability Management & High Value Asset Program

- **Contract Value:** $3,665,841
- **Period of Performance:** March 2021 - March 2029

- **Services:** Modernization of vulnerability management programs, development and implementation of High Value Asset (HVA) programs, risk assessment and mitigation services, and ongoing security governance supporting critical election infrastructure

U.S. Marine Corps - MCTSSA Advanced Persistent Threat Support

- **Contract Value:** $1,364,178
- **Period of Performance:** July 2024 - Present
- **Services:** Advanced vulnerability assessment, penetration testing, incident response support, and security assessment services for critical Marine Corps tactical systems and Program of Record (PoR) systems

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

Marketing Strategy for Master Agreement Participation

Leveraging Existing State Relationships

Assurit's marketing approach builds upon our established presence and proven track record with state governments. We currently hold active contracts with Virginia and Maryland, including our significant $10.4M engagement with the Maryland Department of Human Services. These existing relationships provide a strong foundation for expanding participation, as we can leverage our demonstrated success and deep understanding of state-specific cybersecurity challenges to encourage adoption among peer jurisdictions.

Our strategy includes utilizing our current state clients as reference partners, facilitating knowledge-sharing sessions where we can showcase real-world case studies and lessons learned from successful implementations. Through our work across multiple states, we have gained valuable insights into the common cybersecurity challenges facing state and local governments, enabling us to articulate clear value propositions that resonate with potential participating entities.

Comprehensive Marketing Approach

Our marketing strategy encompasses multiple channels and touchpoints to maximize Master Agreement visibility and adoption:

- **Direct Outreach and Relationship Building:** We will conduct targeted outreach to state CISOs, IT directors, and procurement officials through our existing professional networks and industry relationships. Our team will participate in key conferences such as NASCIO, HIMSS, and state-specific IT leadership forums to build awareness and demonstrate our capabilities.
- **Educational Content and Thought Leadership:** We will develop and distribute educational content, including white papers, webinars, and case studies that highlight cybersecurity best practices and demonstrate the value of cooperative purchasing for cybersecurity services. This content will be tailored to address specific challenges facing state and local governments.
- **Partnership Development:** We will establish strategic partnerships with system integrators, technology vendors, and other service providers who work with state and local governments to expand our reach and create referral opportunities. These partnerships will help us access new markets while providing comprehensive solutions to participating entities.
- **Digital Marketing and Online Presence:** We will maintain an updated website dedicated to the Master Agreement, featuring entity-specific resources, success stories, and easy access to contracting information. We will utilize targeted digital advertising and social media engagement to reach key decision-makers in target jurisdictions.

- **Regional and Industry Events:** We will sponsor and participate in regional government technology events, cybersecurity conferences, and procurement fairs to build relationships and directly demonstrate our capabilities to potential participants.

Through this multi-faceted approach, we will build awareness of the Master Agreement's value proposition while establishing Assurit as the preferred cybersecurity partner for state and local government entities seeking comprehensive, cost-effective security solutions.

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.

Dedicated Master Agreement Website Features

Existing Platform and Customization Experience

Assurit already maintains dedicated websites for each of our current contract vehicles, providing us with proven experience in developing and managing contract-specific online platforms. Building upon this established foundation, we will create a comprehensive, user-friendly website specifically designed for this NASPO ValuePoint Master Agreement. Our existing platform architecture allows us to rapidly deploy and customize new contract-specific sites while maintaining consistent branding and functionality across all our contract vehicles.

Core Website Features and Functionality

Our dedicated Master Agreement website will include several key features designed to streamline the procurement process and enhance user experience:

- **Customized Price Lists:** The website will feature secure, entity-specific pricing sections that provide each Participating Entity with their customized price lists for all applicable service categories. These pricing modules will be regularly updated to reflect any authorized pricing adjustments and will include clear breakdowns of hourly rates, value-added services, and volume discounts where applicable.
- **Comprehensive Staff Contact Information:** We will maintain current contact information for all key personnel, including our Contract Manager, technical leads for each service category, and regional points of contact. This directory will include direct phone numbers, email addresses, and availability schedules to ensure Participating Entities can quickly connect with the appropriate Assurit representatives.
- **Resource Library:** The site will house essential contract documents, including the Master Agreement, Participating Addendum templates, technical specifications, compliance documentation, and case studies from similar engagements. All documents will be organized by service category and easily searchable.
- **Online Ordering Capabilities:** If online ordering functionality is available and applicable for cybersecurity services, we will develop and implement the necessary e-commerce components on our website. This capability will be designed to accommodate the unique requirements of cybersecurity service procurement, including statement of work development tools, secure document exchange, and automated approval workflows. The online ordering system will be readily available to all participating entities that require this functionality.
- **Performance Reporting and Transparency:** The website will include sections for performance metrics, customer testimonials, and project updates to demonstrate ongoing value delivery and maintain transparency with all stakeholders.

This comprehensive web platform will serve as a central hub for all Master Agreement activities, ensuring participating entities have easy access to pricing, personnel, and procurement resources necessary for successful engagement with Assurit's cybersecurity services.

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.

Staff Allocation and Training for Master Agreement Management

Dedicated Administrative and Management Resources

Assurit will allocate our experienced administrative staff to manage all aspects of the Master Agreement, leveraging the same team that currently oversees our portfolio of contract vehicles including GSA MAS, 8(a) STARS III, Navy Seaport NxG, and other consortium agreements. This dedicated team brings decades of collective experience in contract administration, compliance management, and customer relationship management across multiple contract vehicles.

Our administrative staff includes specialists in contract compliance, pricing management, reporting requirements, and customer service coordination. This team has demonstrated expertise in managing complex multi-entity agreements, ensuring consistent adherence to contract terms, and maintaining the detailed documentation and reporting required for large consortium contracts. Their proven track record across our existing contract vehicles provides confidence in their ability to effectively manage the unique requirements of this NASPO ValuePoint Master Agreement.

Comprehensive Staff Training Program

We will implement a multi-faceted training program to ensure all Assurit personnel are thoroughly familiar with Master Agreement terms, pricing structures, and compliance requirements:

- **Direct Training Sessions:** Our administrative team will conduct formal training sessions for all staff who may interact with Participating Entities. These sessions will cover Master Agreement terms and conditions, pricing structures for each service category, compliance requirements, and proper procedures for engaging with participating entities. Training will be mandatory for all project managers, technical leads, and customer-facing personnel.
- **Company-Wide Knowledge Management:** We will develop and maintain a comprehensive wiki system accessible to all staff, providing on-demand access to Master Agreement information, pricing guidelines, compliance checklists, and frequently asked questions. This centralized knowledge repository will be regularly updated to reflect any contract modifications or clarifications, ensuring all staff have access to current information.
- **Semi-Annual Review and Update Meetings:** We will conduct company-wide meetings twice yearly to discuss Master Agreement performance, contract changes, new opportunities, and lessons learned. These meetings will include updates on pricing adjustments, new participating entities, regulatory changes, and best practices for service delivery under the Master Agreement.
- **Ongoing Compliance Monitoring:** Our administrative team will implement regular compliance audits and refresher training to ensure continued adherence to all Master Agreement requirements. This includes monitoring of pricing accuracy, proper invoicing procedures, reporting compliance, and customer service standards.

This comprehensive approach ensures that all Assurit personnel understand their roles and responsibilities under the Master Agreement while maintaining the high service standards that have characterized our performance on existing contract vehicles.

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

Innovative Strategies for Master Agreement Adoption and Usage

Value Demonstration Through Pilot Programs

Assurit will offer "Cybersecurity Health Check" pilot programs to potential Participating Entities, providing limited-scope vulnerability assessments or security posture evaluations at reduced rates through the Master Agreement. These pilots enable entities to experience our service quality firsthand, demonstrating immediate value. By showcasing tangible results and our collaborative approach, these pilot programs serve as powerful catalysts for adoption, converting interest into active participation.

Peer-to-Peer Success Showcases

We will establish a "Cybersecurity Champions Network" connecting CISOs and IT directors from participating entities to share experiences, best practices, and lessons learned. Through quarterly virtual roundtables and annual in-person symposiums, we facilitate knowledge sharing that goes beyond our services to create genuine professional value. When peers hear directly from their counterparts about successful implementations and measurable security improvements, adoption naturally follows through trusted professional networks.

Flexible Engagement Models and Risk Mitigation

Recognizing that cybersecurity needs vary dramatically across entities, we will offer "Security-as-a-Service" subscription models that allow participating entities to access our expertise on an ongoing basis rather than project-by-project. This includes monthly security consultation hours, incident response retainers, and continuous monitoring services that provide predictable budgeting while ensuring immediate access to expertise when needed. For entities hesitant about large commitments, we offer performance guarantees and outcome-based pricing models that align our success with their security improvements.

Technology-Enabled Efficiency and Transparency

We will develop a "Cybersecurity Dashboard" platform accessible to all participating entities, providing real-time visibility into industry threat landscapes, regulatory updates, and peer benchmarking data. This platform includes automated procurement tools that streamline the ordering process, reducing administrative burden while providing valuable intelligence. By making our Master Agreement the most efficient and informative way to access cybersecurity services, we create competitive advantages that drive adoption.

Strategic Partnership and Bundle Opportunities

We will create strategic alliances with complementary service providers on other NASPO ValuePoint contracts, offering integrated solutions that leverage multiple Master Agreements. For example, partnering with IT infrastructure or software licensing contractors to provide comprehensive "cyber-secure technology implementations" that address multiple procurement needs through coordinated Master Agreement usage. This approach positions our contract as part of a larger efficiency strategy rather than an isolated cybersecurity purchase.

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?)

Approach to Participating Addenda Negotiation

Flexible and Collaborative Negotiation Philosophy

Assurit approaches Participating Addenda negotiations with a flexible, entity-centric philosophy that recognizes each participating entity faces unique operational requirements, regulatory environments, and organizational challenges. We understand that state and local governments operate under diverse statutory frameworks, procurement regulations, and administrative procedures that must be reflected in their contracting documents. Our approach prioritizes collaborative problem-solving to ensure each entity receives the specific protections and provisions they require while maintaining the integrity of the Master Agreement framework.

We work in good faith with each entity to negotiate Participating Addenda that meet their specific needs while ensuring we can deliver high-quality cybersecurity services effectively. Our goal is to create mutually beneficial agreements that provide entities with the flexibility they need while establishing clear frameworks for successful service delivery. We recognize that rigid contract terms often hinder effective partnerships, so we emphasize adaptability and creative solutions during negotiations.

Entity-Specific Language and Statutory Requirements

Assurit provides significant flexibility for entities to incorporate entity-specific language into their Participating Addenda. We do not require entities to provide statutory citations for their entity-specific language, though we appreciate when such citations are provided as they help us better understand the underlying requirements and ensure our proposed modifications align with the entity's legal framework. Our experience across multiple state contracts has taught us that legal requirements vary significantly between jurisdictions, and we respect each entity's expertise regarding their own compliance obligations.

When entities propose specific language modifications, our team reviews each request to understand the underlying business or legal requirement and works collaboratively to find acceptable solutions. We maintain access to legal counsel who can quickly review complex provisions and provide guidance on acceptable modifications that protect both parties' interests.

Resource Allocation for Multiple Simultaneous Negotiations

Assurit has the capability and resources to devote to simultaneous negotiation of multiple Participating Addenda. Our administrative team includes experienced contract professionals who can manage parallel negotiation processes efficiently while maintaining attention to each entity's specific requirements. We have established internal workflows and review processes that allow us to handle multiple negotiations without compromising quality or responsiveness.

Our approach includes dedicated project management for each negotiation, ensuring each entity receives focused attention and timely responses throughout the process. We also maintain template libraries and precedent databases from our existing contract vehicles that help streamline negotiations while preserving the customization necessary for each entity's unique requirements.

This resource commitment ensures that interested entities can move forward with Participating Addenda development on their preferred timelines without being delayed by our capacity constraints or competing priorities from other negotiations.

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

Immediate Service Delivery Capability

Proven Track Record of Rapid Deployment

Assurit is fully capable of providing cybersecurity services immediately upon execution of a Master Agreement and Participating Addenda. Our decade of experience working with government agencies has honed our ability to meet aggressive timelines and start dates, developing streamlined processes that enable rapid service initiation without compromising quality or compliance requirements.

Our proven capability is demonstrated through real-world examples such as our recent USDA contract award, where we were selected within a one-week period and successfully initiated service delivery just two weeks after contract signing during the official contract start and onboarding period. This rapid deployment was achieved through our proactive approach to resource allocation and our established operational frameworks that can be quickly adapted to new client requirements.

Strategic Resource Management and Early Identification

Our ability to provide immediate services stems from our strategic approach to talent management and resource allocation. We continuously identify and vet qualified candidates throughout our recruitment process, maintaining a ready pool of cleared and certified cybersecurity professionals who can be rapidly deployed to new engagements. This proactive talent pipeline allows us to respond to immediate staffing needs without the typical delays associated with candidate sourcing and security clearance processing.

We begin the onboarding and vetting process as early as possible in the procurement cycle, conducting preliminary assessments of potential resource requirements and pre-positioning qualified personnel based on anticipated needs. This forward-thinking approach ensures that when a Participating Entity is ready to begin services, we can transition seamlessly from contract execution to active service delivery.

Agile Operational Framework

Assurit maintains agile operational processes specifically designed to accommodate the varied and often urgent needs of government cybersecurity requirements. Our established methodologies, proven project management frameworks, and flexible staffing models allow us to rapidly scale up or down based on immediate client demands. We maintain standardized operating procedures that can be quickly customized to meet entity-specific requirements while ensuring consistent service quality and compliance with all applicable regulations.

Our operational agility extends to our technology platforms, security tools, and administrative systems, which are designed for rapid configuration and deployment across new client environments. This comprehensive readiness ensures that Participating Entities can access our full range of cybersecurity services immediately upon contract execution, enabling them to address urgent security needs without delay.

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.

Sales Reporting and Partner Compliance Management

Direct Service Delivery Model Ensures Complete Reporting

Assurit's approach to sales reporting compliance is fundamentally simplified by our direct service delivery model. As we do not utilize dealers, partners, or resellers for service delivery under this Master Agreement, all sales transactions flow directly through Assurit's internal systems, ensuring 100% visibility and control over all sales data. This direct model eliminates the common challenges associated with partner reporting compliance, data aggregation delays, and potential reporting gaps that can occur in multi-tier distribution arrangements.

All revenue generated through the Master Agreement will be captured directly in our internal financial and project management systems, providing immediate access to both summary and detailed sales information. Our established accounting procedures and project tracking systems automatically generate the comprehensive reporting data required for NASPO ValuePoint compliance, including contract vehicle identification, participating entity details, service categories, and revenue breakdowns.

Comprehensive Internal Reporting Systems and Controls

Assurit maintains robust internal systems designed to ensure prompt, complete, and accurate sales reporting to NASPO ValuePoint. Our project management and financial systems are configured to automatically capture all relevant transaction data at the point of service delivery, including participating entity information, service categories performed, revenue amounts, and performance periods. This automated data capture eliminates manual reporting errors and ensures consistency across all transactions.

Our internal controls include monthly reconciliation processes where sales data is validated against project records, invoicing systems, and financial reports to ensure accuracy and completeness. We have established dedicated administrative personnel responsible for NASPO ValuePoint reporting compliance, with defined roles and responsibilities for data validation, report generation, and timely submission. Regular internal audits verify the accuracy of our reporting systems and identify any potential areas for improvement.

Commitment to Transparency and Compliance

We recognize that accurate and timely sales reporting is critical to the success of the NASPO ValuePoint program and demonstrates our commitment to transparency and accountability. Our established procedures ensure that summary sales reports are submitted to NASPO ValuePoint according to the specified schedule, while detailed transaction data is maintained and made available as required by the Master Agreement terms.

In the unlikely event that we engage any third-party partners for specific aspects of service delivery in the future, we will implement contractual requirements and monitoring systems to ensure complete reporting compliance from any such partners, maintaining the same standards of accuracy and timeliness that characterize our direct reporting capabilities.

G. (ME) **Customer Service**

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

Customer Service Hours and Key Account Staff Availability

Standard Business Hours and Coverage

Assurit provides comprehensive customer service coverage from 9:00 AM to 9:00 PM Eastern Standard Time, Monday through Friday. This extended 12-hour coverage window ensures that participating entities across all U.S. time zones can access our support services during their standard business hours. Our coverage model recognizes that cybersecurity needs often extend beyond traditional 9-to-5 schedules and that government entities may require assistance during extended operational periods.

Leadership and Administrative Staff Accessibility

Throughout our standard operating hours, a member of our leadership or administrative staff will always be available to address participating entity needs, questions, or concerns. This commitment ensures that entities have direct access to decision-makers who can provide immediate resolution for contract-related issues, service modifications, or urgent requests. Our leadership team includes senior personnel with full authority to make operational decisions and authorize service adjustments as needed.

Dedicated NASPO Contract Management Team

A member of our dedicated NASPO ValuePoint contract management team will be available during all standard operating hours to provide specialized support for Master Agreement-related inquiries. This team maintains deep expertise in the specific terms, conditions, and procedures of the NASPO ValuePoint Master Agreement, ensuring that participating entities receive accurate and timely responses to contract-specific questions. Our NASPO contract management team serves as the primary liaison for all administrative matters, pricing inquiries, and procedural guidance.

Emergency and After-Hours Support

While our standard customer service operates within the defined 12-hour window, Assurit recognizes that cybersecurity incidents can occur at any time. For participating entities experiencing active security incidents or urgent cybersecurity needs outside standard hours, we maintain emergency contact procedures that enable rapid escalation to appropriate technical personnel. Our incident response capabilities include 24/7 emergency contact protocols that ensure critical security issues receive immediate attention regardless of the time of day.

This comprehensive customer service approach ensures that participating entities have consistent access to knowledgeable Assurit personnel who can address their needs promptly and effectively throughout the duration of their engagement under the Master Agreement.

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

Problem Identification and Resolution Process

Proactive Problem Identification

Assurit employs a multi-layered approach to problem identification that emphasizes early detection and proactive resolution. Our project managers conduct regular check-ins with participating entities during active engagements,

utilizing structured feedback sessions and performance metrics to identify potential issues before they escalate into formal complaints. We maintain open communication channels that encourage participating entities to raise concerns or observations at any stage of service delivery.

Our internal quality assurance processes include continuous monitoring of project milestones, deliverable quality, and client satisfaction indicators. Weekly internal reviews assess project status, resource allocation, and potential risk factors that could impact service delivery. This proactive monitoring allows us to identify and address emerging issues internally before they affect the participating entity's operations or satisfaction.

Structured Customer Complaint Resolution

When customer complaints or service issues arise, Assurit follows a structured resolution process designed to ensure prompt acknowledgment, thorough investigation, and effective remediation. All complaints are logged in our customer relationship management system with unique tracking numbers and assigned priority levels based on severity and potential impact. Our contract management team acknowledges all complaints within 24 hours and provides initial response timelines based on the complexity of the issue.

Our resolution process includes immediate escalation protocols for critical issues that may impact security or operations. For standard service complaints, we conduct thorough investigations involving relevant project personnel, review of project documentation, and direct communication with the participating entity to understand all aspects of the concern. We provide regular status updates throughout the resolution process and maintain transparent communication regarding timelines and corrective actions.

Corrective Action and Continuous Improvement

Following issue resolution, Assurit implements corrective action plans that address both the immediate problem and underlying root causes to prevent recurrence. These plans may include process modifications, additional training, resource adjustments, or enhanced quality control measures. We document all complaints and resolutions in our lessons learned database, using this information to continuously improve our service delivery processes and prevent similar issues across other engagements.

Our commitment to continuous improvement includes quarterly reviews of complaint trends and resolution effectiveness with senior leadership. We also conduct post-resolution follow-up with participating entities to ensure satisfaction with our corrective actions and to identify any additional improvements that could enhance future service delivery. This comprehensive approach to problem resolution demonstrates our commitment to maintaining the highest service standards and building lasting partnerships with participating entities.

Describe how you will assess customer satisfaction.

Customer Satisfaction Assessment Strategy

Multi-Faceted Satisfaction Measurement Approach

Assurit employs a comprehensive customer satisfaction assessment strategy that combines formal evaluation tools with ongoing relationship management to ensure participating entities receive exceptional value from our cybersecurity services. Our approach recognizes that customer satisfaction in cybersecurity services encompasses both technical delivery excellence and collaborative partnership effectiveness.

We conduct formal satisfaction surveys at key project milestones, including mid-engagement checkpoints and project completion. These surveys utilize both quantitative rating scales and qualitative feedback sections that allow participating entities to provide detailed insights into service quality, communication effectiveness, technical competency, and overall value delivery. Our surveys are designed to capture satisfaction across all service categories while identifying specific areas for improvement or enhancement.

Ongoing Relationship Management and Feedback Collection

Beyond formal surveys, we maintain continuous feedback collection through regular project communications and relationship management activities. Our project managers conduct structured feedback sessions during routine project meetings, creating opportunities for participating entities to share real-time observations about the effectiveness of service delivery. These informal feedback mechanisms often provide the most actionable insights for immediate service improvements.

We also implement quarterly business reviews with key participating entities, providing forums for comprehensive discussion of service performance, satisfaction levels, and future needs. These sessions include presentation of performance metrics, review of completed work, and collaborative planning for upcoming initiatives. The business review format encourages candid dialogue about both successes and areas requiring attention.

Performance Metrics and Satisfaction Tracking

Our customer satisfaction assessment includes tracking of objective performance metrics that correlate with satisfaction levels, such as on-time delivery rates, response times to requests, issue resolution timeframes, and adherence to budget parameters. We maintain satisfaction scorecards for each participating entity that combine survey results, performance metrics, and qualitative feedback to provide comprehensive satisfaction visibility.

We conduct annual satisfaction benchmarking that compares our performance across participating entities and identifies best practices that can be replicated across all engagements. This benchmarking process helps us understand satisfaction drivers and maintain consistently high performance standards. All satisfaction data is reviewed regularly by senior leadership and used to inform strategic decisions about service delivery improvements, resource allocation, and process enhancements.

Our commitment to customer satisfaction assessment ensures that we maintain the highest service standards while building long-term partnerships that deliver sustained value to participating entities throughout the Master Agreement term.

H. (ME) (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. Offeors must provide documentation of their security practices. Offerors who fail to adequately demonstrate their security standards may be deemed non-responsive. .

Security Compliance

Microsoft Office 365 SOC 2 Compliance Coverage

Assurit currently operates on Microsoft 365 Commercial Cloud for all internal communications, document management, and core business operations. We do not host or manage physical infrastructure or on-premises servers. All internal processes are conducted within Microsoft's secure, cloud-based platform, which undergoes rigorous third-party audits and maintains **AICPA SOC 2 Type II compliance** across all five Trust Service Criteria: **Security, Availability, Processing Integrity, Confidentiality, and Privacy**.

As part of this submission, Assurit is including the most recent Microsoft Office 365 SOC 2 Type II report, which provides formal third-party assurance of Microsoft's infrastructure security controls and compliance. This documentation confirms that the systems supporting our internal environment comply with industry standards for security and data protection.

Internal Cybersecurity Controls and Policies

As a cybersecurity-focused firm, Assurit maintains a mature internal security program grounded in best practices and aligned with NIST 800-171 and CMMC Level 2 requirements. While we leverage Microsoft's platform-level controls, we implement robust organizational policies and procedures to secure our users, devices, and data.

Key components of our internal cybersecurity program include:

- **Access and Identity Management:** All accounts are protected by multi-factor authentication (MFA), with least-privilege access policies enforced through role-based controls.
- **Data Protection:** All internal data is encrypted both at rest and in transit. Data classification policies dictate appropriate handling, storage, and transmission procedures.
- **Device Security:** All endpoints are centrally managed with mandatory antivirus, full disk encryption, and automated patching protocols.
- **Incident Response:** We maintain a formal Incident Response Plan, tested annually, with predefined procedures for detection, containment, remediation, and notification.
- **Security Awareness Training:** All personnel undergo recurring security awareness training, which includes phishing simulation exercises and policy acknowledgments.
- **Monitoring and Auditing:** Audit logs are reviewed regularly, and administrative actions are monitored for any anomalous behavior.
- **Vendor Risk Management:** All third-party vendors undergo thorough due diligence reviews, and contracts include clauses that require data protection and breach notification.

GCC Migration and CMMC Level 2 Compliance

Assurit is currently in the process of migrating to Microsoft 365 Government Community Cloud (GCC) as part of our CMMC Level 2 certification initiative, which will enable us to securely handle Controlled Unclassified Information (CUI) and meet the requirements of the Department of Defense (DoD) and other federal customers.

Our CMMC preparation includes:

- Establishing a compliant enclave within GCC for handling sensitive government data.
- Completing System Security Plans (SSP) and Plan of Action and Milestones (POA&M) documentation.
- Implementing additional technical controls required by NIST SP 800-171, including advanced logging, media protection, and access segmentation.
- Working with a Registered Provider Organization (RPO) to conduct a readiness review and prepare for a Certified Third-Party Assessment Organization (C3PAO) audit.

We expect to complete our CMMC audit within the next **3 to 6 months**, at which point we will have a fully validated environment suitable for handling federal CUI and sensitive information subject to elevated security requirements.

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.

Artificial Intelligence Technologies Usage and Safeguards

AI Integration for Enhanced Service Delivery

Assurit utilizes artificial intelligence technologies to enhance the quality, efficiency, and accuracy of our cybersecurity services under this Master Agreement. Our AI applications focus on supporting and augmenting our expert staff capabilities rather than replacing human expertise and judgment. We employ AI tools to assist in reviewing security documentation, developing comprehensive reports, analyzing vulnerability data, and supporting client deliverables. These technologies enable our team to process larger volumes of security information more efficiently while maintaining the high-quality analysis and recommendations that characterize our service delivery.

Our AI implementation supports activities such as automated threat intelligence analysis, vulnerability assessment data correlation, security control documentation review, and preliminary report generation. By leveraging AI for these foundational tasks, our cybersecurity professionals can focus their expertise on higher-value activities, including strategic analysis, complex problem-solving, and collaborative client engagement.

Proprietary AI Development and Internal Tools

Assurit has invested in developing its own AI tools and services, specifically tailored to meet the needs of cybersecurity applications and clients. These proprietary solutions are designed to address the unique challenges of government cybersecurity work while maintaining the strict security and privacy standards required for sensitive operations. Our internal development efforts focus on creating AI capabilities that enhance our core service offerings while ensuring complete control over data handling and processing.

We are currently developing additional proprietary AI tools that will further enhance our service capabilities, though these solutions are not yet deployed in production environments. Our development approach emphasizes thorough testing, validation, and security reviews before implementing any new AI capability in client-facing work.

Comprehensive Safeguards and Review Protocols

Assurit has implemented rigorous safeguards and review protocols to ensure the accuracy, security, and appropriateness of all AI-generated content and analysis. Our internal technical staff conducts comprehensive reviews of all AI models and tools we utilize, including validation of outputs, accuracy testing, and ongoing performance monitoring. Every AI-generated deliverable undergoes human expert review before being included in client work products, ensuring that our professional standards and quality commitments are consistently met.

Data Security and Isolation Measures

All AI processing occurs within our company tenants and controlled environments, ensuring that sensitive client data is never shared with broader AI models or external systems. We maintain strict data isolation protocols that prevent any client information from being exposed to public AI platforms or contributing to external model training. Our AI infrastructure operates within the same secure Microsoft Office 365 environment that houses all our other business operations, providing consistent security controls and data protection measures.

These comprehensive safeguards ensure that our AI technologies enhance service delivery while maintaining the security, confidentiality, and professional standards that participating entities expect from their cybersecurity service provider.

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.

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

June 20, 2025

Date

Sunny Tuteja

Printed Name

President and CEO

Title

sunny.tuteja@assurit.com

Email Address

(703) 927-4111

Phone Number