CYBERSECURITY AND INFORMATION SECURITY SERVICES - Attachment 07: Offeror Response Worksheet, Acknowledgements, and Certifications - CATEGORY 1, CATEGORY 3

REDACTED PUBLIC COPY

Date: 6/26/2025 | State of Idaho in Collaboration with NASPO ValuePoint | RFQ NO: RFP#928

obs global

Rob Harvey
Managing Director
rharvey@obsglobal.com
404.452.7452

Cover Letter

Online Business Systems (OBSGlobal)
8500 Normandale Lake Blvd. Suite 350
Bloomington, Minnesota,
55437 USA
Jun 26, 2025

Mike Gwinn
Contract Administration Supervisor
State of Idaho, Division of Purchasing
650 W. State St., Rm 100
Boise, ID 83720
Mike.Gwinn@adm.idaho.gov
(208) 332-1617

Dear Mr. Gwinn,

We are pleased to submit this proposal in response to *RFP#928 CYBERSECURITY AND INFORMATION SECURITY SERVICES*. Online Business Systems (recently rebranded to OBSGlobal) is an ideal partner to support public sector entities across the country in strengthening their cybersecurity posture. Our US-based Cybersecurity Practice is committed to delivering RIGHT-SIZED SECURITY and helping our clients create and manage cost-efficient and risk-effective information security programs that align with their unique needs and risk appetite. We have steadily grown our footprint as our unsurpassed delivery, people, culture, and commitment continue to set us apart from other firms. Our size and culture foster agility, empowering us to prioritize our clients' needs without the hindrance of corporate bureaucracy. This agility proves indispensable, especially in collaborations with public sector organizations, where flexibility in vendor partnerships is often paramount to adapting to evolving priorities and requirements.

With deep expertise in cybersecurity strategy, risk management, incident response, breach coaching, and compliance, our collective team brings a proven track record of delivering scalable, high-impact security solutions tailored to the unique needs of public sector organizations. Our proposal outlines our approach and experience to deliver **Category 1: Risk Assessment and Mitigation Services** and **Category 3: Breach Coach Services**.
Our services are rooted in collaboration, innovation, and a commitment to excellence—values that align closely with NASPO ValuePoint's mission to advance public procurement through integrity and best practices.

We appreciate the opportunity to be considered for a Master Agreement and look forward to the possibility of contributing to the success of the State of Idaho, NASPO ValuePoint, and other Participating Entities.

Sincerely, on behalf of OBSGlobal,

Rob Harvey
Managing Partner

Amendment 2
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: Online Enterprises Inc. dba Online Business Systems
B. Primary Business Address: 8500 Normandale Lake Blvd. Suite 350, Bloomington, Minnesota, 55437
C. Federal Tax Identification Number: 41-1805060
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

OBSGlobal's Response
Our Proposal Center utilizes the AI-powered Loopio platform to improve efficiency and precision in proposal development.

III. BUSINESS DETAILS

A. Company Website. Provide a URL for your company's website.

OBSGlobal's Response
Our company website is: https://www.obsglobal.com

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

OBSGlobal's Response
Online Business Systems (herein referred to as OBSGlobal) is cybersecurity and digital transformation a consultancy first formed in Winnipeg, Manitoba in 1986. Since its inception, the company has expanded to eight total locations worldwide. Our US headquarters is based on Minnesota and was formed in 1995. Our US-based OBS Cybersecurity Practice is focused on delivering RIGHT-SIZED SECURITY and helping our clients create and manage cost-efficient and risk-effective information security programs that align with their unique needs and risk appetite. We have steadily grown our footprint to over 580 clients as our unsurpassed delivery, people, culture, and commitment continue to set us apart from other firms. Our growth has been entirely organic, achieved **without any mergers or acquisitions**. We have maintained an average annual growth rate of 12%, enabling us to preserve a unified team and culture centered on delivering right-sized, value-driven services tailored to our clients' needs.

C. Company Size. Identify the number of employees working for your company.

OBSGlobal's Response
OBSGlobal currently employs over 400 consultants across eight global offices.

D. Ownership Structure. Describe your company's ownership structure.

OBSGlobal's Response
OBSGlobal is a privately-owned company.

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

OBSGlobal's Response
OBSGlobal has not been party to litigation or have any claims of non-performance or breach.

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.

OBSGlobal's Response

OBSGlobal has designated Melissa Erikson as our Contract Manager and single point of contact for the NASPO ValuePoint Master Agreement. Her contact information is:

Melissa Erikson
Public Sector Lead
merikson@obsglobal.com
303-886-7966

Melissa brings over 15 years of experience successfully managing complex projects and contracts for state and local agencies nationwide. Her experience is rooted in procurements, as she spent years working alongside state agencies to manage complex procurements - from the initial development of the strategy and funding requests to the post-award contract negotiations and vendor management. This background, coupled with her project management foundation, provides Melissa with a unique understanding of public sector procurement and contracting requirements. Her detailed resume is included as Attachment titled "RFP#928_OBSGlobal_Attachment A_Contract Manager Resume."

As the Public Sector Lead, Melissa is responsible for shaping the company's public sector strategy for State, Local, and Education government markets. Her role includes identifying and qualifying new opportunities, cultivating and maintaining relationships with public sector clients, leading the scoping and proposal process, and ensuring the successful delivery and oversight of public sector contracts.

Melissa brings extensive experience in managing contracts governed by Master Service Agreements (MSAs), including engagements with states such as Wyoming, Washington, Minnesota, and Mississippi. At her previous firm, she supported the NASPO Master Service Agreement for Procurement Services, gaining firsthand knowledge of the structure and operational requirements of a NASPO-led MSA model. Her broad expertise in scoping and executing both internal and external initiatives across diverse public sector agencies positions her well to drive strong engagement and value under this Agreement.

Melissa is supported by our Proposal Contact, Candace Bergman. Her contact information is:

Candace Bergman
Proposal Center Lead
cbergman@obsglobal.com
403-399-4038

Candace oversees the management of solicitations and proposals submitted through the various intake channels. She collaborates closely with Melissa and the Proposal Center to qualify, prioritize, and develop responses to opportunities identified by our Contract Manager, Business Development Team, Partners, clients, and internal consultants. For this process, the Proposal Contact will play a vital role in coordinating communications with the Lead State and Participating Entities in partnership with the Contract Manager.

At OBSGlobal, we balance structured business development processes with the flexibility needed to respond swiftly to client needs. We are committed to maintaining timely communication with the Lead State and will notify them within 24 hours of any changes to our designated Proposal or Contract.

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.

OBSGlobal's Response

Risk Assessment and Mitigation Services

At OBSGlobal, we believe Risk Assessments lay the foundation for informed decision-making by providing stakeholders with a prioritized roadmap for remediation and long-term resilience.

Our team brings a comprehensive, agile, and deeply experienced approach to Risk Assessment and Mitigation Services—designed to meet the evolving needs and regulatory changes of our public sector clients. With a "whole-of-state" mindset, we combine technical expertise, regulatory fluency, and operational agility to deliver cybersecurity outcomes that are scalable, actionable, and sustainable.

Since the inception of our Cybersecurity Practice in 2010, our Risk Management consultants are strategically distributed across the United States, working across multiple time zones yet united by a shared mission: to serve as trusted advisors and protect critical assets. Whether we're supporting a single K–12 district in California, a multi-county utility in the Midwest, or a state technology office on the East Coast, we bring the same level of dedication, responsiveness, and excellence to every engagement.

Our national reach is what sets us apart—enabling us to remain flexible, responsive, and closely aligned throughout the risk assessment process, delivering efficient and

comprehensive results. This is demonstrated in the hundreds of Security Risk Assessment services we have conducted in the past 15 years for clients ranging from small, rural Health Centers to state government agencies, to worldwide Fortune 10 retailers.

Government-Wide Coverage and Sector-Specific Expertise

OBSGlobal is prepared to serve the NASPO Purchasing Entities across state, local, and tribal governments, with deep experience delivering Cybersecurity, Privacy, and Risk Management services across a broad range of public sector domains. Our team understands the complex interdependencies, compliance obligations, and resource constraints that government agencies face—and we tailor every engagement to align with each entity's mission, operational needs, and data protection requirements.

We offer proven expertise in the following sectors:

- **State and Local Government:** Comprehensive risk assessments, governance alignment, policy modernization, and interagency coordination across multiple departments and jurisdictions, aligning with NIST CSF, NIST 800-171, MARS-e, ARC-AMPE, FedRAMP, StateRAMP, ISO/IEC 27001:2022, CMMC, and DFARS.
- **Education (K–12 and Higher Education):** FERPA-compliant cybersecurity reviews, ransomware preparedness, secure integration of cloud-based learning tools, and identity management strategies for large user populations.
- **Healthcare and Public Health:** HIPAA, HITECH, and 405(d)-aligned risk assessments; medical IoT (MIoT) and EHR system security; privacy impact assessments; and business continuity planning for critical care environments and Federally Qualified Health Centers (FQHCs).
- **Law Enforcement and Public Safety:** CJIS compliance readiness, endpoint and mobile device hardening, secure digital evidence management, and support for incident response protocols within police, fire, and emergency services.
- **Utilities and Public Infrastructure:** Cybersecurity program development and risk assessments aligned to NERC CIP and other utility-specific requirements, with a focus on OT/IT convergence, access control, and vendor risk management.
- **Transportation and Logistics:** Security assessments of GPS-reliant systems, IoT-connected fleet infrastructure, real-time tracking systems, and third-party logistics coordination with emphasis on data integrity and operational resilience.

Phased Risk Assessment Strategy

To deliver consistent value across these sectors, OBSGlobal applies a phased Risk Assessment methodology tailored to the unique needs of each NASPO Purchasing Entity. We leverage our proprietary Risk Assessment tool that easily scales across multiple frameworks and threat profiles to provide a consistent, standards-based approach to our Risk Assessments aligned with *NIST SP 800-30: Guide to Conducting Risk Assessments*. Our proprietary Risk Assessment Tool is easily tailored to reflect requirements, controls, standards, and best practices for the identified frameworks and regulatory compliance needs. The Tool captures and collates our observations, findings, and maturity ratings throughout general activities below to highlight gaps, vulnerabilities, and calculate our client's specific risk profile.

Prior to starting work on our engagements, we invest time in a Project Initiation Phase to establish a strong foundation for project management and communications. A key activity in Initiation is our recommended Kick-Off meeting. In this, OBSGlobal will meet with the client stakeholders to confirm objectives, review the scope of services, timelines, resources, dependencies, deliverables, and communication needs. In this, we also confirm compliance

requirements for inclusion in our assessment strategy and tooling. We provide clients with a document request list to streamline data collection and prepare for the assessment.

Results from the Kick-Off will be incorporated into a Work Plan and supporting communications that will drive activities and manage resources throughout the course of the engagement. The outputs from Initiation will be used to inform, manage, and monitor the key Risk Assessment Steps:

1. **Risk Discovery & Asset Inventory**
   We begin by identifying critical assets, data flows, and operational dependencies across the organization. Assets are classified based on business impact and mission criticality to establish a clear understanding of what needs protection.

2. **Threat-Based Vulnerability Analysis**
   Whereas other risk analysis processes may begin with evaluation of security controls, we prefer to take a threat-based approach to Security Risk Analysis by focusing on realistic threats to the organization. By first developing a specific threat-profile, the organization can identify and focus on security controls that provide the greatest value to protecting critical assets and, hence, the business.

   OBSGlobal maintains a library of current threats derived from several industry sources including NIST, the Department of Health and Human Services (HHS), the International Standards Organization (ISO), and the US Cybersecurity and Infrastructure Security Agency (CISA).

   We start with a baseline Threat Profile that includes a rating to indicate the likelihood of the threat scenarios occurring for the organization. We then use organizational information, interviews, and workshops to customize the profile for each client.

3. **Control and Compliance Assessment**
   We assess existing technical, physical, and administrative safeguards and controls against leading frameworks including but not limited to NIST SP 800-53 Rev5, CIS, NIST SP 800-171 HIPAA, ISO/IEC 27001 Annex A, and CISA Cybersecurity Performance Goals (CPGs).

   The methodology reflects the Examine, Interview, and Test process.

   Examine. OBSGlobal will begin by requesting documentation and other evidence to support the implementation of security controls. This may include Policies, Procedures, Plans, hardware or software inventories, or screenshots. OBSGlobal will review the provided documentation and evidence to inform our tailored interview needs. OBSGlobal provides clients with a secure Sharepoint fileshare to securely exchange and store files in accordance with the Data Encryption and Data Location Requirements. Though all risk assessment engagements include a policy assessment OBSGlobal may conduct an in-depth policy gap analysis as part of this step to identify specific policy and procedural needs. We have access to our internal Policy and Procedure library to help our clients supplement gaps or language as part of mitigation planning described below.

   Interview. Our team will prepare and facilitate interviews with the various stakeholders to obtain an overall understanding of the

consistency and quality of the controls implemented in the enterprise. OBSGlobal will interview and have subsequent discussions, as necessary, with knowledgeable staff responsible for various aspects of information security management.

Test. As appropriate, OBSGlobal will validate the implementation of security controls as described in the documentation and interviews. Depending on the client's need and scope of work, we complement our Risk Assessment methodology with specific testing or supporting activities including penetration testing, business impact analysis (BIAs), tabletop exercises to better understand and identify risk to the organization. Examples of testing may include:

- Over-the-shoulder or virtual screensharing reviews of system
- configurations
- Consideration of penetration and technical testing results
- Additional system or network scanning or review of scans, if in scope.
- Physical Site Assessments and testing

Results will be tracked in our Tooling for risk consideration.

4. **Risk Register and Reporting**
Results and findings from activities are collated in our Risk Assessment Tool which includes built-in algorithms that consider the client's threat profile, critical assets, evidence, control maturity and implementation status, and calculates vulnerabilities and weighted risk register specific to their environment. Depending on the client's existing risk management program, we may tailor our algorithms and weighting to best align with the client's risk classifications and support long-term risk management within the client organization.

A laundry list of risks is not effective in driving action or mitigation strategies. As part of our reporting, OBSGlobal prefers to highlight the top three to five priority risks for management attention in a "what, so what, now what?" presentation to communicate priority findings and recommendations for stakeholder and leadership attention. However, like each engagement, we will tailor our deliverables to align with the Purchasing Entity's specific needs and deliverable expectations.

5. **Mitigation Strategy Development**
Drawing from assessment results, our experienced virtual Chief Information Security Officers (vCISOs) lead the development of comprehensive, tailored risk mitigation strategies designed to proactively address identified vulnerabilities. These strategies encompass a balanced mix of preventive controls, contingency planning, and business continuity models, all aligned with compliance mandates, industry standards, and the organization's unique priorities. Our team works collaboratively to ensure each strategy is not only actionable but also measurable—presenting detailed implementation plans, resource requirements, and effort estimates. This enables stakeholders to evaluate each strategy's return on investment in the context of its potential to reduce risk and strengthen overall resilience.

6. **Implementation and Monitoring**

To support the effective implementation and monitoring of risk mitigation strategies, our team partners closely with stakeholders to develop and execute prioritized remediation roadmaps that align with business objectives and risk tolerance. We tailor our approach to the client's existing tools and operational landscape, ensuring seamless integration and execution, but offer additional options for clients depending on the maturity of their security program.

Our senior staff complement client teams to provide ongoing monitoring support, which may include activities such as process design, tool or system selection and implementation, tabletop exercises, crisis simulations, and technical testing to monitor progress. We establish routine "Health Checks" with client leadership to provide executive briefings on progress and reevaluate priorities. Additionally, we can integrate with JSOC, SOAR/XIAM platforms, and telemetry feeds to provide near real-time visibility into the threat landscape, enabling rapid response activation and continuous assessment of the organization's risk posture. Through this comprehensive approach, we ensure that mitigation strategies are not only implemented effectively but also monitored and refined over time to adapt to evolving risks.

Specific Experience

To demonstrate our scale of engagements, we highlight our recent public sector engagements to exemplify our ability to meet and exceed the requirements outlined in NASPO's Category 1 – Risk Assessment and Mitigation Services.

1. [redacted]

[redacted]

- HIPAA Security Risk Assessments (SRAs) for the HCCN, along with a selection of participating health centers, aligned with NIST SP 800-30 and OCR guidance.
- Remediation and Maturity Roadmaps tailored to each center's risk profile and operational maturity.
- Cyber Insurance Advisory, helping centers evaluate and align with insurer expectations.
- Policy Development for administrative, technical, and physical safeguards.
- Education and Awareness Programs, including webinars and in-person group training.
- Risk Seminars and Tabletop Exercises simulating ransomware, insider threats, and supply chain attacks.

This engagement has improved audit readiness, reduced risk exposure, and enhanced incident response capabilities across the [redacted]

[redacted]

OBSGlobal was brought in as a partner to support the design, development, and implementation of [redacted] to support the state's Medicaid Enterprise Systems. As part of the scope, OBSGlobal provided security and privacy expertise to support the required security artifacts and processes required by state and federal agencies.

This included conducting a comprehensive Risk Assessment in alignment with the CMS Information System Risk Assessment (ISRA) process to documents the overall risk and potential risk reduction strategies to support the success o[redacted] and its objectives for the state.

[redacted]

Since 2019, OBSGlobal has been a trusted partner to the[redacted] and its member institutions, delivering comprehensive Gap and Risk Assessments as well as penetration testing services. These efforts have helped identify vulnerabilities and define actionable mitigation strategies to strengthen cybersecurity across the state's participating community colleges.

[redacted]

[redacted]

This assessment served as the critical first step in understanding [redacted] current cybersecurity posture, identifying vulnerabilities, and informing a strategic roadmap for modernization. By establishing a clear baseline, the Risk Assessment enabled [redacted] to prioritize investments, align with regulatory requirements, and build a scalable, shared-service model to support its "Whole-of-State" cybersecurity vision.

Our approach was structured into three key phases:

1. **Initiation and Planning**
   - Conducted a stakeholder analysis and project planning to align with [redacted] strategic objectives and operational realities.
   - Defined key performance indicators (KPIs), compliance benchmarks, and regulatory requirements, including CJIS, HIPAA, and NIST frameworks.
   - Established communication protocols and change management strategies to ensure stakeholder engagement and adoption.
2. **Data Collection and Assessment**

- Performed a SOC Capability Maturity Model (CMM) evaluation to benchmark current capabilities.
- Conducted technical assessments and gap analyses of monitoring tools, logging levels, and threat detection capabilities.
- Delivered a SOC Skills Assessment and Business Review to ensure alignment with [redacted]mission and service delivery goals.
- Executed a Regulatory and Compliance Assessment and facilitated an Incident Response Tabletop Exercise to evaluate readiness and identify areas for improvement.

3. **Analysis and Reporting**
   - Compiled findings into a comprehensive Final SOC Assessment Report, detailing risk statements, vulnerabilities, and prioritized recommendations.
   - Developed a Strategic Plan and Implementation Roadmap to guide SOC modernization, enhance operational resilience, and enable statewide scalability.

[redacted]

OBSGlobal partnered with the City to deliver comprehensive Information Security Assessment Services aimed at enhancing the City's overall cybersecurity posture. Our engagement included a suite of services such as vulnerability assessments, penetration testing, critical infrastructure evaluations, and other targeted security assessments aligned with the City's strategic objectives.

As part of this effort, OBSGlobal conducted a thorough evaluation of both physical and digital vulnerabilities across the City's key operational departments—includin[redacted] Development, and the City Manager's Office. The outcome was a prioritized remediation and risk mitigation roadmap, tailored to address the most critical vulnerabilities while supporting a "right-sized" implementation strategy to strengthen the City's security framework effectively and sustainably.

[redacted]

OBSGlobal was contracted by the State to perform recurring MARS-E Security Assessments and Testing for both the [redacted]

As a subcontractor, OBSGlobal delivered a full suite of security assessment services, including vulnerability assessments, internal network and application penetration testing, security controls reviews, and ongoing security consulting throughout the implementation and integration of [redacted]

These assessments played a critical role in supporting the State's Authority to Connect (ATC) to the Federal Data Services Hub. OBSGlobal identified and helped remediate key vulnerabilities within applications, contributing directly to the development of the Plan of Action and Milestones (POA&M). The success of this engagement led to multiple follow-on assessments, reinforcing OBSGlobal's role as a trusted security partner to the State.

Summary of Qualifications

- **5+ Years of Experience:** Delivering Category 1-aligned services since 2010 (15 years).
- **Diverse Scale of Clients:** Ranging from large-scale, statewide agencies to small, rural health centers and cities.
- **Multi-State Engagements:** Supporting large-scale government sectors, ensuring business continuity across NY, MN, WY, and others.
- **Public Service Impact:** Security services addressing potential threats across multi-dimensional government entities protecting millions of citizens annually.
- **Comprehensive Services:** Risk assessments, remediation, policy, insurance, training, and incident response.
- **Framework Alignment:** HIPAA, NIST CSF, SP 800-30, SP 800-53, 800-171, MARS-E, ARC-AMPE, ISO/IEC 27001, ISO/IEC 42001, CJIS, FERPA, and FIPS 140-2.

Our collective OBSGlobal team and network of partners bring unmatched insight into public sector cybersecurity. We offer a flexible, standards-aligned, and deeply experienced approach to risk assessment and mitigation needs. Our phased methodology, sector-specific expertise, and commitment to public sector mission success make us the ideal partner for NASPO ValuePoint entities seeking to build resilient, secure, and future-ready operations.

- **(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.

OBSGlobal's Response

OBSGlobal brings a team of seasoned professionals with an average of 15 years in cybersecurity and over 30 years in IT, spanning a wide range of industries including state and local government, healthcare, retail, e-commerce, travel, finance, telecommunications, and business process outsourcing (BPO). Our consultants have conducted hundreds of security assessments and testing engagements aligned with leading frameworks such as NIST, HIPAA, HITRUST, PCI, GDPR, ISO, and more.

Our team holds a broad array of industry-recognized certifications, including CISSP, OSWP, OSCP, HITRUST CCSFP, HCISPP, CISA, PMP, and QSA—demonstrating our commitment to maintaining the highest standards of expertise and professionalism. (See certification table below for details.)

We take a collaborative, tailored approach to every engagement. Working closely with our resource director and service line leads, we assemble the right mix of consultants based on the project scope, client needs, and required skill sets—ensuring excellence in delivery. Our consultants have transitioned from large firms to join a culture that prioritizes client success over profit margins. We understand the importance of change management and are dedicated to fostering a culture of security awareness, resilience, and continuous improvement. By leveraging our collective expertise and a team-first mindset, we ensure that every engagement is executed with precision, professionalism, and a focus on delivering meaningful outcomes.

Based on the requested roles in the Scope of Work, we highlight our experience in following key roles:

2.3.1 Security/Technology Senior Analyst(s)

Our Security/Technology Senior Analysts bring 5-15 years of experience in security and enterprise IT, serving in key roles to support comprehensive security risk assessments, compliance reviews, controls design and implementation, risk mitigation planning, and more.

Certified in a range of technology and/or security disciplines, our senior analysts bring rigorous quality assurance oversight to every engagement. They are adept at coaching teams, elevating staff capabilities, and ensuring the delivery of high-value technical and security-related outcomes. Their ability to troubleshoot complex issues, communicate across technical and non-technical audiences, and resolve challenges efficiently positions them as a critical asset to the delivery team.

2.3.2 Business Process/Risk Management Senior Consultant

Our team of Senior Risk Management Consultants bring nearly two decades of experience leading cybersecurity, risk management, and enterprise process improvement initiatives across global, regulated, and public sector organizations. With deep expertise in business operations, risk tolerance, and regulatory compliance, this expert delivers tailored, right-sized solutions that align with each client's mission objectives and risk appetite.

With a range of certifications including C|CISO, CISM, CBCP, CISSP, and PMPs, these consultants have built and led programs in alignment with a broad spectrum of industry-recognized standards and government frameworks, including:

- **ISO/IEC 27001** – Information Security Management Systems
- **ISO/IEC 42001** – Artificial Intelligence Management Systems
- **ISO/IEC 22301** – Business Continuity Management
- **NIST CSF** and **NIST SP 800-SERIES**
- **PCI DSS**, **SSAE 18**, and **CJIS SECURITY POLICY**
- **FEDRAMP** and **FISMA** – Federal compliance standards
- **HITRUST CSF** – Integrated security and privacy controls for healthcare
- **HIPAA** – Security Rule, Privacy Rule, and Breach Notification Rule
- **HHS 405(D)** – Cybersecurity guidance for the healthcare sector
- **CMMC** – Cybersecurity Maturity Model Certification for DoD contracts
- **CMMI** – Capability Maturity Model Integration for process maturity
- State-level IT, procurement, and security standards

This group has also led enterprise initiatives such as directing a global Security Operations Center (SOC) with a $14M budget, developing enterprise cybersecurity roadmaps, conducting threat modeling, and implementing security automation platforms (e.g., SIEM, SOAR). Their approach to risk assessments goes beyond checklist compliance—serving as a strategic decision-making tool to support prioritization, investment planning, and long-term risk reduction.

Our consultants are well-equipped to perform the specific functions outlined in NASPO's requirements, including:

- **Vulnerability Assessments, Privacy Impact Reviews, and Internal Control Evaluation:** Comprehensive risk assessments are conducted using a structured, framework-aligned approach. This includes evaluation of vulnerabilities, review of privacy practices, and assessment of internal controls essential to the protection of sensitive data. Proprietary systems and complex environments are assessed with equal rigor.
- **Implementation of Risk Assessments and Mitigation Strategies:** Our team leverages proven methodologies from NIST, ISO, and HITRUST to identify risk, align controls, and implement targeted mitigation strategies. These strategies are grounded in organizational context and designed to align with real-world risk appetite.
- **Compliance Assessments Related to Disclosure Responsibilities:** With extensive experience navigating federal, state, and local compliance obligations, our consultants ensure that Purchasing Entities meet regulatory requirements for data protection, including breach notification and third-party risk. This includes audits against HIPAA, FERPA, CJIS, PCI DSS, and more.
- **Threat and Vulnerability Evaluation:** Consultants performs end-to-end analysis of current-state environments—including application architecture, system configuration, and data flow—to uncover vulnerabilities and identify relevant threat vectors. Proprietary and legacy systems are assessed alongside modern infrastructure.
- **Prioritization and Cost Evaluation of Risks:** Identified risks are prioritized based on severity, likelihood, and potential business impact. Our team provides actionable, cost-aware mitigation recommendations that balance risk reduction with operational feasibility.
- **Security Policy Review and Recommendations:** Senior Consultants conduct comprehensive reviews of existing policies and develops new documentation where gaps exist—ensuring coverage of access control, acceptable use, incident response, and third-party oversight.
- **Design and Development of Business Processes and Applications:** In response to assessment findings, our consultants collaborate with stakeholders to redesign workflows, strengthen control integration, and, where applicable, support application development decisions to embed risk mitigation into operational design.
- **Third-Party Contract Advisory:** Upon request, our team provides expert input on contract language and security terms for vendors and cloud service providers—ensuring alignment with best practices and applicable regulations.

With a proven ability to lead diverse teams, provide strategic counsel, and deliver results in high-stakes, compliance-driven environments, this team of consultants embody the technical rigor, regulatory fluency, and practical experience needed to support NASPO ValuePoint and its member entities with precision and confidence.

2.3.3 Project Manager

Our appointed Project Managers offer 5-15 years of proven experience successfully managing complex initiatives across the public sector, including multi-agency environments and high-visibility statewide projects. With expertise in both strategic project delivery and business process transformation, our Project Managers bring deep familiarity with

government operations, stakeholder alignment, and the rigor required for publicly funded programs.

Certified as a Project Management Professional (PMP), they have a strong track record of leading full lifecycle project execution—from initial scoping and team coordination to budget management, schedule control, and performance reporting. Their disciplined approach incorporates industry-standard methodologies to ensure transparent communication, proactive risk mitigation, and measurable outcomes aligned with engagement objectives.

This role is further reinforced by OBSGlobal's extensive experience managing large-scale government initiatives spanning multiple jurisdictions and operational domains. The team is well-versed in navigating the complexities of public sector delivery, ensuring that oversight, compliance, and strategic goals are consistently met.

With a delivery style rooted in accountability, clear communication, and adaptability, the Project Manager will ensure the engagement remains on track, within budget, and aligned with the client's mission. Backed by OBSGlobal's mature governance framework and history of success in similarly scoped projects, this leadership will provide the structure and confidence needed to ensure outstanding results.

Extended Consulting Team

In addition to the proposed lead roles, OBSGlobal will bring forward a multidisciplinary team of highly qualified professionals to support every phase of this engagement. This extended team draws from decades of combined experience across public sector domains—spanning health and human services, education, financial services, technology, and critical infrastructure—and is positioned to deliver agile, strategic, and high-impact results.

We are best represented by our people. Our consultants average fifteen (15) years of cybersecurity experience and over twenty (20) years in IT. They bring hands-on, real-world expertise from engagements with state departments of Health, Education, Transportation, Public Safety, and Information Technology, as well as municipal governments, housing authorities, public works, fire and police departments, school districts, and financial services organizations.

Our team also has extensive experience in AI Governance, Responsible Data Architecture, and System Interoperability—including support for Nationwide Interoperability Platforms, EHR Integrations, and AI-Readiness Assessments for primary care networks and education systems. We have led initiatives involving AI Management Systems, the implementation of cross-platform data hubs, and the secure integration of cloud, IoT, and medical device data into operational environments.

Collectively, our team has conducted hundreds of security testing engagements, technical assessments, and strategic planning efforts aligned with HIPAA, 405(d), HITRUST, NIST, PCI DSS, GDPR, ISO/IEC 27001, ISO/IEC 42001, SOC 2, CMMC, and other key frameworks.

To ensure delivery is efficient, cost-effective, and aligned with project needs, OBSGlobal utilizes a blended team model—strategically combining Senior Consultants, Advisors, named Sub-Contractors, and subject matter experts with multi-level consultants. Senior resources provide strategic leadership and oversight, while analysts and coordinators handle documentation, reporting, and technical support—allowing senior experts to focus

their time on high-impact activities. This approach maximizes value while maintaining high quality and cost efficiency.

The extended team includes:

- **Virtual CISOs and Senior Risk Advisors** with extensive experience conducting cross-sector risk and compliance assessments—including deep engagement in interoperability challenges, cloud architecture, and data privacy governance across healthcare, education, and financial systems. Framework experience includes HIPAA, HITECH, 405(d), PCI DSS, ISO/IEC 27001, ISO/IEC 42001, NIST 800-53, CMMC, SOC 2, GDPR, and CCPA.
- **AI and Interoperability Experts** who have worked on national and state-level projects involving Interoperable Health Data Systems, Standards-Based EHR Integration, AI Safety And Ethics, and Cross-Sector Data Exchange. Their leadership has informed the design of secure, compliant architectures to support data portability, real-time analytics, and decision support across government, health, and education domains.
- **Education and Public Sector Specialists** with experience integrating cybersecurity into school systems, strengthening identity and access management, and supporting FERPA compliance in K–12 and higher education.
- **Financial Services Consultants** who have supported secure modernization and compliance for banking, insurance, and fintech organizations—including PCI DSS programs, SOC 2 reporting, and secure infrastructure upgrades to support AI-driven financial operations.
- **Strategic Design Experts** specializing in aligning AI, blockchain, and data strategy with business transformation initiatives. These professionals support innovation in highly regulated sectors while maintaining control alignment and risk governance.
- **Operational Design and Change Management Consultants** with proven success optimizing workflows, managing transitions to interoperable systems, and driving adoption of emerging technologies.
- **Cybersecurity Architects and SOC Experts** with deep technical experience supporting global security operations, Red Team engagements, threat detection automation, and governance for AI-enabled platforms. Certifications include CISSP, CEH, C|CISO, PCI-QSA, CISA, CIA, and AWS Security Specialty.
- **Public Sector Compliance Consultants** fluent in aligning operations to frameworks like NIST 800-53, FISMA, CJIS, CMMC, CMMI, and FedRAMP—especially within environments that require high degrees of system integration and cross-agency data sharing.
- **Healthcare Security and Subject Mater Experts** who have supported over 200 public and private healthcare risk assessments, advisory, and led initiatives integrating electronic health record systems with broader state data-sharing platforms.
- **Education and Facilitation Specialists** who deliver AI-awareness training, cybersecurity workshops, and executive briefings tailored to multi-sector leadership and operations staff.
- **Project Managers and Coordinators** who manage complex, multi-jurisdictional programs involving both legacy and modernized platforms, ensuring data integrity, and objectives alignment.

- **Analysts and SOC Advisors** supporting security operations, documentation, system mapping, and compliance tracking—helping ensure seamless integration across multiple environments.

This delivery model provides NASPO ValuePoint and its member agencies with a **Scalable, Cost-Effective team structure** that brings together deep technical and regulatory expertise with a practical understanding of real-world challenges of government, interoperability needs, data governance, and AI readiness.

This is further illustrated in the team matrix below, which highlight how OBSGlobal's team and credentials are tightly aligned to NASPO's strategic goals and service expectations.

Certification	# Employees
Certified Information Systems Security Professional (CISSP)	24
Health Certified Information Systems Security Professional (HCISSP)	2
Masters of Science and Engineering (MScEng.)	2
ISO Lead Implementer	4
ISO 27001 - Lead Auditor	10
Project Management Professional (PMP)	28
Certified Information Systems Auditor (CISA)	23
Security+	3
Network+	1
Certified Secure Software Lifecycle Professional (CSSLP)	2
Certified Secure Software Lifecycle Professional (CSSLP)	2
GIAC Web Application Penetration Tester (GWAPT)	2
GIAC Penetration Tester (GPEN)	1
GIAC Certified Incident Handler (GCIH)	1
Certified Ethical Hacker (CEH)	3
Offensive Security Certified Professional (OSCP)	3
Offensive Security Wireless Professional (OSWP)	3
AWS Certified Security – Specialty Certification	3
AWS Certified Cloud Practitioner	4
AWS Certified Machine Learning – Specialty	1
AWS Certified Solutions Architect – Associate	2
Certified Information Privacy Professional (CIPP)	1
Certified in Risk and Information Systems Control (CRISC)	1

PCI Qualified Security Assessor (QSA)	33
PCI Point to Point Encryption (P2PE) Assessor	3
PCI 3-D Secure Assessor (3DS)	2
PCI Qualified PIN Assessor (QPA)	1
PCI Secure Software Assessor	1
PCI Secure SLC Assessor	1
PCI Associate Qualified Security Assessor (AQSA)	9

- **(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.

OBSGlobal's Response

Service Level Agreements (SLAs): Risk Assessment and Mitigation Services

OBSGlobal is committed to delivering high-quality, responsive, and standards-aligned Risk Assessment and Mitigation Services. Our SLAs are designed to ensure transparency, accountability, and measurable performance throughout the engagement lifecycle for the Purchasing Entity.

Key SLA elements include:

- **Efficient Kick-Off Planning:** Every engagement begins with a structured project initiation phase, including stakeholder alignment, scope validation, and scheduling. We use Prosci-based change management principles to ensure organizational readiness and adoption.
- **Defined Response Times and Service Tiers:** Our SLA matrix, below, outlines clear expectations for response and resolution times based on risk severity, ensuring timely action and prioritization.
- **Communication and Escalation Protocols:** We establish dedicated communication channels and escalation paths from day one. Our Contract Manager will remain actively engaged throughout the engagement to ensure responsiveness and issue resolution.

1. Typical Response Times and Service Tiers

Service Type	Anticipated Response Time	Resolution/Action Time	Availability
Critical Risk Discovery (e.g., active threat)	2 hours	Mitigation plan within 24 hours	24/7 during engagement
High Risk Vulnerability	4 hours	Remediation plan within 2 days	Business hours (M–F)

Medium Risk Finding	1 business day	Recommendations within 5 days	Business hours (M–F)
Low Risk / Advisory	2 business days	Included in final report	Business hours (M–F)
General Inquiry / Support	1 business day	2 business days	Business hours (M–F)

Our tiered escalation path for unresolved issues typically follows the following process:

- **Tier 1:** Project Manager (response within 1 business day)
- **Tier 2:** Business Development Lead / Engagement Team (response within 4 hours)
- **Tier 3:** Contract Manager (response within 24 hours)

2. Responsibilities

To summarize responsibilities for Category 1: Risk Assessment and Mitigation:

Contractor Responsibilities	Participating Entity Responsibilities

• Conduct all assessments in accordance with applicable frameworks in alignment such as, HIPAA, NIST CSF, SP 800-30, SP 800-53, 800-171, MARS-E, ARC-AMPE, CMMC, ISO/IEC 27001, ISO/IEC 42001, CJIS, FERPA, FIPS 140-2, CISA, MS-ISAC, PCI DSS, and other applicable frameworks.
• Encrypt all Non-Public Data in transit and at rest using FIPS 140-2 validated cryptographic modules.
• Store all data exclusively within U.S.-based data centers with physical and logical access controls.
• Provide a comprehensive final report within one (1) week of completed activities (or agreed upon timeframe), including:
  ○ Risk statements
  ○ Threat prioritization
  ○ Mitigation recommendations
  ○ Compliance gaps
• Maintain weekly status reporting and stakeholder communication (or agreed upon timeframe).
• Ensure all services are delivered in accordance with applicable state and federal breach notification laws.
	• Provide timely access to relevant personnel, systems, and documentation.
	• Identify and classify data as Public or Non-Public.
	• Participate in stakeholder interviews and tabletop exercises.
	• Review and approve project plans, timelines, and deliverables.
	• Ensure internal coordination for implementation of recommended mitigations.

- **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.

OBSGlobal's Response	
In addition to our Category 1: Risk Assessment and Mitigation Services, our comprehensive team offers the following "Value-Added Services" to support clients' strategies to reducing risk and improving their overarching security posture:	
Risk Assessment and Mitigation Value-Added Services	**Attachment 09 - Pricing Correlation Role**
PCI Compliance and Assessment: OBSGlobal's QSA-certified team (33 QSAs, 8 AQSAs) supports public sector entities in achieving PCI DSS compliance, ensuring secure handling of payment card data across government-operated services such as licensing, permitting, and public utilities. We have been a PCI SSC approved firm for 12 years, and along with 4.0 our QSAs can deliver: P2PE, PCI PIN, PCI 3DS, PA-DSS.	PCI QSA, PCI AQSA
Offensive Security, Simulation, and Continuous Monitoring Services: Our Offensive Security team has a comprehensive suite of proactive security services designed to identify, test, and continuously monitor vulnerabilities across government environments. This includes penetration testing (network, wireless, web, and application), red and blue team exercises, social engineering, secure code review, and autonomous testing. These services are complemented by tabletop simulations and real-time telemetry pipelines that enhance situational awareness, validate incident response capabilities, and support continuous risk readiness across multi-entity public sector ecosystems.	OSS Tester
AI Assessment and Advisory Services: We provide AI governance and advisory services tailored for government entities. These services include guidance on AI governance frameworks, policy creation for ethical and secure AI use, and compliance with public sector standards. We conduct AI impact assessments and third-party reviews to evaluate risks to privacy, security, and operational integrity, and regulatory alignment. This ensures responsible AI adoption across departments, agencies, and jurisdictions.	vCISO
Security Advisory Services: We offer strategic guidance on digital forensics and incident response (DFIR), disaster recovery planning, Business Continuity Planning (BCP), Business Impact Analysis (BIA), and Cloud security program development to enhance resilience and regulatory alignment.	vCISO
CISO Services: Our team of professionals work alongside Participating Entities offering virtual and fractional CISO support for agencies needing executive-level cybersecurity leadership, policy development, and strategic planning.	vCISO
Privacy Assessment And Policy Guidance: We help government entities assess privacy risks and align with evolving regulations such as HIPAA, FERPA, GDPR, and state-specific laws. We evaluate current practices, identify compliance gaps, and provide actionable recommendations. Our services include drafting and updating privacy policies, advising on data classification, consent, and cross-agency	vCISO

data sharing, and ensuring governance frameworks stay current with regulatory changes.	
Cybersecurity Governance & Policy Alignment: We support the development and modernization of cybersecurity governance frameworks, including board-level training, policy lifecycle management, and structured decision-making pathways.	vCISO
Cyber Insurance Strategy & Risk Transfer Advisory: Guidance on cyber insurance procurement, risk quantification, and alignment of controls with insurer expectations to reduce premiums and improve coverage.	vCISO
Zero Trust Architecture & SOAR/XIAM Integration: We offer design and deployment of modern security architectures and automation platforms to support scalable, adaptive defense strategies across distributed government environments.	vCISO
Security Operations Center Design and Deployment: Our strategic partner, BisBlox, pioneered the JCSOC model, now implemented across 14 states, enabling shared-service cybersecurity operations for over 2,600 local and educational entities. This model supports smaller agencies with enterprise-grade capabilities.	Senior SOC Architect
Program Management: Our Program Managers bring deep expertise in supporting Purchasing Entities with a wide range of program initiatives. This includes guidance on securing federal and state cybersecurity funding—such as ARPA, FEMA, and CISA grants—as well as assistance with procurement planning and implementation oversight. By aligning funding strategies with program goals, we help accelerate the deployment of risk mitigation efforts and ensure that initiatives are executed efficiently and effectively.	Senior Program Manager
Cloud Security Architecture and Advisory: Cloud Security Architecture and Advisory experts provide strategic guidance, architectural design, and in-depth assessments tailored to the unique needs of each client. We support secure cloud adoption and optimization across all major cloud platforms, including AWS, Microsoft Azure, and Google Cloud Platform. Our services encompass the design of secure and scalable cloud environments, evaluation of existing cloud infrastructures to identify vulnerabilities and compliance gaps, and the development of actionable remediation strategies. We also assist with secure cloud migrations, integrate security into DevSecOps pipelines, and ensure alignment with industry best practices and regulatory requirements. This holistic approach enables our clients to build resilient, compliant, and future-ready cloud ecosystems.	Senior Cloud Security Architect
Public Healthcare SME: This team of specialized health cybersecurity professionals provide tailored services for public health agencies and Medicaid providers, including HIPAA compliance, HITRUST readiness, MARS-E guidance, and risk management program development to meet OCR regulations.	Public Healthcare SME

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

OBSGlobal is not providing a response to Category 2- Incident Response and Services.

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

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.

OBSGlobal's Response
Our partnership with Polsinelli brings over two decades of experience delivering comprehensive breach response services to public and private sector clients. Given the legal focus of Category 3 activities, we offer NASPO members a highly qualified team with deep, practical expertise across the entire data breach lifecycle—from initial investigation through regulatory response, notification, and post-incident remediation. Polsinelli has been a national leader in breach response since 2003, when they managed one of the first high-profile cases under California's pioneering breach notification law. Since then, the firm has supported thousands of breach events across industries, including state and local governments, higher education institutions, healthcare systems, financial institutions, and insurance carriers. Their Data Breach & Incident Response team includes former U.S. Attorneys, Assistant U.S. Attorneys, officials from the Office of Inspector General (OIG), and in-house counsel from major public institutions—providing clients with unmatched insight into regulatory expectations and enforcement dynamics.

Polsinelli has represented clients in hundreds of regulatory investigations led by State Attorneys General, OCR, and other enforcement bodies. Their experience includes high-impact incidents such as:

- System-wide ransomware attacks affecting multi-agency networks
- Business email compromise and cyber extortion events
- Data loss from stolen devices and ATM skimming
- Website defacements and internal misconduct

Our proposed Breach Coach, Iliana Peters, formerly served as Deputy Director for the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), where she led national enforcement of HIPAA and advised on breach response policy. Her leadership ensures that NASPO members receive guidance grounded in both regulatory expertise and real-world enforcement experience.

Breach Coach services span the full breach lifecycle, including:

- Leading forensic investigations and coordinating with IT and PR teams
- Determining notification obligations under state and federal law
- Advising on communications with regulators, affected individuals, and the media
- Providing legal counsel on ethical, reputational, and compliance risks
- Representing clients in regulatory investigations and litigation
- Supporting proactive planning, including incident response plans and board-level training
- Supporting communication with law enforcement, credit monitoring vendors, forensic accountants, and other stakeholders

OBSGlobal complements this legal expertise with a team of project managers, technical forensic specialists, and incident responders who provide real-time impact assessments, root cause analysis, and recovery support when needed to best support the client.

This extensive experience in both public and private sector uniquely positions our team to deliver exceptional Breach Coach Services under this Master Agreement.

- **(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.

OBSGlobal's Response

Our partnership with Polsinelli offers NASPO members access to a highly credentialed and experienced team of Breach Response Specialists who meet and exceed the qualifications outlined in Attachment 02, Section 4.3. Our lead Breach Coach, **Iliana Peters**, brings unparalleled expertise in data privacy, cybersecurity law, and breach response, with a career that spans both federal enforcement and private sector advisory roles.

Iliana Peters is a nationally recognized authority on data privacy and security, with deep specialization in HIPAA, the HITECH Act, FERPA, the Privacy Act, and state-level breach notification laws. She served as Deputy Director for the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR), where she led national enforcement of HIPAA and co-authored the HIPAA Breach Notification Rule. During her tenure, she also trained State Attorneys General and collaborated with the Federal Trade Commission on joint enforcement actions—giving her a unique perspective on regulatory expectations and inter-agency coordination.

Since joining Polsinelli in 2018, Ms. Peters has served as a Breach Coach for a wide range of public and private sector clients, including those covered under cyber insurance panels. She holds the Certified Information Systems Security Professional (CISSP) credential, which reflects her ability to bridge legal and technical domains—translating cybersecurity best practices into actionable legal guidance.

The broader Data Breach & Incident Response team includes former U.S. Attorneys, Assistant U.S. Attorneys, in-house counsel from major public institutions, and forensic specialists. This interdisciplinary team has managed thousands of breach events and is equipped to support clients through every phase of the breach lifecycle, including:

- Immediate incident response coordination and forensic oversight
- Regulatory compliance and breach notification under federal and state laws
- Communications strategy for regulators, affected individuals, and the media
- Legal counsel on reputational risk, ethical considerations, and litigation exposure
- Representation in regulatory investigations and enforcement actions

The deep bench of Breach Coaches and supporting consultants allows us to scale to various client needs and regulatory environments. If additional Beach Coaches are needed, OBSGlobal will work with Polsinelli to secure a resource based on the following criteria:

- Minimum of 5 years of direct experience managing breach response for public sector or regulated entities
- Legal or technical certifications such as CISSP, CIPP/US, or CISM
- Demonstrated ability to lead cross-functional response teams and coordinate with third-party vendors, law enforcement, and regulatory bodies
- Experience advising on breach notification laws across multiple jurisdictions

This collaboration provide a seamless, end-to-end Breach Coach service offering that is fully aligned with NASPO ValuePoint's requirements. The team is prepared to respond immediately to a Triggering Event, guide Participating Entities through the appropriate response steps, and ensure compliance with all applicable legal and regulatory obligations.

- **(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.

OBSGlobal's Response
The team has established a high-availability response model to support Participating Entities with timely, coordinated, and compliant Breach Coach Services under Category 3. The service levels are designed to reflect the urgency and sensitivity of data breach

events, ensuring rapid mobilization and clear communication from the moment a Triggering Event occurs.

Response Times and Availability

Client responsiveness is a core philosophy and continues to be our highest priority to this day. As a result, phone calls are returned within **one hour.** Likewise, policy dictates that all emails are to be responded based on level of urgency, **but within the same day.**

Additionally, a group e-mail account is monitored 24/7 to ensure prompt response. Email receipt is acknowledged receipt within the hour, if not quicker. In terms of conflicts checks, Polsinelli have a dedicated team within the firm's conflict department that allows us to typically clear conflicts within **thirty minutes**.

Due to the deep bench of staff, the team is typically available for initial scoping calls within **thirty minutes** after receiving the initial request. The practice is to immediately acknowledge receipt of an assignment and provide available times for the initial scoping call to enable prompt scheduling of the call. We will then run the conflicts check and move forward with the scoping call. In incidents involving ransomware or other similar urgent matters, we can immediately make ourselves available for the initial scoping call, pending conflicts clearance. Following the initial scoping call, we will coordinate with the Contract Manager and provide the proposed Engagement Letter or other proposal response needs to the client within the hour.

Ongoing Communication and Coordination

OBSGlobal will assign a dedicated Project Manager to coordinate logistics, schedule regular status meetings, and serve as the liaison between the Participating Entity, Polsinelli, and any third-party vendors (e.g., forensic firms, PR agencies, credit monitoring providers) as appropriate for the requested scope of services. This ensures a unified and transparent response effort from start to finish.

To summarize responsibilities for Category 3: Breach Coach Services:

Contractor Responsibilities	Participating Entity Responsibilities
• Maintain 24/7 availability for breach intake and triage. • Establish the initial scoping call within thirty minutes of receiving request, and provide the proposed Engagement Letter or proposal response within the hour. • Provide a designated Breach Coach and legal team with experience in public sector breach response. • Coordinate team members to align legal and forensic response strategies. • Facilitate all required regulatory notifications, communications, and documentation.	• Promptly notify OBSGlobal/Polsinelli of a Triggering Event via the designated contact channel. • Provide relevant background information and access to internal stakeholders for scoping and investigation. • Review and execute the engagement letter and any required authorizations in a timely manner. • Coordinate with internal IT, legal, and communications teams to support the breach response process.

• Provide regular status updates and final reporting to the Participating Entity. • Ensure all services are delivered in accordance with applicable state and federal breach notification laws	

The team's commitment to timely, responsive communication is a cornerstone of the service delivery model. This dedication ensures that Participating Entities receive the support they need—when they need it—across all phases of breach response. Whether coordinating an initial scoping call, managing regulatory notifications, or providing ongoing legal and technical guidance, clear and immediate engagement remain a top priority. This responsiveness reflects our collective readiness and capability to effectively serve a diverse array of Participating Entities under the NASPO Master Agreement.

- **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.

OBSGlobal's Response

In addition to our Category 3: Breach Coach Services, our comprehensive team offers the following "Value-Added Services" to support clients' ability to prevent, detect, respond, and recover from security breaches:

Breach Coach Value Added Services	Attachment 09 - Pricing Correlation Role
Technical and Legal Assistance which includes expert guidance on regulatory enforcement actions related to data breaches, including representation during investigations initiated by federal and state agencies such as the U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR), the Federal Trade Commission (FTC), and State Attorneys General. We also offer litigation support for breach-related legal proceedings, including individual claims and class action lawsuits. In addition to breach response, we provide ongoing consultation on compliance with key data protection laws such as HIPAA, GDPR, CCPA, and other federal and state privacy regulations. Recognizing the growing role of Artificial Intelligence in public sector operations, we also offer strategic advisory services focused on AI governance and compliance. This includes guidance on algorithmic transparency, ethical use of AI, data governance, and adherence to emerging regulatory frameworks governing automated decision-making and machine learning technologies. Additionally, we frequently develop and provide training programs to clients for their in-house legal teams and operational teams.	Technical and Legal Assistance
Cybersecurity Workshop and Tabletop: Raising awareness about cyberthreats is a critical part of preventing incidents. When key decision-makers understand the frequency of attacks and their potential financial and reputational fallout, they are more likely to support cybersecurity initiatives that reduce the likelihood of an	Table Top Exercise Specialist

incident. Moreover, walking through a simulated incident helps an organization identify gaps in its response process and better situates it to respond to a real incident. Conducting this type of workshop will put the organization in a position to improve its preparedness and streamline its incident response processes. • 2-4 hour workshop with leadership and incident response teams, which consists of the following: • an overview of data breach trends and the cyber/ privacy legal landscape • a tabletop simulating a real-world data breach scenario that develops in phases, discussing at each step how the organization would respond based on the facts available.	
Forensic Assistance provides in-depth support during active incident response such as forensic analysis on: • Hard drives from affected systems. • Memory dumps from potentially compromised devices. • Mobile devices within the impacted environment. • Credit card endpoint devices requiring forensic review. • Analyzing network traffic traversing internal and external boundaries	Forensic Specialist

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

OBSGlobal is not providing a response to Category 4 - Notification and Credit Monitoring Services.

- **(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.

AMD 2 E. ~~(ME)~~ (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.

OBSGlobal's Response

Our dedicated focus on cybersecurity services has enabled us to develop a robust network of industry partners with complementary expertise, allowing us to deliver a **"best-of-breed"** solution tailored to the unique needs of our public sector clients.

Under this Master Agreement, OBSGlobal will serve as the Prime Contractor, maintaining full responsibility for contract performance, compliance, and oversight. We will manage all aspects of service delivery and coordination, ensuring that any subcontractor engagement enhances—not complicates—the client experience.

Subcontractors will only be engaged with prior written approval from the Lead State or Participating Entity, in full accordance with the terms of the Master Agreement. OBSGlobal will ensure that all subcontractors meet or exceed the minimum qualifications, insurance requirements, and service standards outlined in the agreement.

Category 1: Risk Assessment and Mitigation Services Subcontractors

BISBLOX

OBSGlobal intends to strategically engage BisBlox, LLC as a subcontractor under this Master Agreement to support specific service Categories related to Category 1: Risk Assessment and Mitigation Services. BisBlox, a certified Minority-owned, Service-Disabled Veteran-led firm headquartered in Bismarck, North Dakota, brings nationally recognized expertise in public sector cybersecurity innovation and operational resilience.

BisBlox's executive team averages over 20 years of experience across C-suite roles and leads a network of more than 300 professionals with deep cross-sector knowledge. Their mission—Be Bold. Disrupt Boring. Strengthen Growth.—is reflected in their transformative work with government entities across the country. One of their most impactful contributions is the development and operationalization of the Joint Cyber Security Operations Center (JCSOC) model, which has been

implemented in 14 states and supports over 2,600 local and educational entities. This model has significantly reduced cybersecurity staffing burdens and costs—saving **over $400 million in projected expenses** in North Dakota alone—while enhancing visibility and resilience across jurisdictions.

BisBlox's services include comprehensive cyber risk assessments, maturity modeling, control validation, inter-agency risk exposure mapping, and real-time telemetry analysis. These capabilities directly enhance our ability to bring additional Value Added Services under Category 1 of the Master Agreement.

In North Dakota, team led a transformative statewide cybersecurity initiative centered around a comprehensive Risk Assessment and the implementation of the Joint Cyber Security Operations Center (JCSOC) model. This engagement supported the cybersecurity needs of over 400 government entities, including state agencies, counties, cities, tribal governments, K–12 school districts, and higher education institutions.

HealthTech SOLUTIONS

As a value-added service, OBSGlobal has established strategic partnerships with specialized vendors to enhance our ability to deliver targeted subject matter expertise and scalable project support tailored to client needs. A key partnership in this ecosystem is with HealthTech Solutions, a nationally recognized consulting and technology firm with deep domain expertise in the health and human services (HHS) sector.

Through this collaboration, HealthTech Solutions complements OBSGlobal's core capabilities by providing specialized knowledge in business process optimization, regulatory compliance, and domain-specific functions that intersect with cloud services and cybersecurity. Their experience spans engagements with over 30 states, including State Medicaid Agencies (SMAs), HHS departments, Fortune 500 companies, top 25 Managed Care Organizations (MCOs), and the Centers for Medicare and Medicaid Services (CMS) through a subcontract with the Urban Institute.

HealthTech Solutions is a GSA Schedule holder and a pre-qualified vendor on the New Mexico Statewide Pricing Agreement. They also hold a NASPO Cloud Services price agreement through Carahsoft, which has been leveraged for statewide contracts in Arizona and Hawaii—demonstrating their credibility and reach within the public sector procurement landscape.

Their involvement is particularly valuable in projects requiring a nuanced understanding of HHS operations, where their insight helps enhance risk mitigation strategies, inform secure and compliant system design, and align solutions with federal and state program requirements. OBSGlobal anticipates leveraging HealthTech's deep industry knowledge to strengthen our service delivery for public sector clients—ensuring that our solutions are not only technically robust but also contextually informed and operationally relevant to the realities of HHS agencies.

Category 3: Breach Coach Services Subcontractor

POLSINELLI

Given the potential need for legal expertise outlined in the Scope of Work for Category 3: Breach Coach Services, OBSGlobal has partnered with Polsinelli, a nationally recognized law firm, to deliver Purchasing Entities a fully integrated and comprehensive breach response solution.

Polsinelli is one of the largest law firms in the United States, with a broad national presence and deep experience across a wide range of legal disciplines. Their Data Breach & Incident Response

team includes former in-house counsel from major healthcare institutions, former officials from the Office of Inspector General (OIG), and former U.S. Attorneys and Assistant U.S. Attorneys—many of whom have direct experience advising public sector clients. This interdisciplinary team brings unmatched legal insight and practical experience to support public entities through every phase of a cybersecurity incident.

Breach Coach Services provide centralized legal coordination during a breach, including oversight of forensic investigations, regulatory compliance, notification obligations, and post-incident litigation or enforcement response. Their attorneys are among the most experienced in the country, offering both legal protection and strategic guidance tailored to the unique needs of government agencies and public institutions.

OBSGlobal complements Polsinelli's legal leadership with a team of technical forensic specialists and incident responders, enabling a seamless, end-to-end breach response capability. Our role serves to provide actionable insights and impact assessments derived from forensic analysis and incident response activities, ensuring that legal and technical efforts are aligned from the outset.

This collaboration includes a coordinated approach to engagement management and third-party support, including but not limited to:

- Facilitating in-briefings and regular status meetings to maintain alignment and transparency
- Assisting clients in coordinating with external stakeholders involved in the incident response process, including vendors, regulators, and law enforcement
- Coordinating internal and external resources to meet response timelines
- Providing regular status updates to stakeholders
- Delivering final reports summarizing findings, impact, and recommendations

Together, this team offers scalable Breach Coach solution that meets the highest standards of legal, technical, and operational excellence—ensuring public sector clients are fully supported before, during, and after a cybersecurity incident.

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.

OBSGlobal's Response

OBSGlobal has steadily expanded its presence nationwide, partnering with state and local government organizations to deliver specialized cybersecurity services. Our extensive expertise in security and privacy enables us to collaborate with a wide range of consulting firms and strategic partners to support complex IT projects—including security and risk assessments, strategic roadmapping, technical testing, Security Operation Center (SOC) development, and implementation efforts—for agencies across Wyoming, Minnesota, Idaho, New Mexico, Mississippi, California, Oregon, and Washington.

In addition to our public sector work, our experience with private sector organizations—including Fortune 10 companies—has equipped us with deep expertise in regulatory compliance, cybersecurity frameworks, advanced tools, and effective remediation strategies. This broad exposure enables us to address the evolving cybersecurity threats facing our clients with agility and insight.

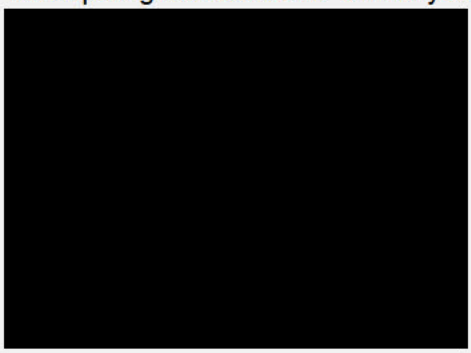
Our business development strategy emphasizes statewide and large-scale consortium contracts, recognizing the critical need for timely cybersecurity services. Traditional procurement processes often fall short in meeting urgent security demands. We understand the efficiencies and responsiveness that these contract structures offer Participating Entities, and we are committed to delivering secure, scalable solutions through these models.

We designate a dedicated team of Business Development Leads directed by our Contract Manager to oversee each consortium contract to identity targeted opportunities and foster the relationship with contract participants. All opportunities are funneled through our centralized Proposal Center, where they undergo an initial qualification process and a go/no-go decision. This evaluation is conducted in collaboration with key internal subject matter experts (SMEs) to ensure we have the appropriate resources and expertise to deliver the requested services at the high standard of quality we uphold. If the opportunity is advanced to the next stage, our Proposal Center will coordinate with our SMEs to support the scoping of the requested scope of work.

We have successfully completed managed similar consortiums and task-order based Master Agreements for agencies across the US, including:

- Washington Health Care Authority
- Mississippi Department of Information & Technology Security Services
- Minnesota MNSITE 2.0 Professional and Technical Master Contract
- Wyoming Community College Commission

In addition, our firm has established itself as a leading security consulting provider for Health Center Controlled Networks (HCCNs), with provides us added experience managing large-scale, consortium-style contracts under HRSA grant recipients. We have successfully partnered with the following HCCNs across the country to deliver concurrent risk assessments, mitigation services, and a range of technical assistance to their 200+ Participating Members over a multi-year contract period:



As part of our awarded HCCN contracts, the assigned Business Development Lead meets regularly with the designated HCCN point of contact (POC) to review active and completed task orders, provide updates on ongoing activities, and plan for upcoming initiatives or potential Health Center targets. Task orders are issued by the HCCN under our Master

Agreement to support work identified by Participating Members. Given that these initiatives are often grant-funded, our Business Development Lead or designated Project Manager maintains detailed records of all billed activities and services, and delivers monthly reports to the HCCN to support ongoing grant administration and compliance requirements.

To maximize the impact of our services through HCCN partner contracts, our team actively engages in outreach and education by hosting webinars, participating in regional conferences, and organizing live events tailored to the needs of HCCN network partners. These efforts not only expand the reach of our security services but also enhance the value HCCNs deliver to their member Health Centers and Primary Care Organizations. Our proven ability to scale services through these contract vehicles contributes to both our continued growth and the success of our HCCN partners.

Our expertise in this space is best illustrated through the following sample contracts. It's important to note that, based on our selected categories of services and publicly available data, risk assessment engagements typically range from $25,000 to $250,000, depending on the chosen framework and the complexity of the assessment.

Client	Contract Scope	~Dollar Value
[redacted]	OBSGlobal and its partners contracted with the state to conduct a baseline assessment of internal risk readiness and security operations. The goal was to identify gaps and develop a comprehensive roadmap and implementation plan aimed at reducing statewide risk and enhancing the prevention and detection of cyber threats.	[redacted]
[redacted]	[redacted] [redacted] • NIST Threat-Based Risk Assessments for over 25 participating health centers, using NIST CSF and NIST SP 800-53 as foundational frameworks. • Security Posture Evaluations and Gap Analyses to identify vulnerabilities and prioritize remediation. • Custom Maturity Roadmaps using our proprietary assessment tooling to guide centers through phased improvements in	[redacted]

	cybersecurity governance, controls, and resilience. • Policy and Procedure Development aligned with HIPAA, NIST 800-171, and MARS-E. • Incident Response Tabletop Exercises testing Incident Response Plans, both virtually and in-person for health center staff, providing after-action recommendations and prioritized remediation. • Cybersecurity Awareness Campaigns and Training deploying customized simulated phishing campaigns and provide tailored cybersecurity awareness training for clinical and key administrative staff. The combined findings from the initia[redacted] center risk assessments were synthesized into a prioritized list of the top 10 most common cybersecurity issues. This list was shared with the remaining [redacted] member centers, enabling them to proactively address high-risk areas and benchmark their own security posture against peer organizations. [redacted]	
[redacted]	[redacted]	

Additionally, we are currently in process of finalizing two long-term projects stemming directly from an existing statewide Master Service Agreement model. In these examples, we leveraged our existing contract vehicle to develop a targeted Statement of Work to the requesting state to support a detailed request for security support on long-term IT initiatives.

In addition to our US-based contract, our team is also actively managing work under several Vendor of Records (VOR) in the Canadian market, including:

- Government of Manitoba
- City of Winnipeg
- Manitoba Public Insurance
- Manitoba Agriculture Services Corporation
- Ontario Ministry of Government and Consumer Services
- Manitoba Liquor and Lotteries
- The Workers Compensation Board of Manitoba
- WestJet, Alberta Partnership

In alignment with our U.S.-based consortium contracts, our designated Business Development Lead oversees the client relationship and actively monitors for new opportunities issued under the VOR. All opportunities are funneled through our centralized Proposal Center, where they undergo qualification, scoping, and delivery of the requested proposal or Purchase Order.

This collective experience across North America further demonstrates our unified corporate strategy to target and grow our business through long-term relationships with our public sector agencies and partners.

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

OBSGlobal's Response

OBSGlobal is committed to maximizing the visibility and adoption of the Master Agreement across state governments and other Participating Entities. Our tiered approach combines strategic outreach, targeted marketing, and thought leadership to ensure broad engagement and sustained participation while recognizing the confines of public sector marketing rules and restrictions.

Tier One: Relationship-Driven Outreach

The foundation of our strategy lies in leveraging our deep-rooted network of relationships with state and local agencies—connections built through years of successful public sector engagements by our consultants and partners. Our track record of success is built on the foundation of these authentic, long-standing connections. We focus our efforts where we know we can deliver the greatest value, targeting opportunities that align with our strengths and enable us to drive meaningful outcomes for our clients.

We will develop specific communication materials and campaigns to target our network to advertise the NASPO Master Agreement and options in accordance with the terms and agreements outlined in the Master Agreement. We will complement our targeted materials with meetings and discussions on how to best leverage the NASPO Master Agreement to align with client needs and future opportunities.

Tier Two: Strategic Targeting and Localized Engagement

To expand awareness and engagement with the NASPO Master Agreement, our second tier focuses on applying data-driven insights and procurement intelligence to identify and prioritize strategic states. This process includes a thorough evaluation of legislative trends, procurement cycles, and—critically—our organizational fit with each potential client. By assessing where our capabilities align most effectively with Participating Entities' needs, we

ensure that our outreach efforts are both targeted and impactful, maximizing the likelihood of successful adoption and long-term value creation.

In regions identified in our strategic plan, we invest in localized marketing efforts and actively participate in regional conferences, such as the Minnesota GovIT Symposium and the Rocky Mountain User Group Conference. These events allow us to engage directly with decision-makers in environments tailored to their unique challenges. Additionally, our team regularly contributes to local chapters of professional organizations such as HIMSS, Information Systems Security Association (ISSA), and InfraGard. These forums provide valuable opportunities for ongoing dialogue and relationship-building with potential clients in a more intimate, trusted setting.

Through these focused efforts, we aim to grow our client base and expand our network, uncovering new opportunities to maximize the value of the NASPO Master Agreement model.

Tier Three: Scalable Campaigns to Improve Visibility

The third tier of our strategy is designed to reach a broader audience through scalable, marketing strategies intended to target procurement officials, IT leaders, and agency executives. Our core methods include:

Digital Campaigns: We will leverage our Hubspot tool to launch campaigns to targeted contacts, coupled with prospecting ads on Linkedin that target new contacts based on location, titles, and potential organization. We will also leverage social media platforms to amplify key messages, share success stories, and promote upcoming events or webinars. Engagement metrics will be closely monitored to refine our messaging and identify high-interest regions, ensuring our outreach remains effective and responsive to market needs.

Immersive Website: We will develop a dedicated landing page to serve as a central hub for our NASPO-related services and marketing campaigns. As further in detailed in our response below, our website will include resources, such as FAQs, scoping and pricing guides, NASPO Master Agreement information, and contact information for direct support. The Website will aggregate published articles, blogs, eBooks, and whitepapers authored by internal thought leaders.

We are successfully managing similar sites such as our PCI DSS Resource Site and healthcare-focused OnPulse Health CyberCenter, which provides resources to our HCCN clients to help serve their collective 200 networked Health Centers across the country.

Conference Attendance: Our focused team actively participates in national and regional conferences across the country, where we regularly present and engage with public sector leaders. We often sponsor selected conferences or events based on our targeted client attendees to allow us additional opportunities for personal connections and touch points. We are, by design, not a Big 4 consulting firm, so put extra effort into designing conference strategies and events that will appeal to our target buyers.

Webinars and Thought Leadership: Our team regularly contributes and hosts industry webinars and panels, reinforcing our position as a trusted advisor in the public sector space. This visibility not only strengthens our brand but also fosters trust and interest among potential Participating Entities. To highlight:

- **Jeff Man** is a highly respected advocate and advisor in the field of Information Security, known for his deep expertise, thought leadership, and decades of hands-on experience.

He has served as a hacker, mentor, teacher, international keynote speaker, and former host of Security & Compliance Weekly, as well as a co-host on Paul's Security Weekly. Jeff is also a contributor to the Tribe of Hackers series, including the Red Team, Security Leaders, and Blue Team editions, and is a member of the Cabal of the Curmudgeons. Currently, Jeff serves as a PCI Qualified Security Assessor (QSA) and Trusted Advisor at OBSGlobal. He also contributes to the broader cybersecurity community as a Grant Advisory Board Member for the Gula Tech Foundation, an Advisory Board Member for the Technology Advancement Center (TAC), and as the Director of Diversity, Equity, and Inclusion for Hak4Kidz NFP. Earlier in his career, Jeff was a Certified Cryptanalyst with the National Security Agency (NSA), where he designed and deployed the agency's first software-based cryptosystem. He is the inventor of the "whiz wheel," a cryptologic cipher tool used by U.S. Special Forces for over a decade and now displayed at the National Cryptologic Museum. Jeff was also a pioneering member of the NSA's first penetration testing red team and has held leadership roles in security research, product development, and management across both government and private-sector organizations.

Iliana Peters regularly co-chairs national forums, including the HIPAA Sumit. Her expansive list of events and publications are available at: https://www.polsinelli.com/iliana-l-peters/events Most recently, Iliana and her team were recognized in the 2025 Chambers USA Guide for top lawyers and firms in our country.

Shawn Riley brings first-hand state security experience as the former CIO & Cabinet Member of North Dakota and was pivotal in leading the state to be the first state in the nation to have seven branches of government cyber security strategy. Shawn holds several national award winner for Government Experience and Cyber Education Programs. Shawn is a regular contributor to the CyberWire's network of webinars and podcasts, specifically the CSO Perspectives Podcast, providing expert commentary and sharing professional insights to their global audience of cybersecurity professionals.

This multi-channel strategy ensures that the Master Agreement is not only well-publicized but also positioned as a valuable, easy-to-adopt solution for Participating Entities nationwide.

- 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.

OBSGlobal's Response

OBSGlobal will develop a dynamic, interactive landing page to serve as the central hub for our NASPO-related services and marketing efforts. Building on the proven success of our PCI DSS Resource Site and healthcare-focused OnPulse Health CyberCenter, this dedicated site will be designed to meet the unique needs of public sector clients by offering intuitive access to relevant tools and information.

Upon award, our in-house development team will enhance the site with a suite of resources, including FAQs, scoping and pricing guides, NASPO Master Agreement details, and direct contact options for personalized support. To further streamline user experience, we will integrate AI-powered where agents, where appropriate, capable of

triaging inquiries and routing users to the appropriate team members quickly and efficiently.

To drive engagement and deliver ongoing value, the site will feature a curated library of thought leadership content—including articles, blogs, eBooks, and whitepapers—authored by our internal experts and trusted partners. This content-rich approach will position the site as a go-to resource for NASPO-related insights, helping Purchasing Entities stay informed and empowered throughout the purchasing lifecycle.

- 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.

OBSGlobal's Response

OBSGlobal will integrate the NASPO ValuePoint Master Agreement into its Enterprise Sales structure into the to ensure a coordinated, responsive, and compliant approach to serving Participating and Purchasing Entities. We allocate a dedicated team of experienced professionals and supporting resources to manage all aspects of the agreement—from opportunity identification to contract execution and delivery oversight.

At the core of this structure is our **Contract Manager**, who serves as the internal lead for the Master Agreement. This individual is responsible for overseeing strategy, compliance, partner coordination, and alignment with public sector trends and legislative developments. The Contract Manager works closely with our Business Development Directors and Service Line Leads, each of whom is assigned to a specific region and serves as the primary sales contact for their territory. Together, they ensure that all opportunities under the Master Agreement are managed with consistency, responsiveness, and a deep understanding of client needs.

Supporting this team is our Proposal Contact, which collaborates with Business Development, Proposal Center, and subject matter experts to scope, qualify, and respond to opportunities. We use a centralized Salesforce CRM platform to manage opportunity intake, triage, and tracking. Opportunities are typically submitted via an internal Intake Form, which populates a shared queue reviewed during stand-ups. If a more immediate response is needed, the opportunity is internally escalated through our dedicated Teams channels for triage.

This process, as outlined below, allows us to remain agile and responsive without the administrative overhead of larger firms.

Once an opportunity is qualified, our team leverages internal SMEs, delivery leads, and partner resources to scope the engagement and develop response strategies that align with the Master Agreement's terms. The Contract Manager, in coordination with our Managing Partner and partner liaisons, will finalize agreements and ensure compliance with all contractual requirements. Upon award, the Contract Manager and Business Development Lead coordinate with our assigned team to conduct a formal project kickoff with the client and delivery team, ensuring a smooth transition from sales to execution.

To ensure all staff and partners are fully informed and compliant with the Master Agreement, OBSGlobal will develop and deliver custom NASPO-specific training. This training will cover the agreement's terms, pricing structure, reporting requirements, and compliance obligations. Initial training will be conducted upon contract award, followed by quarterly refresher sessions aligned with sales reporting cycles. In addition, we use our weekly Business Development calls as an ongoing forum to reinforce key contract elements, share updates, and address questions in real time.

This integrated staffing model, supported by robust tools and continuous training, ensures that OBSGlobal can manage the Master Agreement efficiently, maintain full compliance, and deliver exceptional service to NASPO members.

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

OBSGlobal's Response

OBSGlobal is committed to driving adoption and usage of the NASPO ValuePoint Master Agreement through our comprehensive, multi-tiered outreach strategy that combines targeted relationship-building with scalable marketing efforts.

Our approach begins with leveraging our extensive network of existing public sector clients and strategic partners. Through direct engagement—such as in-person meetings, executive briefings, conference attendance, and program-level discussions—we will educate agency leaders and procurement officials on the benefits of utilizing the Master Agreement. These conversations allow us to address common concerns, clarify perceived limitations, and demonstrate how the agreement streamlines procurement, reduces administrative burden, and accelerates time-to-value.

To complement our relationship-driven outreach, OBSGlobal will deploy a tailored marketing strategy that includes customized collateral, case studies, and success stories that highlight how similar agencies have benefited from engagements that would fall under the scope of this Master Agreement. These materials will be distributed through digital campaigns, webinars, and targeted email outreach to ensure broad visibility across Participating and Purchasing Entities.

Additionally, we will develop a dedicated landing page and resource hub that outlines the value proposition of the Master Agreement, provides step-by-step guidance on how to participate, and showcases the breadth of services available. This digital presence will be supported by ongoing social media engagement and participation in relevant public sector conferences and procurement forums.

By combining personalized relationship management with scalable, informative marketing, OBSGlobal will actively promote the Master Agreement as a trusted, efficient, and flexible

procurement vehicle—ultimately driving awareness, adoption, and long-term usage across the NASPO ValuePoint network.

- 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?)

OBSGlobal's Response

At OBSGlobal, we take a flexible and collaborative approach to contracting. Our organizational size and culture promote agility, allowing us to respond quickly to the unique needs of Participating Entities without the layers of bureaucracy often found in larger firms. We understand that each entity may have specific statutory, regulatory, or operational requirements, and we are committed to accommodating those needs wherever possible.

To streamline the process, we plan to leverage our existing Statement of Work templates and standard terms and conditions to develop a Participating Addenda Template that aligns with the appropriate NASPO Master Agreement terms and the awarded service category offerings. Our goal is to offer a "catalog-style" Participating Addendum that enables Participating Entities to easily select from our standard service offerings while also proposing entity-specific terms for added flexibility in a standardized form-like document.

We do not require statutory citations for every customization, though we welcome them when available to ensure compliance and clarity. Additionally, we are prepared to dedicate resources to support the simultaneous negotiation of multiple Participating Addenda, ensuring timely and efficient onboarding for interested entities across jurisdictions. Our Contract Manager will be primarily responsible for coordinating internal resources required to support the successful execution of Participating Addenda.

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

OBSGlobal's Response

Our organizational size and structure enables us to prioritize client needs and respond swiftly to service requests. Our mature operational framework, pre-defined service offerings, and an extensive bench experienced consultants and partners support our rapid response and execution of public sector engagements.

As detailed in our Intake and Triage process above, we've established internal workflows and recurring touchpoints to evaluate and respond to opportunities in a timely and efficient manner. Our team is empowered through multiple communication channels, allowing for real-time collaboration and the ability to escalate to subject matter experts or Managing Partners when a faster response is required.

A key component of our readiness is our dedicated Resource Director, who actively manages our scalable bench of qualified professionals. This role works closely with Service Line Leads, Business Development Leads, and the Contract Manager to monitor availability and quickly mobilize the right resources to support new opportunities.

To further accelerate service delivery, we utilize our service catalog, standardized pricing models, and templated Participating Addenda. This approach minimizes administrative

overhead and enables Participating Entities to access our services efficiently—ensuring we can begin delivering value immediately upon contract execution

- 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.

OBSGlobal's Response

OBSGlobal will leverage its robust and proactive sales reporting framework to ensure that summary and detailed sales information is promptly, completely, and accurately reported by our team and partners in compliance with the NASPO ValuePoint Master Agreement.

Centralized Oversight:
Our dedicated Contract Manager will serve as the primary point of contact and coordinator for all NASPO-related activities. This individual will work closely with our Business Development Directors and strategic partners to ensure timely and accurate data collection and reporting.

Direct Engagement and Coordination:
Because OBSGlobal will maintain a direct role in every engagement under the NASPO Master Agreement, we are well-positioned to actively manage and oversee the flow of sales data from all participating entities. We will maintain regular communication with our partners to ensure that all sales transactions are captured and submitted in accordance with NASPO's reporting schedule.

Technology-Driven Reporting:
We utilize Salesforce, our enterprise-grade CRM platform, to track all opportunities and associated contacts. To align with NASPO ValuePoint's reporting requirements, our internal Salesforce development team will implement a custom opportunity record structure that mirrors the data fields required in the NASPO Sales Report Template. This tailored configuration enables us to generate standardized, export-ready reports that ensure accuracy, completeness, and consistency.

Quality Assurance:
Before submission of any Sales Report, all sales data will undergo a thorough review process to validate completeness and accuracy. This includes cross-checking partner submissions against internal records and automated data integrity checks within Salesforce.

Through this integrated approach—combining centralized oversight, direct partner coordination, and customized CRM reporting—OBSGlobal ensures full compliance with NASPO ValuePoint's sales reporting requirements.

G. (ME) **Customer Service**

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

OBSGlobal's Response

Our white-glove approach to customer service includes providing direct contact information for the assigned point of contact (POC) for each engagement. Every client has direct access

to their team—there are no outsourced call centers or intermediaries, ensuring our clients always interact with professionals who are directly involved in your engagement.

Each client engagement is generally supported by a dedicated Project Manager, who serves as the primary point of contact to ensure streamlined communication and prompt issue resolution. In addition, clients are provided with direct contact information to key personnel assigned to their account, including but not limited to:

- **Business Development Leads** for strategic guidance
- **Contract Manager** for contract compliance and reporting
- **Managing Partner** for executive-level oversight and escalation

While our core hours define our standard availability, we have a distributed US team of consultants that span West to East time zones, aligning to each member's local time zone where typical working hours range from 7 AM PT to 6 PM PT. Given the urgency of Breach Coach service requests, customer service is available 24/7 through a centralized email.

Our team remains flexible and responsive to client needs outside of these hours when necessary. We are committed to ensuring that our clients can reach knowledgeable, accountable professionals who are directly involved in their engagement—whenever support is needed.

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

OBSGlobal's Response

OBSGlobal takes a proactive and structured approach to identifying and resolving service issues and customer complaints, with a strong emphasis on transparency, accountability, and responsiveness—values that align with the expectations of our public sector clients. At each stage of the engagement, we assign a single point of contact to streamline communication and ensure continuity.

During the **pre-sales and sales phase**, the designated Business Development Lead serves as the client advocate, addressing concerns and coordinating internal resources, including our Contract Manager.

Once the engagement is active, a dedicated Project Manager typically becomes the primary liaison, working closely with the client to implement a communication strategy that emphasizes early risk identification and mitigation. Regular internal reviews and client status meetings are conducted to monitor progress and flag potential issues before they escalate.

When problems do arise, they are triaged and escalated as needed to the Contract Manager for compliance matters or to the Managing Partner for executive oversight. Our team collaborates internally to develop resolution strategies, which are then reviewed with the client to ensure alignment and transparency.

We also offer regular customer satisfaction meetings—monthly, quarterly, or annually, based on client preference—to proactively address concerns, review performance, and identify opportunities for continuous improvement. This comprehensive approach ensures that issues are resolved efficiently and that our public sector clients receive the high level of service and accountability they expect.

- Describe how you will assess customer satisfaction.

OBSGlobal's Response
OBSGlobal employs a multi-layered approach to assessing customer satisfaction, ensuring that client feedback is continuously gathered, evaluated, and used to improve service delivery. At the core of this approach is the designated Business Development Lead, who serves as the primary client advocate throughout the engagement. This individual maintains regular communication with client stakeholders to understand evolving needs, ensure responsiveness, and confirm that our services are aligned with client expectations. By staying closely involved, the Business Development Lead can proactively identify areas for improvement and ensure that the right resources are deployed at the right time. In parallel, our Contract Manager provides oversight for all public sector engagements and facilitates periodic check-ins—both internally and with client teams—to assess satisfaction levels and ensure alignment with contractual and performance expectations. These touchpoints are structured to capture both qualitative and quantitative feedback, allowing us to make real-time adjustments when necessary. To formalize our feedback process, OBSGlobal conducts post-engagement "Lessons Learned" sessions with both internal teams and client stakeholders. These sessions are designed to capture insights on what worked well, what could be improved, and how future engagements can be optimized. Additionally, we administer customer satisfaction surveys at key milestones and at the conclusion of each engagement. These surveys are tailored to the public sector context and focus on service quality, communication, responsiveness, and overall satisfaction. This comprehensive feedback loop—combining ongoing dialogue, structured reviews, and formal surveys—ensures that OBSGlobal remains responsive to client needs and continuously improves the quality of our services.

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

OBSGlobal's Response
OBSGlobal contracted with CPA firm, Linford&Co LLP, to examine its infrastructure and application managed services and client portal solution titled, "Online's Description of Its Infrastructure and Application Services and Client Portal Solution" throughout the period January 1, 2024 to December 31, 2024 based on the criteria for a description of a service organization's system in DC section 200, 2018 *Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, Description Criteria) (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 2024 to December 31, 2024 to provide reasonable assurance that OBSGlobal's service commitments and system requirements were achieved based on the trust services criteria relevant to security set forth in TSP section 100,

2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

The Report concluded that:

a. The description presents OBSGlobal's infrastructure and application managed services and client portal solution that were designed and implemented throughout the period January 1, 2024 to December 31, 2024 in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period January 1, 2024 to December 31, 2024 to provide reasonable assurance that Online's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of OBSGlobal's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period January 1, 2024 to December 31, 2024 to provide reasonable assurance that OBSGlobal's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of OBSGlobal's controls operated effectively throughout that period.

A copy of the Report is available upon request.

In addition, OBSGlobal maintains a corporate Information Security Policy, which is read and acknowledged by each employee upon hire and on an annual basis. OBSGlobal's leadership team is committed to this policy to ensure our corporate and our client's critical assets are protected. OBSGlobal also has a Privacy Policy in place to protect our clients' and staff privacy.

OBSGlobal performs annual risk assessments and security reviews of its infrastructure. The scope of this review includes repositories where client artifacts and reports are stored as well as authentication mechanisms to protect those artifacts. Our dedicated Cybersecurity Practice is organizationally independent of the personnel who maintain OBSGlobal's infrastructure services.

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

OBSGlobal's Response

Our organization enforces strict safeguards, protocols, and oversight mechanisms for the responsible use of AI, governed by a formal AI Usage Policy, supported by our SOC 2 Type II certification, and enabled through secure infrastructure, including a private instance of GitHub Co-Pilot. Following is OBSGlobal's governance of AI usage:

- **SOC 2 Type II Controls:** Our SOC 2 Type II certification ensures we meet rigorous standards for data security, availability, and confidentiality—critical for governing AI tooling and workflows. All AI use is aligned with these audited controls, including access restrictions, activity monitoring, and secure data management practices.

- **AI Usage Policy and Governance Framework:** We maintain a formal, organization-wide **AI Usage Policy** that governs all aspects of AI integration, from procurement and evaluation to deployment and decommissioning. This policy includes clear boundaries on the use of generative AI, mandates human review for critical outputs, and outlines acceptable use standards tailored to client-specific risk profiles.

Although we see AI as an effective tool to optimize workflows and business processes, we as security consultants have a unique appreciation for the risk factors associated AI tools and technologies and are sensitive to balance the efficiencies with the potential impacts AI introduces to a business.

Internally, we have identified two potential AI tools that may be used to support work under Category 1 and Category 3 of this Master Service Agreement:

- **Private GitHub Co-Pilot Instance:** To support secure AI-assisted development, our teams utilize a private, enterprise instance of GitHub Co-Pilot, ensuring that AI code suggestions are contained within our internal environment and do not transmit client code or intellectual property to public models. This allows us to leverage AI productivity gains while retaining full control over data residency, privacy, and security. Although we do not anticipate using Co-Pilot on any client-specific Risk Assessments or data, it may be used to implement enhancements to our internal Security Risk Assessment tooling.
- **Loopio:** Our Proposal Center utilizes the AI-powered Loopio platform to improve efficiency and precision in proposal development. While we do not anticipate employing Loopio for any executed Purchase Orders under the Master Agreement, it may be used to support the creation of requested proposals or related business development materials. This enables us to respond to Participating Entities more effectively and in a timely manner.

And as a final safeguard, we require **human oversight for all AI-generated outputs**—including those from Co-Pilot and other tools—are reviewed by qualified team members to ensure correctness, compliance, and context-appropriate results. No automated output is deployed or relied upon without human validation.

VII. ACKNOWLEDGEMENTS AND CERTIFICATIONS

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

A. <u>Debarment.</u> (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.

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

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

Date

Rob Harvey

Managing Partner

Printed Name

Title

rharvey@obsglobal.com

404.452.7452

Email Address

Phone Number