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: Cogent Infotech Corporation
B. Primary Business Address: 1035 Boyce Rd, Pittsburgh, PA 15241
C. Federal Tax Identification Number: 32-0083904
D. Entity Type:

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

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

- ☐ Yes
- ☒ No

III. BUSINESS DETAILS

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

https://www.cogentinfo.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.

Founded in 2003, Cogent Infotech Corporation (Cogent) is a nationally recognized consulting firm headquartered in Pittsburgh, Pennsylvania. With over 21 years of experience, Cogent has been a trusted partner to more than 150 public sector clients, including federal, state, and local governments, as well as higher education institutions.

Cogent has not been involved in any mergers or acquisitions since its inception. The company has achieved sustained, organic growth driven by its commitment to quality, innovation, and public sector value delivery. We have built a strong reputation by delivering specialized services in risk assessment, mitigation, and breach response management. Our expertise is centered on supporting organizations in proactively identifying Cybersecurity risks, developing strategies to mitigate them, and providing critical incident response services during and after security breaches. Our deep experience in these areas has positioned us as a preferred partner for government agencies looking to enhance their Cybersecurity resilience and ensure compliance with security regulations.

Our services in Risk Assessment and Mitigation (Category 1) and Breach Coach Services (Category 3) are at the core of our Cybersecurity offerings. These include:

- **Risk Assessment and Mitigation:** Conducting vulnerability assessments, privacy impact analyses, and developing actionable mitigation strategies in alignment with industry standards.
- **Breach Response:** Providing expert support for managing and mitigating data breaches, including crisis management, legal compliance, and communication strategies.
- **Incident Response Management:** Offering services that help organizations contain and eradicate threats, recover systems, and perform forensic analysis.
- **Breach Coaching:** Assisting organizations in navigating the aftermath of a data breach, including working with legal teams, regulators, and public relations to minimize reputational damage and comply with breach notification laws.

Cogent's growth has been fueled by our commitment to service excellence and our ability to scale agile solutions to meet the unique needs of our clients. We bring a team of experts in Cybersecurity, risk management, and compliance who are equipped to address the dynamic challenges faced by public sector organizations.

In addition to our full-service Cybersecurity expertise, Cogent brings substantial cooperative contracting experience across the U.S. public sector landscape. As one of the fastest-growing company in the country, we maintain multiple contracts with national and state-level procurement cooperatives, including [redacted]

Cogent's portfolio includes successful engagements across all the 50 states including Arizona, Colorado, Hawaii, Maine, Oregon, Rhode Island, South Dakota, Utah, Vermont, and Washington. Within these and other states, Cogent has supported a wide range of public sector clients from state departments and city governments to regional authorities and higher education institutions.

Some of our representative clients include the [redacted], among many others. These partnerships have involved the successful delivery of the risk assessment, risk mitigation, and breach coach services.

We maintain a team of seasoned professionals and leverage an ISO 9001-certified quality management system and ISO 27001-certified security framework to ensure operational excellence, data integrity, and regulatory compliance across all projects. Cogent's national delivery model and extensive experience managing cooperative purchasing relationships position us as a reliable partner under the NASPO ValuePoint Cybersecurity and Information Security Services Master Agreement, focusing on Category 1 and Category 3 services.

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

Cogent boasts a substantial workforce, with approximately 1000+ employees actively contributing to its operations and success. Our workforce encompasses a range of roles and expertise, including but not limited to executives, managers, technical professionals, and support staff. Within this dynamic employee base, there exists a rich tapestry of skills, experiences, and backgrounds, fostering a collaborative and innovative work environment. The significant number of employees underscores Cogent's capacity to handle complex projects, deliver diverse services, and adapt to the evolving needs of its clients and the industry.

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

Cogent is the S Corporation headquartered in Pittsburgh, Pennsylvania. The company is jointly owned by two executives - Mr. Manu Mehta (President) and Mr. Nandan Banerjee (Chief Executive Officer), [redacted]. This balanced ownership structure ensures collaborative strategic direction and unified leadership across all operations.

MANU MEHTA - PRESIDENT

Mr. Manu Mehta (Founder, President) brings twenty-five (25+) years of progressive techno commercial experience in the Information Technology industry. He is committed to transitioning Cogent into a leading Information Technology firm. Manu has held various leadership positions in technology, sales, strategy and general management throughout his career. He holds a bachelor's degree in Mathematics and a master's degree in Computers. In the year 2018, Manu, was awarded the "BEST CEO" award by "The CEO Magazine".

NANDAN BANERJEE - CEO

Mr. Nandan Banerjee is the CEO & co-founder and holds over twenty (20+) years of experience in the Information Technology industry in both advisory and operational roles. His visionary leadership and can-do attitude are propelling Cogent into a fast growing, premier IT services provide. In his role as CEO, Nandan has full responsibility for Cogent's global delivery, client servicing, process initiatives and general management. Nandan has held various management and operational positions throughout his career. He has worked in various roles managing global resourcing and strategic supply chain relationships with diverse companies. He holds a master's degree in Electronics from University of Bombay, and a degree in Business Management.

Together, Mr. Mehta and Mr. Banerjee form a seasoned and synergistic executive team committed to Cogent's long-term vision and public sector service excellence.

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.

Cogent has had no claims of non-performance or breach from customers in excess of $5,000 in the past five years. There are no pending litigation matters, including civil, criminal, or appellate cases, nor any criminal convictions involving the company or its principals during this period.

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.

Cogent designates the following individuals as the key contacts for the NASPO ValuePoint Master Agreement administered by the State of Idaho:

Contract Manager (Primary Point of Contact)

- **Name:** Manu Mehta
- **Title:** President
- **Email:** [redacted]
- **Phone:** [redacted]
- **Work Hours:** 9:00 AM – 6:00 PM ET

Mr. Manu Mehta will serve as the Contract Manager and the single point of contact for the management and oversight of the NASPO ValuePoint Master Agreement. As Contract Manager, he will be responsible for ensuring compliance with contract terms, managing overall service delivery, coordinating with Participating Entities, and maintaining communication with the Lead State. Mr. Mehta brings over 25 years of executive experience in the IT industry and has managed numerous large-scale public sector engagements. His leadership ensures continuity and responsiveness across multi-jurisdictional contracts.

Proposal Contact (Secondary Point of Contact)

- **Name:** Justin Acord
- **Title:** Proposal Manager
- **Email:** [redacted]
- **Phone:** [redacted]
- **Work Hours:** 9:00 AM – 6:00 PM ET

Mr. Justin Acord will serve as the Secondary Proposal Contact and will be responsible for all proposal-related communications during the evaluation period. He will ensure timely responses to all inquiries from the Lead State and coordinate any updates or clarifications needed.

Project Manager (Service Delivery Lead)

- **Name:** Mike Wilkes
- **Title:** Director of Cybersecurity Services

Mr. Mike Wilkes will serve as Project Manager, leading delivery execution across services under the Master Agreement. He will oversee implementation teams, quality assurance, and performance reporting for participating entities. Mr. Wilkes brings over 20 years of cyber security leadership experience, having held executive roles such as CISO for firms like Security Scorecard and Marvel. His

experience includes managing security programs aligned with SOC 2, NIST 800-53, HIPAA, and Fed RAMP standards.

Cogent will ensure timely and effective communication with NASPO ValuePoint and the Lead State throughout the life of the contract. In accordance with the RFP requirements, Cogent will notify the Lead State within 24 hours of any changes to the Proposal Contact or Contract Manager assignments.

Manu Mehta	
Professional Summary	Mr. Manu Mehta is the ***Founder and President of Cogent Infotech Corporation*** and brings over 25 years of progressive experience in the Information Technology, staffing, consulting, and managed services industries. As a visionary executive, he has guided Cogent's transformation into a nationally recognized provider of Cybersecurity, IT managed services, and workforce solutions for public sector and commercial clients. Mr. Mehta has extensive expertise in managing ***cooperative contracts***, having led Cogent's participation in major frameworks including ***NASPO ValuePoint, Texas DIR, TIPS-USA, Florida Statewide IT, Massachusetts ITS77, and the Cooperative Council of Governments on behalf of Equalis Group for IT Managed Services.*** His leadership ensures operational compliance, scalable delivery, and value creation across multi-jurisdictional environments. Under his direction, Cogent has delivered critical solutions to over ***150 public agencies and higher education institutions***, consistently exceeding expectations in service performance, innovation, and client satisfaction. Recognized for his industry impact, Mr. Mehta was awarded the "Best CEO" title by The CEO Magazine in 2018. His core competencies include strategic growth planning, RFP response leadership, public sector governance, and executive-level relationship management across technology, healthcare, education, and government sectors.
Education	• Master's degree in Computer Science • Bachelor's Degree in Mathematics
Certifications	• Project Management Professional (PMP)
Professional Experience	**Cogent Infotech Corporation** **President** **Jun 2003 – Present** • Mr. Manu Mehta holds a critical leadership position and plays a vital role in driving the overall success and growth of our organization. Here are the key roles and responsibilities of our President: ***Strategic Leadership:*** • Mr. Manu Mehta provides strategic direction and vision for the organization, working closely with the executive team and the board of directors. • He leads the development and execution of business strategies to achieve our mission, goals, and long-term objectives. ***Executive Management:*** • Mr. Manu Mehta oversees the day-to-day operations of the company, ensuring the efficient execution of business plans and initiatives. • Work closely with the executive team, providing guidance, support, and mentorship to key leaders in various departments. ***Business Development:***

- Leads public sector and cooperative contract strategy across all 50 states.
- Directly manages Cogent's portfolio of cooperative contracts, including participation in national and state-level vehicles such as: ***NASPO ValuePoint, Texas DIR – ITSAC & DBITS, Florida Statewide IT Contracts, IT Managed Services - The Cooperative Council of Governments On Behalf of Equalis Group, OH, Massachusetts ITS77, TIPS-USA, Vizient, ESC Region 19,*** and others.
- Ensures compliance, delivery quality, and stakeholder alignment across multi-state cooperative purchasing engagements.

Financial Performance:

- He is accountable for the financial performance and overall fiscal health of the company.
- He works with the CFO (Chief Financial Officer) and finance team to monitor financial metrics, manage budgets, and ensure profitability.

Innovation and Market Leadership:

- He fosters a culture of innovation, agility, and market leadership within the organization.
- Also, he encourages creativity, forward-thinking, and continuous improvement to stay ahead in a competitive industry.

Corporate Culture and Values:

- He ensures that the company's actions align with its core values and ethical standards.
- Also promote a strong corporate culture that fosters inclusivity, diversity, and a sense of purpose among employees.

Board of Directors Support:

- Manu Mehta collaborates closely with the board of directors, providing updates on the company's performance, major decisions, and strategic plans.
- Manage work in partnership with the board to align organizational objectives and ensure effective governance.

Crisis Management:

- He leads the organization through times of crisis, making critical decisions and implementing strategies to address challenges effectively.

Highlights of Work at Cogent

- Holds overarching responsibility for Cogent's national sales, delivery, and contract success across all 50 states, including engagements with Federal agencies, State and Local Governments, Managed Care Organizations (MCOs), Higher Education Institutions, and Fortune 500 companies.
- Leads strategic delivery of services and solutions to C-level executives, IT decision-makers, healthcare administrators, and public sector procurement officials, with a focus on maximizing value through customized, mission-aligned engagement strategies.
- Directs and manages a portfolio of multi-million-dollar workforce solutions and IT staffing contracts, particularly in healthcare and education sectors. Notable clients include:
- ***University of California San Francisco (UCSF), Cal Optima Health, Santa Clara University, San Bernardino County, University of Texas at San Antonio, Rowan University,***

	University Hospital – Newark, University of Wisconsin, Wake Forest University Medical Center, and others. • Provides executive oversight for key statewide public health and technology programs, including partnerships with ***the Maryland Health Benefit Exchange (MHBE), Texas Health and Human Services Commission, Washington Health Benefit Exchange (WAHBE), South Carolina DHHS, and Illinois Healthcare and Family Services (HFS).*** • Oversees Cogent's multi-state delivery model, including managing geographically dispersed sales teams in Dallas, Pittsburgh, and California, as well as international sourcing and support operations. Supervises recruitment and consultant retention strategies across high-demand regions such as California, Texas, and the Western U.S. • Brings a strong record of exceeding client-defined KPIs, particularly for executive talent search and specialized IT project staffing. Effectively resolves client concerns and maintains stakeholder confidence through transparent communication and agile service execution. • Champions Cogent's public sector and cooperative contract initiatives, leading successful participation in contracts such as ***NASPO ValuePoint, TIPS-USA, Texas DIR, Florida Statewide IT, and the Cooperative Council of Governments on behalf of Equalis Group.*** Proven expertise in navigating complex cooperative procurement processes and scaling services across participating entities. • Has led project delivery for city and county agencies in ***California, including the City of Sacramento, City of Los Angeles, Sacramento County, San Mateo County, and Riverside Unified School District,*** driving impactful outcomes through client-focused staffing and consulting engagements. • Drives Cogent's federal government strategy under the 8(a) program, securing awards with the Department of Justice, Department of State, and the General Services Administration (GSA). Oversees account management for public sector contracts across states such as California, Missouri, Texas, Florida, Oregon, Georgia, and New Jersey. • Serves as lead author and executive sponsor for numerous high-value RFP responses involving IT augmentation, healthcare staffing, and administrative support services, ensuring strategic alignment with client needs and regulatory requirements. • Leads new business development and partnership cultivation across the public and private sectors, building and maintaining trusted relationships with senior stakeholders to deliver innovative, cost-effective, and scalable workforce and technology solutions.

Justin Acord	
Professional Summary	Justin Acord is the Executive Vice President and possesses over fourteen (14) years of experience servicing clients in The Public Sector (federal/state/local). He has successfully managed delivery teams that are responsible for servicing several State IT contracts – North Carolina, New York Florida, Texas, Utah, Arizona, Georgia, Oregon, Maine - to name a few. Also, he has managed the delivery

	team for various State of Florida entities including but not limited to Department of Transportation, Department of Financial Services, Department of Environmental Protection, Department of State, Department of Education, Department of Children & Families, Pinellas County, Broward County Public Schools, Tampa International Airport Authority, Orange County Public Schools and Miami-Dade County.
Professional Experience	**Cogent Infotech Corporation** **Executive Vice President** **Jan 2013 – Present** • Overall responsibility for the success of all sales related activities. • Oversee, manage and ensure success with clients in over 35 different states including Federal Government, State & Local Governments and Fortune 500 companies. • Highly experienced in serving as Key Account Manager for various similar sized city and county clients including but not limited to City of Phoenix, New York City Housing Authority, City of Durham, City of Philadelphia, Harris County, TX, County of Santa Clara, CA, Ramsey County, MN, Miami Dade County, FL, Hennepin County, MN, and Multnomah County, OR. • Heavily focused on servicing clients including New York Housing Authority Dallas Fort Worth International Airport Authority, Tampa International Airport Authority, City of Austin, Texas Workforce Commission, Department of Motor Vehicles and other Public funded entities. Responsible for delivering solutions and services to C-Level executives, IT Decision Makers and Procurement/Contracting personnel. • Develop account penetration strategies to maximize our success rate with new and existing customers. • Experience successfully managing Multi-Million Dollar Government contracts including: State of Texas - DIR Staff Augmentation Contract, State of Florida IT Staff Augmentation Contract, City of Austin IT Consulting Services and GSA 8(a) STARS II GWAC. • Managing a sales team consisting of individuals in Dallas, Pittsburgh and Internationally. • Experienced consistently exceeding customer set KPI's on Staff Augmentation contracts. • Mitigating objections and compliance issues with current clients to resolve any issues. • Ensuring Sales targets and goals are met, while maximizing company profits. • Overseeing timeframes and updating clients on projects moving through the research and development process. • Responsible for responding to RFQ's by presenting winning proposals for new client acquisition. **Cogent Infotech Corporation** **Business Development Manager** **Jan 2009 – Jan 2013** • Responsible for leading the company initiatives in the Public Sector. • Tasked with marketing our 8(a) Certification to Federal Agencies which led to contracts with several agencies including the Department of Justice, Department of State and the General Services Administration. Tasked with overall Account

	Management responsibility for State Government contracts including: State of TX, FL, OR and GA. • Tasked with responding to all relevant RFQ's as a Prime. • Developed partnerships with firms who could add value for our customers enabling us to provide the absolute best solutions. Responded and won direct contracts with the State of Florida and State of Texas to provide IT Consulting Services. **Cogent Infotech Corporation** **Account Executive** **Aug 2007 – Jan 2009** • Responsible for new business development in the Private Sector. • Focused on connecting with IT Executives to understand the challenges they were faced with and developed solutions to solve those problems.

Mike Wilkes	
Professional Summary	Accomplished Chief Information Security Officer (CISO) and technology executive with over two decades of leadership in Cybersecurity, IT operations, and infrastructure transformation across startups, Fortune 500 firms, and global institutions. Proven expertise in building security programs from the ground up, leading SOC2, HIPAA/HITRUST audits, and aligning Cybersecurity strategies with business objectives. A trusted advisor to executive boards and a published author, Mike has contributed to major digital transformations at organizations such as Marvel, ASCAP, Security Scorecard, and CME Group.
Education	• Master's Degree, Stanford University, Stanford, CA • Bachelor's Degree, University of Wisconsin-Madison, Madison, WI
Professional Experience	**Lark Technologies, Mountain View, CA –** **CIS** **Nov 2022 – Present** • Head of security and IT for an innovative healthcare startup building a mobile coaching application for diabetes prevention, weight management complement to GLP-1 and hypertension programs. Lark's mission is to create compassionate technology that empowers people everywhere to live healthier lives. • Execute compliance audits for SOC2, HIPAA/HITRUST as required by our health plan partners, employers and channel sales organizations including Anthem/BCBS and many others. Report to the board of directors and investors on security program initiatives, risks and remediation projects. **SecurityScorecard, New York, NY –** **CISO** **Aug 2020 – Aug 2022** • Developed modern security program with SOC2 Type2 controls and rigor to protect corporate systems to grow and extend the security ratings SaaS platform for customers, executives and their boards of directors. • Entrusted with managing IT department in addition to security team to form a consolidated top-performing team that enjoyed career growth cross-training opportunities, mentoring responsibilities and up skilling. • Advanced the credibility of this unicorn-class startup by delivering thought leadership on security ratings, systemic risk and emerging trends in Cybersecurity presenting at Black Hat, SANS,

	Gartner, FS-ISAC and international security conferences contributing to a successful Series E raise of $180 million. **ASCAP, New York, NY –** **CISO** **Jan 2019 – Jul 2020** • As the first-ever security officer, efficiently introduced tools and processes for IAM, Incident Response, Vulnerability Management, Security Awareness Training, Endpoint Protection, BCP/DR, Asset Management, Insider Threat Program, Compliance and Governance and Supply Chain Risk. • Maintained trusted business and client relationships, liaising with external IT vendors, security experts and advisors to ensure continuous service availability for $1.2 billion revenue, 800,000 member organization. **Marvel, New York, NY –** **CISO** **Dec 2016 – Dec 2018** • As head of DevOps, enterprise architecture, and InfoSec supporting hybrid platforms for Marvel Entertainment and The Walt Disney Company, partnered across the various lines of businesses and third parties to deliver scalable, stable and secure solutions deployed on-prem and in the cloud. • Introduced comprehensive application security program for mobile and web development with a "shift left" approach for automated code analysis, pen testing and vulnerability remediation. Addressed security standards, peer code review, training and SDLC guidelines with zero impact on development velocity. • Dramatically improved API, mobile application and website performance and simultaneously reduced risk to customer data by migrating to a new data center, decommissioning the legacy content management system and introducing global content caching design with DDoS protections and WAF capabilities. **AQR Capital Management, Greenwich, CT –** **Vice President** **Nov 2015 – Oct 2016** • Authored and implemented cloud roadmap with AWS and Azure components for appropriate workloads given the firm's requirements for privacy and security. Identified early adopters within the business to develop orchestrated deployments of multi-server blueprints for research, reporting and core services (document sharing, rights management, identity management and authorization services). • Responsible for balancing projects and run-the-business workloads, introducing new and decommissioning legacy technology where appropriate. Building automation and process controls to support the continued

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.

  Cogent is a trusted provider of Cybersecurity and risk management services, with decades of experience delivering Risk Assessment and Mitigation Services across federal, state and local agencies nationwide. We have supported public and private sector clients, health benefit exchanges, colleges, and critical infrastructure institutions in proactively identifying, evaluating, and addressing Cybersecurity risks. Our team possesses extensive experience in delivering assessments aligned with NIST 800-53, ISO 27001, and FIPS 140-2 frameworks, while ensuring compliance with regulatory standards such as HIPAA, FERPA, and SOX.

  Cogent delivers high-impact services such as threat identification and prioritization, vulnerability assessments, risk mitigation planning, and security control evaluations using GRC platforms (e.g., One Trust, RSA Archer). We bring a robust bench of seasoned analysts, engineers, and project managers with security certifications and deep expertise in cyber risk management.

  Example Projects Illustrating Relevant Experience

  Project #1 Data Protection and Compliance Strengthening Project

  [redacted]

  Project #2: Cybersecurity Risk Assessment and Mitigation Strategy

  [redacted]

  Project #3: Cybersecurity Risk Maturity Assessment and Roadmap Development

  [redacted]

  Project #4: Cybersecurity Risk Assessment and Roadmap Development

  [redacted]

  Project #5: Risk Management Information System (RMIS) Support

  [redacted]

Across each engagement, Cogent has demonstrated our ability to deliver tailored, scalable, and compliant Risk Assessment and Mitigation Services to a wide variety of public sector organizations. Our security professionals are experienced in identifying enterprise risks, performing technical assessments, and crafting risk remediation strategies that enhance organizational resilience and ensure compliance. We are confident in our ability to fulfill the Category 1 Scope of Work with excellence.

- **(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.

  We have thoroughly reviewed the minimum qualifications outlined in Attachment 02, Section 2.3, and we are committed to ensuring that the staff performing these services possess the necessary skills, certifications, and experience to meet and exceed these requirements.
  We will ensure that all contractor staff assigned to this category of Risk Assessment and Mitigation Services possess relevant certifications and have the specialized expertise required for the effective identification, assessment, and mitigation of Cybersecurity risks. The qualifications of our team members are carefully selected based on their experience in the field of Cybersecurity and their proven ability to work in multi-agency environments.
  Our team will include professionals with extensive experience in auditing, information security management, and Cybersecurity program development. Many of our key personnel are Certified Information Systems Auditors (CISA) and Certified Information Security Managers (CISM), ensuring a solid foundation in auditing, control, and security practices. Their expertise enables them to perform detailed risk assessments across complex IT infrastructures and provide actionable mitigation strategies aligned with the highest industry standards.

Figure 1 Our Core Qualifications

  In addition to these foundational certifications, our team includes Certified Information Systems Security Professionals (CISSP), who bring advanced knowledge and practical experience in developing, implementing, and managing comprehensive Cybersecurity programs. This ensures that our team is well-equipped to secure both IT and operational technology (OT) environments, addressing the full scope of your risk assessment needs.

  Our personnel also possess the expertise to proactively identify vulnerabilities, with several team members holding Certified Ethical Hacker (CEH) certifications. These professionals bring valuable skills in simulating cyber attacks and identifying system weaknesses. Their ability to perform penetration testing and evaluate both IT and OT security defenses allows us to uncover hidden risks before they become threats.

Where applicable, we also consider professionals with GPEN (GIAC Penetration Tester), GEVA (Governance of Enterprise IT and Vulnerability Analysis), or Certified Regulatory and Compliance Professional (CRCP) by FINRA designations, especially for projects with forensic investigation or regulatory compliance emphasis.

Additionally, Governance, Risk, and Compliance (GRC) specialists on our team bring experience in navigating the complexities of regulatory compliance. With backgrounds in frameworks such as NERC CIP, GDPR, and HIPAA, these professionals ensure that our risk assessments are not only comprehensive but also aligned with local, national, and international regulatory requirements. Their work guarantees that our recommendations will help you stay compliant while minimizing security gaps.

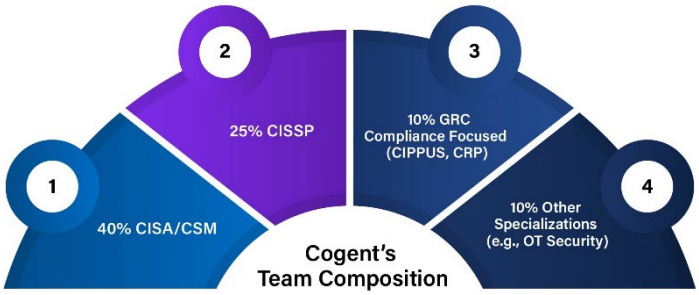


Figure 2 Cogent's Team Composition

Our team also includes professionals with specialized expertise in critical infrastructure protection, particularly in sectors like energy, utilities, and public safety. This expertise is particularly valuable when addressing SCADA system security and ensuring the secure convergence of OT and IT systems. We have successfully worked with high-stakes industries to assess risks, identify vulnerabilities, and implement effective mitigation strategies that protect mission-critical systems.

- **(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.

  Cogent is committed to providing timely, high-quality risk assessment and mitigation services to ensure that Participating Entities can proactively identify, evaluate, and address Cybersecurity risks. Our Service Level Agreements (SLAs) are designed to ensure the highest standards of service, with clear response times, defined responsibilities for both Cogent and the Participating Entity, and effective escalation procedures.

Service	Response Time	Responsible Party
Initial Acknowledgement of Service Request	Within 1 business day of request	Cogent
Risk Assessment and Vulnerability Identification	Within 10 business days from project kick-off	Cogent
Development of Risk Mitigation Plan	Within 15 business days after initial assessment	Cogent
Ongoing Reporting and Monitoring	Weekly or bi-weekly updates provided during engagement	Cogent
Escalation Process for Issues	Escalated within 2 business hours if issues arise	Cogent
Final Deliverables (including reports)	Within 30 business days from the final risk assessment or phase	Cogent

Figure 3 Cogent's SLA surrounding Category 1

Cogent's Responsibilities:
As outlined in the table above, Cogent is responsible for delivering all risk assessment and mitigation services in accordance with the specified timelines and escalation procedures. Our team will identify vulnerabilities across IT and OT systems, develop actionable mitigation strategies, and ensure alignment with leading frameworks such as NIST 800-53 and ISO 27001. We will maintain open communication with the Participating Entity throughout the engagement, providing status updates, managing risks, and initiating escalations within 2 business hours when necessary to ensure project continuity and service quality.

Responsibilities of the Participating Entity:
The Participating Entity's responsibilities in the SLA will include:

- **Access to Systems and Data:** The Participating Entity must provide timely access to all necessary systems, data, and personnel to enable Cogent to perform thorough risk assessments and identify vulnerabilities.
- **Collaboration and Engagement:** The Participating Entity is expected to participate actively in meetings and consultations throughout the project. Feedback on draft deliverables and final reports will be required within 5 business days to keep the project on schedule.
- **Approval and Sign-Off:** The Participating Entity will be responsible for reviewing and approving key deliverables such as risk assessments, mitigation plans, and final reports within 5 business days of submission to ensure the timely continuation of the project.

Escalation and Resolution of Issues:
In the event that any issues arise that may impact the delivery of services or the fulfillment of SLAs, Cogent has established clear escalation protocols to ensure timely resolution. Should any issue threaten to delay service delivery or affect the quality of the project, it will be escalated to senior management within 2 business hours. Cogent will then develop a resolution plan and keep the Participating Entity informed on the corrective actions being taken. The resolution timeframe for any issues will typically be 2-5 business days, depending on the complexity of the problem. During this period, Cogent's team will collaborate closely with the Participating Entity to address the issue efficiently and minimize any disruption to the project timeline.

Flexibility and Quality Assurance:
Our SLAs are designed to be adaptable, acknowledging that project scopes may evolve over time or new risks may emerge. Any necessary adjustments to the SLA will be agreed upon by both Cogent and the Participating Entity, ensuring that all changes are well-managed and in the best interest of project success.

Furthermore, we adhere to a rigorous quality assurance process that guarantees all deliverables meet the highest standards of excellence. All SLA commitments are tracked through an internal project management dashboard and reviewed regularly for compliance and client satisfaction. We are dedicated to providing reliable, actionable, and compliant risk assessments that empower the Participating Entity to manage and mitigate Cybersecurity risks effectively, while continuously improving the overall quality of the services provided.

- **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.

  Cogent has successfully delivered a range of Value-Added Services that complement our core Risk Assessment and Mitigation Services in Category 1. These services have been pivotal in enhancing the Cybersecurity posture of organizations across various sectors, and we are proud to offer them to the Participating Entity as part of our comprehensive Cybersecurity solutions.

Our proven experience in delivering these services to public sector entities such as NYPA, DISD, NYCHA, and Amtrak, among others, demonstrates our ability to handle complex Cybersecurity challenges across IT and OT environments. Based on our successful engagements, we can offer the following Value-Added Services tailored to your specific needs:

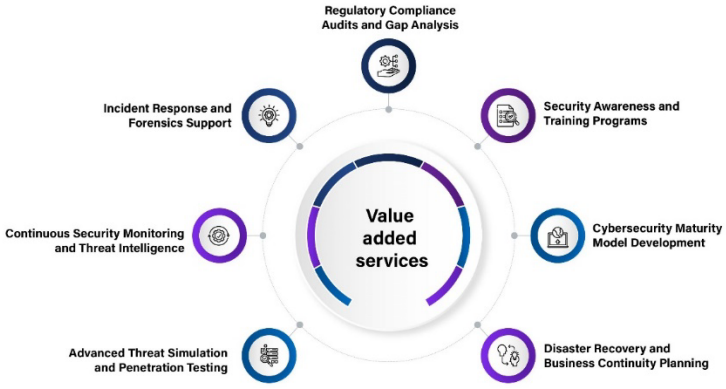


Figure 4 Our Value added services

Advanced Threat Simulation and Penetration Testing: Cogent can conduct advanced threat simulations and penetration testing on your systems to identify potential vulnerabilities that could be exploited by malicious actors. This proactive service simulates real-world attacks to identify weaknesses and provide actionable insights to improve your security defenses.

Continuous Security Monitoring and Threat Intelligence: We offer 24/7 monitoring services that track your systems for real-time threats, leveraging threat intelligence feeds and security information and event management (SIEM) tools. This service provides ongoing monitoring to detect and respond to potential threats before they become incidents.

Incident Response and Forensics Support: While Incident Response is part of the standard engagement, we can provide additional forensics services to investigate and analyze Cybersecurity breaches. Our forensic team will perform an in-depth analysis to determine the cause and impact of an incident, recover lost data, and advice on future prevention strategies.

Regulatory Compliance Audits and Gap Analysis: In addition to the risk assessments, Cogent can perform a comprehensive regulatory compliance audit to ensure your systems meet specific industry standards such as GDPR, HIPAA, PCI DSS, and SOX. We can identify any compliance gaps and help you implement measures to close them.

Security Awareness and Training Programs: Human error is often a critical factor in Cybersecurity incidents. To combat this, we offer security awareness training for your employees, tailored to your organization's needs. This training helps staff recognize and mitigate Cybersecurity risks, such as phishing attacks, and fosters a culture of security awareness across the organization.

Cybersecurity Maturity Model Development: Cogent can assist in developing a Cybersecurity maturity model to assess the current state of your organization's security posture. This service includes creating a maturity roadmap to align with industry standards and help you progress toward stronger Cybersecurity practices.

Disaster Recovery and Business Continuity Planning: In addition to risk assessments, we offer disaster recovery and business continuity planning services. These services ensure that your organization is prepared to respond to and recover from Cybersecurity events, ensuring minimal disruption to business operations.

All Value-Added Services mentioned above are available upon request, and we will provide detailed pricing in response to Attachment 09. We understand that each organization has unique needs, and our pricing will be tailored accordingly to reflect the scope and level of service required.

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

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

  Cogent has years of experience delivering breach response and breach coach services to public and private sector organizations across critical industries, including healthcare, education, transportation, and state and local government. We specialize in guiding entities through the full lifecycle of a data breach from initial investigation to final notification, regulatory engagement, and post-incident remediation.

  Our legal-technical teams have worked alongside CISOs, legal counsel, privacy officers, and public relations teams to manage breaches involving personally identifiable information (PII), protected health information (PHI), and payment data. We are well-versed in regulatory

frameworks including HIPAA, GLBA, GDPR, FERPA, and multiple state-level breach notification laws. Our playbooks and protocols are aligned with best practices outlined in NIST 800-61 (Computer Security Incident Handling Guide) and ISO/IEC 27035 (Information Security Incident Management).

Project #1 Breach Response and Legal Advisory Support

[redacted]

Project #2 Breach Notification and Legal Coordination Services

[redacted]

Project #3 Strategic Breach Response and Regulatory Guidance

[redacted]

Project #4 Breach Response Strategy and Risk Advisory

[redacted]

Project #5 Breach Response Strategy and Advisory

[redacted]

Across each of these engagements, Cogent has demonstrated a deep understanding of the breach lifecycle and regulatory landscape. Our services have directly supported affected entities through legal strategy, notification readiness, regulator communication, and litigation preparedness. With years of sustained Breach Coach experience and a strong track record of managing sensitive incidents for large-scale public sector clients, Cogent is uniquely positioned to fulfill the Category 3 Scope of Work with precision, speed, and legal acumen.

- **(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.

  Cogent recognizes the urgency, legal sensitivity, and cross-functional complexity of Cybersecurity breaches and is fully committed to deploying highly qualified Breach Coaches to support Participating Entities from the moment a Triggering Event occurs. Our Breach Response Specialists are equipped not only to activate services quickly but also to provide strategic, regulatory, and communications guidance through every phase of the incident lifecycle.

  We have thoroughly reviewed the minimum qualifications outlined in Attachment 02, Section 4.3, and we are committed to ensuring that all Breach Coaches and Breach Response Specialists assigned to perform services under Category 3 meet and exceed these requirements.

  Our personnel are carefully selected for their legal, technical, and operational experience in managing high-impact Cybersecurity incidents in regulated public and private sector environments.

  Our Breach Coaches are seasoned professionals with advanced knowledge of breach lifecycle management and incident coordination. They are equipped to guide Participating Entities

through every phase of a Triggering Event from breach discovery and regulatory analysis to notification planning and post-incident remediation. Our team has supported breach responses for entities operating under complex regulatory frameworks, including HIPAA, FERPA, GLBA, 23 NYCRR 500, GDPR, and state-specific breach notification laws.

Cogent's Breach Coaches are seasoned professionals with advanced knowledge of breach lifecycle management and incident coordination. They are equipped to guide Participating Entities through every phase of a Triggering Event from breach discovery and regulatory analysis to notification planning and post-incident remediation. Our team has supported breach responses for entities operating under complex regulatory frameworks, including HIPAA, FERPA, GLBA, 23 NYCRR 500, GDPR, and state-specific breach notification laws.

Our breach coaches have led the incident response of various agencies, reducing potential fines through swift regulatory engagement and precise consumer notification within the mandated timeline, achieving full compliance and preventing reputational damage. Our team has assisted healthcare agencies with a PHI breaches that involved 40,000+ impacted individuals. Our team worked with the Office for Civil Rights (OCR) and state attorneys to ensure timely reporting, which resulted in no penalties and minimal corrective actions. We helped the agency implement long-term compliance improvements.

In addition to satisfying the required experience threshold, many of our Breach Coaches hold relevant industry-recognized certifications, including Certified Information Privacy Professional, Certified Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), among others. These certifications equip our Breach Coaches to evaluate breach scenarios with legal precision, regulatory insight, and practical crisis management acumen.

Our personnel also bring specialized experience in:

- Regulatory and consumer breach notification strategies, including multilingual notice preparation and compliance with complex statutory requirements
- Privilege management and legal coordination, ensuring that breach communications remain protected and litigation-ready
- Cross-functional response planning, working in alignment with legal, communications, forensics, and executive leadership teams
- Engagement with insurers and cyber liability carriers, ensuring alignment with coverage requirements and carrier-approved panel counsel

Each Participating Entity will have access to a Primary Breach Coach supported by a Deputy Breach Coach and a 24x7x365 breach hotline, ensuring consistent, rapid, and expert support from the moment a breach is identified. All escalations will follow a structured governance process that ensures senior oversight and legal-aligned resolution.

Figure 5 Timeline of the Breach Lifecycle

Cogent's Breach Coaches are not only experienced professionals meeting RFP-defined standards. They are proven leaders in breach response with the certifications, communication

skills, and strategic foresight required to guide Participating Entities through complex, time-sensitive Cybersecurity incidents.

- **(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.

  Cogent is dedicated to delivering fast, accurate, and strategic Breach Coach Services that support Participating Entities through every phase of a Cybersecurity incident. Our SLAs for Category 3 are tailored to ensure that legal, regulatory, and reputational risks are proactively managed through timely advice, coordinated response planning, and cross-functional support. These SLAs define clear timelines, responsibilities, escalation paths, and quality controls to ensure optimal outcomes under stressful and high-stakes conditions.

Service	Response Time	Responsible Party
Initial Acknowledgment of Incident	Within 30 minutes of receiving breach notification	Cogent
Breach Coach Assignment and Engagement	Within 2 hours of incident confirmation	Cogent
On-site Strategic Support (if required)	Within 24 hours of request	Cogent
Legal & Notification Guidance	Within 1 business day of receiving required documentation	Cogent
Draft Notification and Escalation Plan Review	Within 2 business days from data receipt	Cogent
Regulatory/Litigation Coordination	Ongoing throughout incident lifecycle	Cogent
After-Action Review (AAR)	Within 5 business days after incident closure	Cogent

Figure 6 SLA's surrounding Category 3

After-Action Review (AAR):
Within 5 business days after incident closure, Cogent will conduct an After-Action Review (AAR) to assess the overall effectiveness of the breach response. During this phase, our team will identify key lessons learned, evaluate the performance of the breach response, and assess the adherence to regulatory timelines.

Following the AAR, Cogent provides a comprehensive incident report, which includes:

- Detailed insights into what went well during the breach response
- Actionable recommendations for improving breach readiness and response processes
- Suggestions for enhancing coordination among cross-functional teams (legal, communications, IT, etc.)
- Opportunities for process improvement to optimize future incident management

This report ensures that Participating Entities not only improve their response to the current incident but are better prepared for any potential future breaches.

Our responsibilities as the Breach Coach provider include:

- We provide detailed guidance on state and federal breach laws (e.g., HIPAA, GLBA, GDPR), including timelines, thresholds, and notification obligations. Our team ensures all actions are legally defensible and privilege-protected where applicable.
- Cogent facilitates communication with legal teams, insurers, public relations advisors, technical response teams, and regulators as needed.
- We help develop and vet breach notification language, coordinate delivery methods, and ensure compliance with content and timing requirements.
- Our resources are available around the clock for urgent advisory needs, including weekends and holidays.
- All guidance, timelines, and actions are recorded in a secure case management platform, accessible to the Participating Entity for audit and litigation purposes.
- Any impediments to incident progression are escalated to our Program Lead within 12 hours for resolution.

Responsibilities of the Participating Entity:

For successful service delivery, the Participating Entity is expected to:

- **Incident Reporting:** Notify Cogent promptly upon detection or suspicion of a breach. The earlier the notice, the greater the likelihood of effective response.
- **Access to Information:** Provide timely access to relevant facts, systems logs, communication drafts, and incident response records.
- **Internal Coordination:** Designate a primary liaison for legal and strategic decision-making. This ensures that privileged conversations and approvals occur without delay.
- **Review and Feedback:** Review proposed notification language, regulatory reports, or communication timelines within 2 business days to maintain SLA compliance.
- **Participation in Post-Incident Review:** Engage with Cogent during the After-Action Review phase to capture lessons learned and optimize future response protocols.

Escalation and Resolution of Issues:

If any roadblocks or service-impacting issues arise during an incident, Cogent follows an established escalation protocol:

- **Tier 1 Escalation:** Project-level escalation to Breach Coach Lead within 4 hours of the issue.
- **Tier 2 Escalation:** If unresolved, issue is elevated to the Director of Incident Services within 12 hours.
- **Resolution Timeline:** Most issues are resolved within 2–3 business days, depending on complexity. All escalations are tracked through a centralized ticketing system with real-time updates.

Flexibility and Quality Assurance

Our SLAs are designed to be adaptable, acknowledging that project scopes may evolve over time or new risks may emerge. Any necessary adjustments to the SLA will be agreed upon by both Cogent and the Participating Entity, ensuring that all changes are well-managed

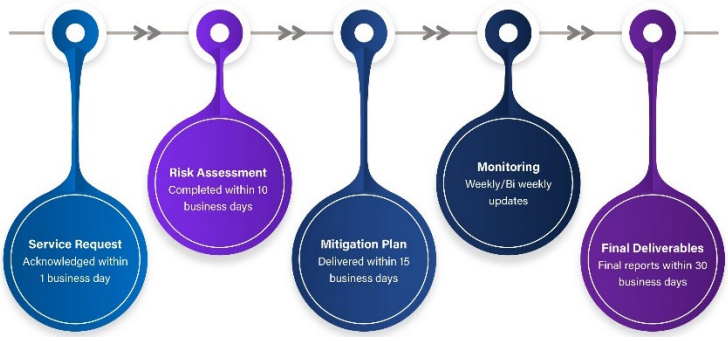


Figure 7 Our SLA's at a Glance

and in the best interest of project success.

- Quality assurance is integrated through:
- Regular performance reviews of SLA compliance.
- Continuous improvement via post-incident retrospectives.
- Training updates to keep Breach Coaches aligned with evolving regulations and breach trends.

All SLA commitments will be tracked through an internal dashboard, ensuring compliance is monitored in real-time and reported monthly to the Participating Entity. This system enables proactive management of performance metrics, providing transparency and ensuring that all service level agreements are adhered to throughout the engagement.

Cogent's Breach Coach Services empower Participating Entities to respond confidently and compliantly to security incidents—minimizing legal exposure, regulatory risk, and reputational harm through expert legal and strategic guidance.

- **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.

  Cogent offers a range of Value-Added Services designed to enhance and complement our core Breach Coach Services under Category 3. Our Value-Added Services are scalable and can be tailored to meet the unique needs of each organization, ensuring comprehensive incident management and long-term breach preparedness.

  Below is a list of the Value-Added Services we can offer, which are aligned with the requirements and objectives of Category 3 services. The associated pricing for these services will be detailed in our response to Attachment 09.

  Advanced Threat Simulation and Penetration Testing
  Cogent offers advanced penetration testing and threat simulation to proactively identify vulnerabilities in your systems. These simulated attacks help uncover weaknesses before they can be exploited by malicious actors, strengthening the overall security posture of your organization. Service Includes:
  - **Internal and external penetration testing**
  - **Red team simulations to mimic real-world attacks**
  - **Vulnerability scanning and reporting**

  Continuous Security Monitoring and Threat Intelligence
  Our 24/7 security monitoring service provides real-time threat detection and analysis using the latest threat intelligence feeds and SIEM (Security Information and Event Management) tools. This service continuously tracks and monitors your systems for emerging threats, allowing us to detect and mitigate risks before they escalate into incidents. Service Includes:
  - **Real-time incident detection and response**
  - **Threat intelligence feeds to stay ahead of new attack vectors**
  - **Continuous security monitoring and alerts**

  Incident Response and Forensics Support
  While incident response is part of our core breach coach services, we can also provide additional forensics services to investigate and analyze the cause and impact of Cybersecurity incidents. This includes data recovery, incident classification, and actionable post-incident recommendations to enhance future preparedness. Service Includes:
  - **Data recovery and forensic analysis**

- **Detailed incident classification and attribution**
- **Post-incident root cause analysis and remediation recommendations**

Regulatory Compliance Audits and Gap Analysis

Cogent can conduct regulatory compliance audits to ensure that your systems meet the relevant laws and standards, such as HIPAA, GDPR, PCI-DSS, and SOX. We identify any compliance gaps and help you implement corrective actions, ensuring your organization is always prepared for regulatory audits. Service Includes:

- **Comprehensive regulatory audit against relevant frameworks**
- **Gap analysis for non-compliance areas**
- **Remediation planning and compliance documentation**

Security Awareness and Training Programs

Human error is often a major contributing factor in Cybersecurity incidents. To help mitigate this risk, we offer security awareness training tailored to your organization. This training equips your employees with the knowledge to recognize and avoid common threats, such as phishing attacks and social engineering. Service Includes:

- **Employee training programs on security best practices**
- **Phishing simulation exercises**
- **Ongoing training updates to keep staff aware of emerging threats**

Cybersecurity Maturity Model Development

Cogent can assist in developing a Cybersecurity Maturity Model (CMM) that assesses the current state of your organization's security posture. We provide a roadmap that aligns with industry standards and help you progress toward stronger Cybersecurity practices over time. Service Includes:

- **Assessment of current security maturity**
- **Development of a Cybersecurity roadmap for improvement**
- **Ongoing progress tracking against the maturity model**

Disaster Recovery and Business Continuity Planning

In addition to the risk assessments, Cogent offers disaster recovery and business continuity planning services. These services ensure that your organization is prepared to respond to and recover from Cybersecurity incidents, minimizing downtime and disruption to business operations. Service Includes:

- **Business continuity planning and disaster recovery strategies**
- **Development of emergency response protocols**
- **Business impact analysis to ensure critical functions are maintained**

Cogent remains committed to providing comprehensive Breach Coach Services that not only address the immediate incident response needs but also offer value-added solutions that contribute to long-term cybersecurity resilience. These services enhance your organization's ability to prevent, respond to, and recover from security incidents while ensuring compliance with relevant regulations.

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

- **(ME) Category 4 – Offeror's Experience. Describe your company's experience** demonstrating that your company has a minimum of five (5) years of experience providing services similar in scope and size to the Category 4 Notification and Credit Monitoring Services required in section Attachment 02, Scope of Work. Provide specific examples that illustrate the specific services furnished and the size, composition, etc. of the entities for whom you have

provided services that you are using to demonstrate that your experience meets this minimum requirement.

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

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.

Cogent intends to serve as the prime contractor for the NASPO ValuePoint Cybersecurity and Information Security Services Master Agreement. We do not plan to use subcontractors for the performance of services under this agreement. All services, including Risk Assessment and Mitigation Services (Category 1) and Breach Coach Services (Category 3), will be delivered directly by our in-house team of experts.

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.

Cogent has a proven history of successfully delivering Cybersecurity, risk mitigation, and incident and breach response services under statewide contracts and large cooperative purchasing agreements. Our experience spans multiple cooperative procurement vehicles, including ***NASPO ValuePoint, Texas Department of Information Resources (DIR) – ITSAC & DBITS, Florida Statewide IT Contracts, Massachusetts ITS77, TIPS-USA, Vizient, ESC Region 19 Allied States Cooperative, and the Cooperative Council of Governments on behalf of Equalis Group for IT Managed Services***. These partnerships demonstrate our ability to scale services across jurisdictions while ensuring consistency, compliance, and high-impact outcomes.

The following examples highlight three of Cogent's largest and most relevant engagements over the past five years, each reflecting services closely aligned with those defined in Attachment 02 – Scope of Work, particularly in Category 1: Risk Assessment and Mitigation and Category 3: Breach Coach Services.

Case Study #1: [redacted]	
Client:	[redacted]
Contract Type:	State and Local Cybersecurity Grant Program (SLCGP)
Approximate Value:	[redacted]
Duration:	2024 – Ongoing through 2026
Scope of Work	• Cyber Planning • Risk Assessment • Communications • Project Management • Stakeholder Engagement • Federal Submission Support

Project Summary

Under the federally funded State and Local Cybersecurity Grant Program (SLCGP), Cogent was engaged by the [redacted] to deliver critical support in executing and scaling its statewide cybersecurity initiatives. This engagement is administered under [redacted] Master IT Services Agreement, reflecting Cogent's qualifications for high-sensitivity, compliance-driven engagements.

Cogent was tasked with supporting key initiatives tied to [redacted]'s Cybersecurity improvement roadmap across four federal fiscal years. This included deliverables such as refining the Cybersecurity Plan (FFY23), managing the execution of FFY22 projects, stakeholder communications, and drafting submission materials to CISA and DHS.

Scope of Services Provided

1. Cybersecurity Planning & Strategy

- Refined [redacted]'s FFY23 Cybersecurity Plan by integrating risk-based frameworks (NIST 800-53, CIS Controls v8.1, CMMC 2.0).
- Conducted stakeholder-driven gap assessments and incorporated remediation strategies including IAM modernization and .gov adoption.

2. FFY22 Project Delivery Oversight

- Led execution of three primary Cybersecurity deliverables: MFA token deployment, .gov domain migration, and security training for local governments.

- Applied agile project management with iterative sprints, stakeholder engagement, and milestone monitoring.
- Designed and executed end-to-end communications and documentation strategies for CISA approval

3. Communications & Engagement

- Developed a multi-channel communications plan to ensure every [redacted] municipality was aware of and engaged in the SLCGP offerings.
- Created stakeholder maps, town hall meeting schedules, and a dedicated communications portal for outreach and support.

4. Grant Administration Support

- Authored and packaged official SLCGP submission documents to CISA on behalf of the State — including risk reports, budget narratives, compliance matrices, and FFATA data.

5. Security Controls Implementation

- Facilitated delivery of Microsoft Defender, Crowd Strike, and Sentinel One EDR solutions.
- Rolled out Mobile Device Management (MDM), Single Sign-On (SSO), and MFA tools across local government systems

Outcomes and Value Delivered

- Enabled full compliance with DHS and CISA mandates under the SLCGP.
- Delivered training and resources to over 100+ local government IT staff.
- Empowered municipalities with secure communications, credentialing, and remote access infrastructure.
- Met all reporting, documentation, and project delivery milestones with zero delays.

Case Study #2: Cybersecurity Penetration Testing Services – [redacted]	
Client:	[redacted]
Contract Type:	IDIQ Contract – Cybersecurity Services via Task Orders
Approximate Value:	[redacted]
Duration:	2022 – Ongoing
Scope of Work	• Penetration Testing • Cyber Risk Assessment • Security Audit • Red Teaming • Regulatory Compliance • Secure System Configuration

Project Summary

As part of its enterprise-wide security assessment strategy, [redacted] engaged Cogent to provide comprehensive Cybersecurity Penetration Testing Services across its large and decentralized IT environment. Home to 50+ departments, 800+ applications, and 40,000+ hardware/software assets, the County required a strategic vendor capable of performing high-stakes, standards-compliant testing across diverse platforms.

Cogent was selected for its deep technical capabilities, advanced toolsets, certified testing personnel, and adherence to federal Cybersecurity frameworks. This engagement continues to deliver proactive risk mitigation strategies, enhanced compliance posture, and reduced attack surfaces for [redacted].

Scope of Services Provided

1. Comprehensive Penetration Testing

Cogent performed both automated and manual penetration testing activities, including:

- External and Internal Network Pen Testing
- Web Application Security Testing (OWASP Top 10)
- Physical Security and Social Engineering Simulations
- Cloud Infrastructure and Container Security (AWS, Kubernetes)
- Custom Manual Exploits and Zero-day Simulation Scenarios

Each engagement adhered to structured methodologies aligned with NIST SP 800-115, SANS, and MITRE ATT&CK, supported by formal documentation, including Rules of Engagement (RoE), toolsets, and risk classification matrices.

2. Regulatory and Compliance Assessment

- Evaluated County systems for compliance with HIPAA, CJIS, FISMA, PCI-DSS, and NIST 800-53 frameworks.
- Delivered audit-ready test reports, remediation plans, and stakeholder briefings.
- Implemented risk-ranking of vulnerabilities and recommended mitigation strategies using Cogent's proprietary risk scoring algorithm.

3. Test Toolchain and Customization

- Utilized over a dozen security tools such as Nessus, Nmap, Burp Suite, Nikto, Aircrack-ng, SQLMap, and Safe3 Scanner for vulnerability discovery.
- Developed custom test scripts and threat modeling scenarios to identify business logic flaws and simulate advanced persistent threat (APT) attacks.

4. Documentation and Reporting

Delivered exhaustive test documentation including:

- Vulnerability Reports with screenshots and timelines
- Risk Impact Narratives and GAP Analyses
- Remediation Roadmaps categorized by severity
- Attestation of Cleanup, Tool Removal, and Credential Purging

5. Stakeholder Communication and Project Management

- Deployed a dedicated project team, including a PMP-certified Project Manager, Technical Lead, and Pen Testers with GWAPT, GPEN, CISSP, and OSCP certifications.
- Conducted stakeholder briefings, real-time alerting, and continuous reporting throughout each test cycle.

Outcomes and Value Delivered

- Secured infrastructure spanning 50+ departments and 14,000 employees.
- Helped County address zero-day and privilege escalation vulnerabilities prior to public exposure.
- Demonstrated compliance across multiple federal cybersecurity regulations.
- Streamlined repeatable testing processes for future Task Orders under the contract.
- Earned commendations from the County's CISO for rapid mobilization and delivery excellence.

Case Study #3: [redacted]	
Client:	[redacted]
Contract Type:	State Public Safety
Approximate Value:	[redacted]

Duration:	April 2024 – Ongoing
Scope of Work	• Cybersecurity Architecture and Design • Firewall and Network Hardening • Policy Development and Compliance • Vendor Technical Integration (ESInet, GIS, L&R) • DevSecOps and Threat Mitigation

Project Summary

Cogent provided a Cybersecurity services to the [redacted] as part of the State's critical Next Generation 9-1-1 (NG911) system modernization. This engagement directly supported the design, procurement, and implementation of a new emergency call infrastructure that adheres to national public safety standards while ensuring advanced security protocols for real-time communication environments.

The NG911 system upgrade was highly sensitive, requiring expertise across secure network architecture, firewall configuration, identity protection, and compliance with state and federal security mandates. We operated across multi-vendor environments, ensuring seamless integration of ESInet, GIS, and Logging & Recording platforms with robust Cybersecurity controls.

Scope of Services Provided

1. Cybersecurity Strategy & Architecture

- Led the Cybersecurity architecture efforts during NG911's design and build phases.
- Delivered high-assurance designs using Next-Gen Firewall (NGFW), DNS/DNSSEC, DLP, and enterprise-grade MFA systems.
- Developed secure configurations aligned with NIST and CJIS policies.

2. DevSecOps and Automation

- Implemented DevSecOps best practices for automated security control integration within continuous deployment pipelines.
- Provided architecture guidance that reduced operational overhead while enhancing security.

3. Policy, Compliance & Risk Management

- Developed and enforced [redacted] specific security policies and procedures.
- Ensured architectural compliance with all state and [redacted] regulatory frameworks during system design and procurement.
- Provided comprehensive threat modeling and risk analysis, aligning with evolving [redacted] Cybersecurity mandates.

4. Vendor Coordination & Security Oversight

- Actively engaged in technical design sessions with ESInet, GIS, and L&R vendors.
- Reviewed and approved vendor architecture proposals from a security and performance standpoint.
- Managed the intake-to-implementation lifecycle for security bill of materials (BOM).

Outcomes and Value Delivered

- Designed a highly secure, scalable foundation for [redacted]'s NG911 infrastructure—vital to public safety and emergency response.
- Established compliance-driven architectural baselines across multiple system vendors.
- Introduced modern DLP and DNSSEC strategies into public safety IT, significantly mitigating data leakage and spoofing risks.
- Elevated [redacted]'s Cybersecurity maturity through policy creation and hands-on implementation of next-generation tools.

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

  Cogent's marketing strategy for the NASPO ValuePoint Master Agreement will leverage a multi-channel approach, combining tailored outreach, educational initiatives, and strategic relationship management to effectively promote the Master Agreement and encourage participation from potential Participating Entities, including state governments. Our strategy builds on our proven track record with similar large-scale contracts and will ensure maximum visibility, engagement, and adoption. Below are the key elements of our strategy:

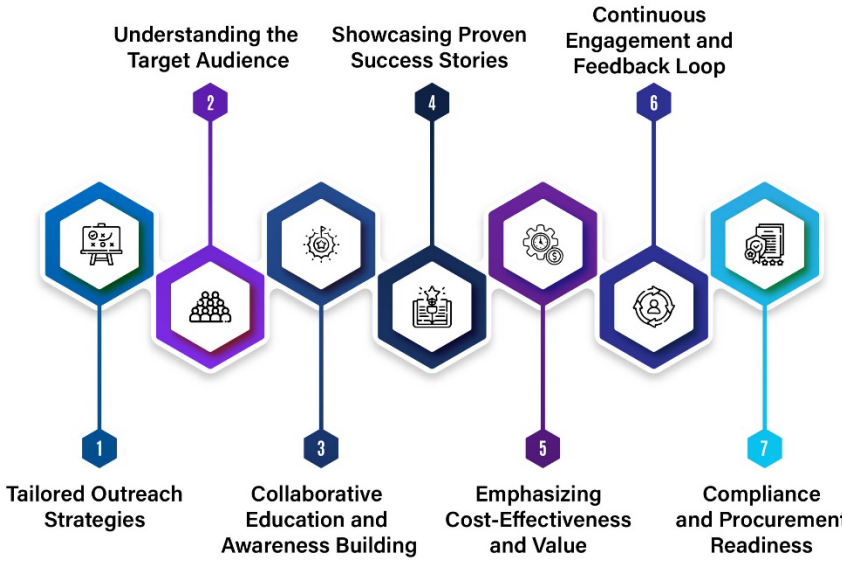


Figure 8 Our Marketing Approach

Targeted Outreach and Awareness Campaigns: We will increase awareness of the NASPO ValuePoint Master Agreement by creating targeted content and campaigns aimed at potential Participating Entities across the United States. Our efforts will focus on emphasizing the scope and advantages of the agreement, particularly in the areas of Cybersecurity, AI readiness, and information security services. To reach these entities effectively, we will:

- ***Develop Tailored Content:*** This includes targeted email campaigns, case studies, and educational resources that highlight the specific needs of state governments and public-sector agencies, demonstrating how the Master Agreement can help meet those needs.
- ***Collaborate with NASPO:*** We will work closely with NASPO to feature the Master Agreement through its existing platforms, such as newsletters, webinars, and other marketing channels. This will ensure the agreement is visible to the broad network of eligible entities within the NASPO community.

Digital Presence and Dedicated Resources: Cogent will develop and maintain a dedicated website and landing page that will serve as a comprehensive hub for the Master Agreement. This platform will be designed to:

- ***Showcase Services and Benefits:*** The website will outline all services available under the Master Agreement, including detailed descriptions of pricing, customized offerings, and the value of using the cooperative purchasing model.

- ***Provide Easy Access to Information:*** We will include FAQs, contract details, and instructions for onboarding. Our SEO efforts will ensure that the page ranks high in search results for relevant terms like "Cybersecurity contracts" and "state government IT services."

- ***Facilitate Onboarding:*** The platform will provide tools for easy onboarding, including an online ordering system, submission forms, and direct contact information for client engagement.

Educational and Relationship-Building Initiatives: Education will be at the core of our marketing approach. We recognize that each state government or public entity operates within a unique environment, with varying priorities and procurement challenges. To address this, we will:

- ***Host Webinars and Virtual Briefings:*** These sessions will introduce the Master Agreement to key stakeholders and procurement officers, explaining its structure, benefits, and how to utilize the agreement.

- ***Offer On-Demand Workshops and Presentations:*** These resources will guide entities through the contract's offerings, focusing on real-world use cases and success stories that highlight the value of participating in the cooperative contract.

- ***Share Case Studies and Success Stories:*** We will leverage testimonials and case studies from previous successful engagements with government entities to demonstrate how our services have helped similar organizations meet their goals. This storytelling approach will build trust and showcase our proven track record.

Utilizing Existing Relationships to Drive Participation: Our established relationships with a variety of public-sector entities will play a key role in driving the adoption of the Master Agreement. We will tap into these connections, particularly with government agencies and educational institutions, to encourage their participation in the cooperative contract. Specifically:

- ***Leverage Existing Relationships:*** Our sales team will reach out to existing clients like the New York City Housing Authority (NYCHA) and others who have benefited from similar agreements, highlighting the streamlined procurement process and cost savings available under the Master Agreement.

- ***Provide Smooth Transition Support:*** For organizations already working with us, we will emphasize the ease of transitioning to the NASPO ValuePoint agreement, reducing the administrative burden and enabling faster procurement.

Cost-Effectiveness and Value Proposition: Cogent's marketing will highlight the financial and operational advantages of using the cooperative purchasing model. We will:

- ***Emphasize the Benefits of the Cooperative Model:*** Our marketing materials will emphasize the cost-effectiveness of using the NASPO ValuePoint Master Agreement, including transparent pricing models, volume discounts, and reduced administrative overhead.

- ***Provide ROI Models and Savings Calculators:*** These tools will help potential Participating Entities quantify the financial benefits of adopting the agreement.

Ongoing Engagement and Feedback Loop: Our marketing efforts will not end with initial outreach. To ensure continued participation and usage of the Master Agreement, we will:

- ***Establish Continuous Engagement:*** We will maintain regular communication through email updates, client check-ins, and feedback surveys. This will ensure that Participating Entities remain informed about the latest updates to the Master Agreement and the services available.
- ***Gather and Incorporate Feedback:*** Ongoing feedback from Participating Entities will help us refine our marketing materials and service offerings, ensuring that we continue to meet the evolving needs of public-sector organizations.

By combining targeted communication, personalized outreach, and strategic education, Cogent will ensure that the NASPO ValuePoint Master Agreement is widely recognized, adopted, and utilized by a diverse range of state governments and public-sector organizations. Our approach will not only raise awareness but will also create long-lasting partnerships based on trust, value, and mutual success.

- 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.

  Cogent is committed to providing an intuitive, user-friendly, and fully accessible digital platform to support the NASPO ValuePoint Master Agreement. The dedicated website will serve as a centralized resource for Participating Entities, offering seamless access to critical contract details, services, customized pricing, and efficient ordering capabilities. Our platform is designed with clarity, usability, and compliance at its core, ensuring that Participating Entities can navigate and utilize the resources with ease. Below are the key features of the website:

  Customized Price Lists for Each Participating Entity: To ensure transparency and alignment with the unique needs of each Participating Entity, the website will feature customized price lists tailored to each entity's requirements. These price lists will include:

  - ***Pre-approved labor categories and rates:*** Each Participating Entity will have access to customized pricing, based on the negotiated rates and any volume discounts or incentives that may apply to their specific needs.
  - ***Negotiated discounts and incentives:*** Participating Entities can view any applicable discounts, ensuring that they are able to see the full financial benefits of utilizing the Master Agreement. This feature will be particularly beneficial for large-scale or multi-year engagements.

  Comprehensive Contract Overview and Service Scope: The website will provide a clear and structured overview of the NASPO ValuePoint Master Agreement, detailing the scope of services available under the contract. Key elements will include:

  - ***Service Categories:*** A breakdown of available services, such as cybersecurity, data breach response, risk assessments, and more, with detailed descriptions to help entities understand the full range of offerings.
  - ***Contract Terms:*** Full access to contract terms, including amendment history, scope of work, and any changes or updates made throughout the life of the agreement.

  Online Ordering System: Our online ordering system will offer a streamlined, secure, and auditable way for Participating Entities to request services under the Master Agreement. Features of the ordering system will include:

  - ***Request-for-Services (RFS) Forms:*** Participating Entities can easily submit service requests via pre-configured forms. This will allow for a standardized process to gather key information for efficient fulfillment.

- ***Pre-configured Scopes of Work:*** Entities will be able to select from pre-configured service packages based on their needs, simplifying the ordering process and reducing the time spent on customizing individual requests.
- ***Submission of Procurement Documents:*** The system will allow entities to submit relevant procurement documents, such as purchase orders or project specifications, directly through the platform.
- ***Order Confirmation and Next-Step Guidance:*** Upon submission, entities will receive immediate confirmation of their order along with guidance on the next steps. This will include details on project timelines, key contacts, and any other relevant instructions for implementation.

Staff Directory and Points of Contact: To ensure easy communication, the website will include a real-time staff directory featuring key personnel involved in supporting the Master Agreement. This will provide:

- ***Account Managers and Support Staff:*** Contact details, including email addresses, phone numbers, and scheduling links, will be available for dedicated account managers, category leads, and technical support staff.
- ***Dedicated Points of Contact:*** Participating Entities will have access to the appropriate contact person based on their service needs, ensuring that they can receive prompt assistance and efficient service delivery.

Client Resources and Knowledge Base: Cogent will create a robust knowledge base to support Participating Entities throughout their engagement with the Master Agreement. This will include:

- ***Onboarding Guides and Tutorials:*** Step-by-step resources that will help new clients navigate the contract, submit orders, and understand the services available.
- ***Training Webinars and Recorded Sessions:*** Educational materials will be available to help Participating Entities understand how to maximize the benefits of the Master Agreement, including best practices, compliance requirements, and detailed service overviews.
- ***Case Studies and Success Stories:*** Real-world examples showcasing how other entities have successfully implemented services under the agreement, providing valuable insights into potential applications and outcomes.

Accessibility and Compliance Features: Cogent is committed to ensuring that the website is accessible to all users. Features will include:

- ***Compliance with WCAG 2.1 Accessibility Standards:*** The website will adhere to accessibility guidelines to ensure inclusivity for users with disabilities.
- ***Mobile-Friendly Design:*** The platform will be optimized for mobile devices to ensure users can access it on any device, whether they are in the office or on the go.
- ***Security and Data Protection:*** The website will incorporate robust security measures, including encryption, multi-factor authentication for ordering, and compliance with industry standards to ensure the confidentiality and protection of all data.

Reporting and Feedback Tools: The website will offer reporting and feedback tools to support continuous improvement and engagement with Participating Entities. Key features include:

- ***Feedback Forms:*** Participating Entities can easily provide feedback on services, order fulfillment, and overall experience.
- ***Performance Reports:*** Entities can request detailed reports on service usage, order status, and other relevant metrics, helping them monitor progress and ensure alignment with their goals.
- ***Customer Support Channels:*** Dedicated support channels will be available through chat, email, and phone, providing entities with timely assistance as needed.

By incorporating these features, the dedicated website will serve as an indispensable resource for Participating Entities, streamlining the process of accessing services, submitting orders, and engaging with Cogent throughout the duration of the Master Agreement. This platform will not only enhance the user experience but also ensure compliance, transparency, and ease of access for all users.

- 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.

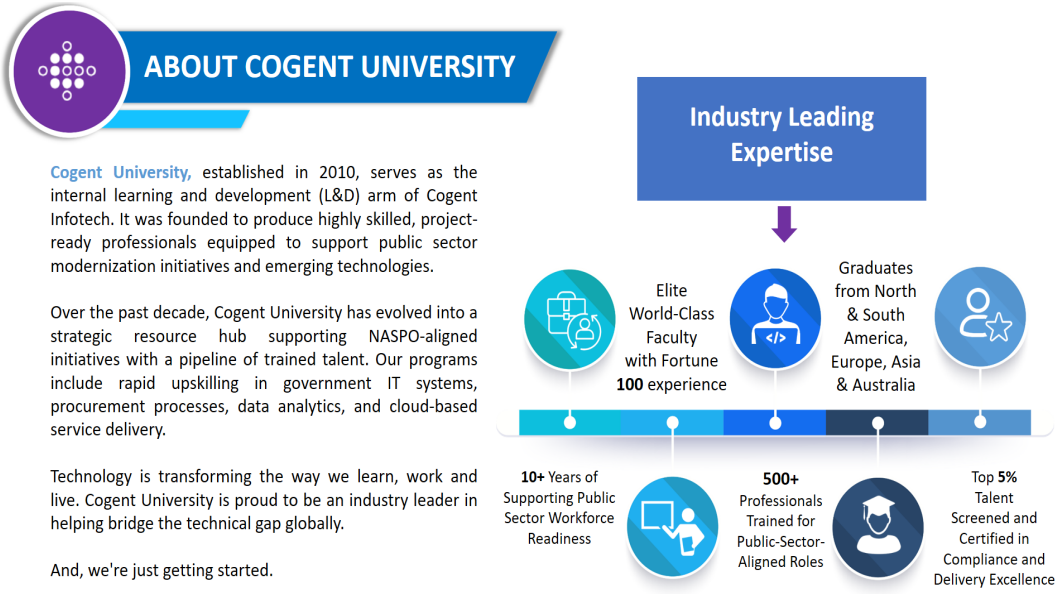
Cogent will assign a dedicated, multidisciplinary team to manage and support the NASPO ValuePoint Master Agreement. This team will consist of experienced Project Managers, Contract Specialists, Account Executives, Procurement Coordinators, and Administrative Staff, each with deep familiarity in cooperative contract administration, public sector service delivery, and compliance operations.

Project Managers will oversee service delivery, manage performance metrics, and ensure operational alignment with contract terms. Contract Specialists will support pricing integrity, manage legal adherence, and oversee documentation of scopes and amendments. Account Executives will serve as the primary point of contact for Participating Entities, facilitating proactive communication, customization of services, and stakeholder engagement. Administrative Support Staff will ensure audit-readiness and maintain comprehensive reporting, document retention, and usage logs.

Training & Familiarization with the Master Agreement - Cogent will deploy a structured, multi-phase Training and Onboarding Program to ensure that all personnel supporting the NASPO Master Agreement are deeply familiar with its pricing structure, terms and conditions, and compliance obligations. This includes:

- Formal training workshops on the Master Agreement framework, including rate structures, ordering processes, and allowable modifications.
- Scenario-based simulations to prepare staff for real-world client requests and order customization workflows.
- Quarterly refresher courses and compliance updates to reflect any amendments, new Participating Entity terms, or changes in NASPO policy.
- A centralized knowledgebase and internal LMS (Learning Management System) for continual reference and just-in-time learning.

Customer Training and Knowledge Transfer - For Participating Entities and client stakeholders, Cogent will provide end-user training on order placement, contract use, reporting tools, and performance expectations. These sessions will be coordinated in advance and tracked using a Training Plan and Log, which captures curriculum, participant attendance, and feedback. Final client-facing training will be delivered as part of project closure or onboarding phases, tailored to each agency's preferences.



Cogent University – Training Our People, Powering Your Projects

At the heart of our staff development strategy is Cogent University—our proprietary learning and development platform. Operating from our headquarters in Pittsburgh, PA and accessible remotely, Cogent University provides technical, compliance, and project delivery training tailored to the public sector. We invest heavily in upskilling through:

- Full-time trainers and SMEs offering domain-specific certifications.
- Cross-training in emerging technologies (AI, cloud, cybersecurity, procurement systems).
- Fast-track onboarding programs for new hires supporting NASPO engagements.

Through Cogent University, we ensure that staff assigned to NASPO are not only trained but are leaders in service innovation, compliance, and operational delivery—positioning us to deliver with excellence from day one.

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

  Cogent is committed to ensuring that the NASPO ValuePoint Master Agreement becomes a valuable and frequently utilized resource for all Participating and Purchasing Entities. Our approach to encouraging adoption and maximizing usage is centered around education, seamless onboarding, ongoing support, and clear value demonstration. By offering a combination of personalized outreach, user-friendly resources, and targeted engagement strategies, we will ensure that our Master Agreement is not only adopted but actively leveraged by public-sector organizations. Below are the key strategies we will employ to foster adoption and encourage sustained usage of the agreement:

  Targeted Outreach and Personalized Engagement: Our outreach efforts will be personalized to address the unique needs and challenges of each Participating Entity. To promote initial adoption and usage, we will:

  - ***Customized Communication:*** We will develop tailored communication strategies for different sectors (e.g., state governments, local municipalities, education, healthcare), ensuring that the benefits of the Master Agreement are aligned with their specific goals and operational needs.

- ***Direct Engagement with Key Stakeholders:*** Through dedicated account managers and field representatives, we will engage directly with procurement officers, IT departments, and other decision-makers to explain the advantages of using the cooperative contract.
- ***Success Stories and Testimonials:*** We will share real-world examples of how other entities have successfully utilized the Master Agreement. This will include case studies, client testimonials, and examples from similar public-sector organizations, demonstrating how the agreement delivers value.

Educational Programs and Resources: We believe that a key factor in encouraging adoption is ensuring that potential Participating and Purchasing Entities fully understand how to use the Master Agreement effectively. To achieve this, we will:

- ***Webinars and Virtual Briefings:*** We will host educational webinars and virtual briefings to walk through the Master Agreement's terms, benefits, and process for ordering services. These sessions will be designed to address any questions and ensure that all participants are comfortable with the agreement's framework.
- ***Onboarding Guides and Training Materials:*** Cogent will provide clear, accessible guides to help new users understand how to engage with the agreement. This will include step-by-step instructions for submitting orders, understanding pricing structures, and accessing support.
- ***On-Demand Workshops and Resources:*** Our website will host on-demand workshops and instructional content that Participating Entities can access at their convenience, reinforcing the details of the agreement and encouraging them to begin utilizing the services available.

Simplified Onboarding Process: We recognize that adopting a new contract can sometimes be a time-consuming process for Participating Entities. To ease this transition and encourage quick adoption, we will:

- ***Streamline the Onboarding Process:*** We will offer dedicated onboarding support for each Participating Entity, including a step-by-step guide to ensure smooth integration of services. This includes assisting with contract registration, order submission, and understanding how to customize their services to meet specific needs.
- ***Dedicated Account Managers:*** Each Participating Entity will be assigned an account manager who will guide them through the entire process—from the initial introduction to the agreement to the first service order, ensuring they have a consistent point of contact for questions and support.
- ***Pre-configured Scopes of Work and Services:*** By offering pre-configured service packages and customizable options, we make it easy for Participating Entities to quickly begin using the agreement without needing to create customized service contracts from scratch.

Clear Value Demonstration and Cost-Effectiveness: To incentivize continued usage, we will highlight the cost-effectiveness and operational advantages of the Master Agreement, ensuring that Participating Entities see the value from the start. Our approach includes:

- ***ROI Models and Savings Calculators:*** Cogent will provide clear tools, including return-on-investment models and savings calculators, that show how entities can benefit financially by using the cooperative purchasing model. These tools will help demonstrate that participating in the Master Agreement leads to cost savings and reduced procurement overhead.

- ***Volume-Based Discounts:*** Where applicable, we will highlight volume-based pricing models and how increasing service usage over time can lead to greater cost savings.
- ***Transparent Pricing:*** By providing clear, up-front pricing and regularly updating the price lists for each Participating Entity, we will eliminate confusion and allow entities to make informed purchasing decisions with confidence.

Ongoing Support and Customer Success Initiatives: Once an entity begins using the Master Agreement, we will provide ongoing support to ensure that they continue to get value and make the most of the services offered. Key components of this strategy include:

- ***Regular Check-Ins and Support:*** Our team will proactively reach out to Participating Entities to check on their progress, answer questions, and offer assistance as needed. This ongoing engagement will help ensure that entities continue to feel supported throughout their relationship with the Master Agreement.
- ***Quarterly Reviews and Feedback Loops:*** We will schedule quarterly reviews with Participating Entities to gather feedback, identify any challenges, and ensure that the Master Agreement is still meeting their needs. We will use this feedback to continuously improve our offerings and services.
- ***Dedicated Customer Success Team:*** A dedicated customer success team will be available to assist with any issues, from technical support to procurement challenges. This ensures that each Participating Entity has the resources they need to continue using the Master Agreement efficiently.

Incentivizing Long-Term Usage: To drive long-term adoption and usage of the Master Agreement, we will provide incentives that reward continued engagement and volume increases. These incentives include:

- ***Volume-Based Discounts and Incentive Programs:*** We will offer volume-based discounts for Participating Entities that increase their usage over time, ensuring that entities are encouraged to consolidate their purchasing and gain additional savings.
- ***Loyalty Programs:*** For long-term users, we will offer loyalty incentives such as access to exclusive services, early access to new features or offerings, and even discounted rates on future service orders.

Collaborative Engagement with NASPO: We will also leverage NASPO's platform and network to further encourage adoption and increase awareness of the Master Agreement:

- ***Joint Marketing and Co-Branded Campaigns:*** Through joint marketing efforts with NASPO, we will ensure that the Master Agreement receives consistent visibility across NASPO's established network of participating entities. This will include co-branded campaigns, webinars, and events designed to raise awareness and promote usage of the agreement.

By combining targeted outreach, educational initiatives, seamless onboarding, clear value demonstrations, and ongoing support, Cogent will ensure high levels of adoption and usage of the NASPO ValuePoint Master Agreement. Our approach is designed to create long-term engagement, making the agreement a trusted, valuable resource for all Participating and Purchasing Entities.

- 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?)

We understand that Participating Entities operate under diverse legal, regulatory, and procurement frameworks, so a one-size-fits-all approach is neither practical nor ideal. Our approach to the negotiation of Participating Addenda will focus on collaboration, transparency, and flexibility

We provide flexibility in the negotiation of Participating Addenda. We do not impose rigid constraints on entities when modifying or supplementing terms. We understand that each Participating Entity may have specific legal or operational requirements that need to be addressed for compliance or risk management purposes. While we encourage entities to provide statutory citations where applicable to help expedite the review process, we do not require them as a precondition. Our goal is to ensure the Participating Addenda reflect the unique needs of each state or agency while maintaining alignment with the Master Agreement's overall framework.

We are also fully equipped to support the simultaneous negotiation of multiple Participating Addenda. Our dedicated legal and contracts team, experienced in managing multi-state government contracts, will work closely with account executives and delivery leads to ensure efficient coordination and quick turnaround times. Our centralized contract management system enables version control, audit trails, and real-time updates, allowing us to maintain responsiveness even under volume.

Each Participating Entity will have a dedicated point of contact, typically a contract manager, supported by legal counsel and client success teams. This ensures that each negotiation is handled efficiently and with consistency, reducing bottlenecks and building trust throughout the process.

To ensure timely progress, we maintain clear internal service level agreements (SLAs) for the review and feedback of Participating Addenda. Once an entity provides proposed language or terms, we commit to responding within 5–10 business days, depending on the complexity. All requests are tracked through our contract management system, ensuring transparency and accountability at every stage.

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

  Cogent is fully committed to ensuring that products and services are available for immediate deployment upon the execution of the NASPO ValuePoint Master Agreement and Participating Addenda. Our operational model is designed for rapid mobilization, scalability, and immediate service delivery, enabling us to swiftly meet the needs of Participating Entities and ensure seamless transitions into active service. Below, we outline our approach and the resources we have in place to deliver services and products without delay.

  Pre-Established Delivery Infrastructure: Cogent has built an extensive nationwide network of pre-vetted professionals and consultants who are organized by skill set and geographic location. This allows us to deploy resources immediately upon execution of the Master Agreement and Participating Addenda. Key components of our delivery infrastructure include:

  - ***Pre-Qualified Experts:*** We maintain an active pipeline of highly skilled professionals across various service areas, such as Cybersecurity, AI readiness, and data breach response. Our pre-screened team of experts ensures that we can meet the specific needs of Participating Entities immediately, with little to no ramp-up time required.
  - ***Dedicated Delivery Managers:*** Each Participating Entity will be assigned a dedicated delivery manager who will oversee the initiation of services and ensure that all

requirements are met promptly. These managers are well-versed in the nuances of public-sector procurement, ensuring that services are delivered in accordance with the contract's terms.

Robust Project Intake System: Cogent's centralized project intake system enables efficient routing of service requests to the appropriate subject matter experts (SMEs) for fast response and fulfillment. This system helps ensure that each request is immediately logged and processed, with clear timelines and milestones for delivery. Features of this system include:

- ***Real-Time Service Request Tracking:*** Service requests from Participating Entities are captured and tracked in real-time, providing visibility into the status of each request and ensuring transparency throughout the process.
- ***Automated Routing and Prioritization:*** The system automatically routes requests to the most appropriate SME based on their expertise and availability, ensuring that the right resources are assigned to each project without delay.

Rapid Resource Mobilization and Scalability: We understand that Participating Entities may need to mobilize quickly to meet urgent requirements. Our operational model is designed to scale rapidly, ensuring that we can deploy resources at short notice. This includes:

- ***Flexible Staffing Models:*** Whether it's a small, specialized project or a large-scale engagement, we have the flexibility to scale our resources up or down based on the scope of the work. This ensures that services are delivered efficiently and within the timeframes required by the Participating Entity.
- ***National Coverage:*** With a network of professionals across the country, we are equipped to provide nationwide coverage and deliver services wherever they are needed, including remote or on-site engagements, without delays.

Established Onboarding and Compliance Processes: Cogent has streamlined onboarding processes in place that are fully aligned with state and local compliance protocols. This includes background checks, badging, training modules, and technology access setups, which can be initiated as soon as the Master Agreement is executed. Our processes ensure that we are ready to provide services immediately after contract execution, with the following steps in place:

- ***Pre-Contract Compliance Checks:*** In anticipation of the contract's execution, we ensure that all necessary compliance checks, security clearances, and certifications are in place. This includes pre-screening for IT professionals, completing background checks, and ensuring that personnel are equipped with the necessary tools and access to initiate services without delay.
- ***Technology and System Readiness:*** For tech-dependent services (e.g., cybersecurity, cloud integration), we ensure that all required systems, software, and platforms are fully operational and ready for deployment. This allows us to begin service delivery immediately after the Participating Addenda is signed.

Dedicated Customer Success Team: Upon the execution of the Master Agreement and Participating Addenda, Cogent assigns a customer success manager (CSM) to each Participating Entity. The CSM will facilitate a smooth transition from contract execution to active service delivery, ensuring that any custom requirements or specifications are met without delay. This includes:

- ***Ongoing Support and Consultation:*** The CSM will be the primary point of contact for any questions or issues that arise, ensuring that Participating Entities have immediate access to support.

- ***Performance Monitoring:*** The CSM will also oversee the ongoing performance of services, ensuring that they are delivered in accordance with the terms of the Master Agreement and meeting the expectations of the Participating Entity.

Pre-Configured Service Offerings: In order to expedite the service delivery process, Cogent will provide pre-configured service offerings that can be customized as needed. These services include common solutions that many Participating Entities may require, such as:

- ***Risk Assessments and Security Audits:*** Pre-configured packages for cybersecurity risk assessments and security audits, designed to be quickly implemented.
- ***Data Breach Response:*** Ready-to-activate breach response plans that can be tailored to the specific needs of each entity.
- ***Training and Workshops:*** Pre-scheduled and customizable training programs on Cybersecurity best practices, incident response, and AI readiness, ensuring quick access to education and skills development for the Participating Entity.

Continuous Improvement and Feedback: Cogent is committed to continuous improvement, using feedback from Participating Entities to refine and optimize service delivery. We collect ongoing feedback throughout the engagement process and make necessary adjustments to ensure that services are meeting the needs and expectations of the entities. This feedback loop ensures that:

- ***Quick Issue Resolution:*** Any service issues or adjustments needed will be addressed immediately, ensuring that there is no disruption to service delivery.
- ***Ongoing Optimization:*** We continuously improve our services based on feedback, ensuring that we adapt to the evolving needs of Participating Entities over time.

By maintaining a flexible, scalable, and resource-ready operational model, Cogent is equipped to immediately provide products and services upon the execution of the Master Agreement and Participating Addenda. From the moment the agreement is signed, our efficient processes, pre-established resources, and dedicated customer success teams ensure that Participating Entities can begin utilizing the services they need without delay.

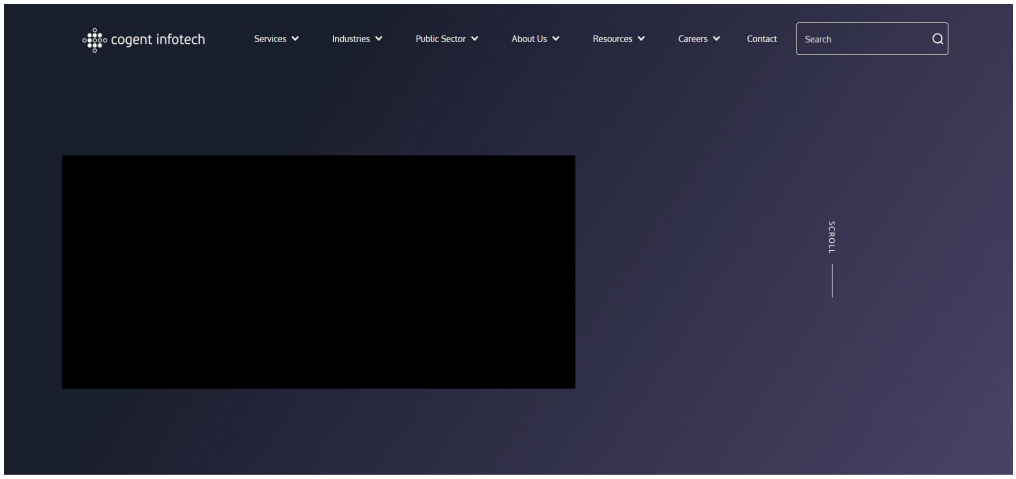
- Describe how you will ensure summary and detailed sales information is promptly, completely, and accurately reported to you by your dealers, partners, and resellers for aggregation and reporting to NASPO ValuePoint in compliance with the terms of your Master Agreement.
Cogent is committed to ensuring that all sales data from dealers, partners, and resellers is reported in a timely, accurate, and complete manner, in compliance with the NASPO ValuePoint Master Agreement. We have implemented clear processes and systems that streamline this process, ensuring full transparency and compliance.

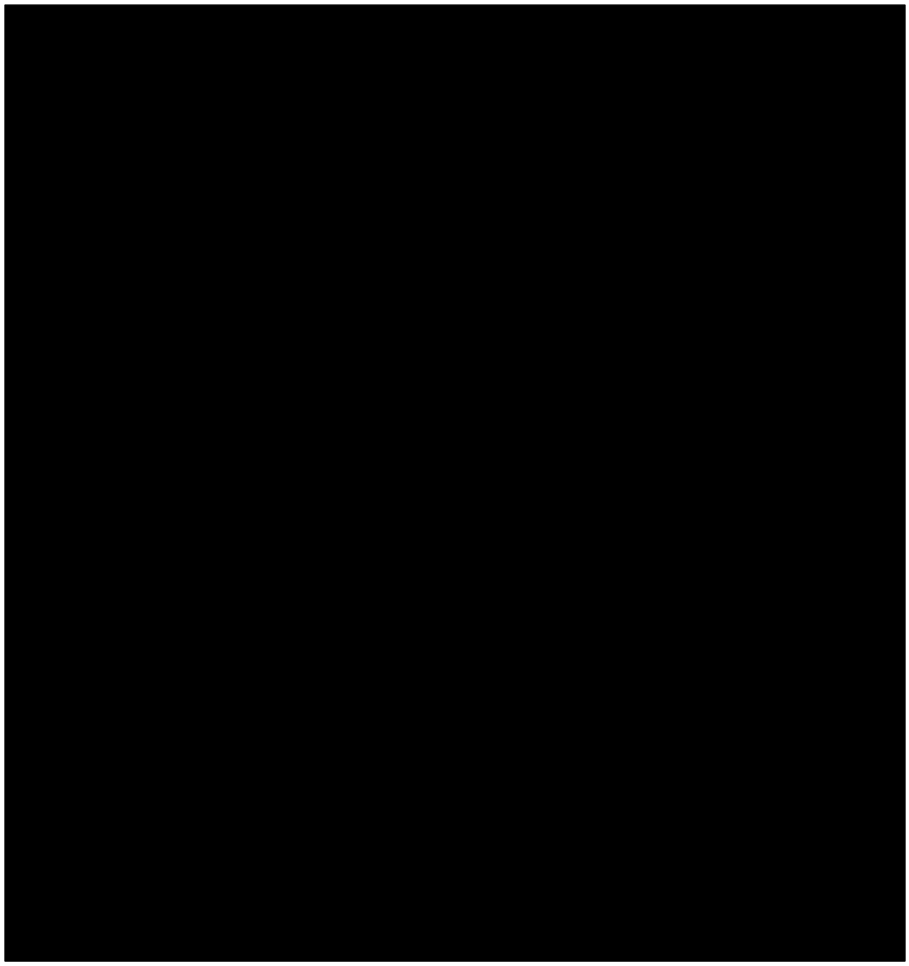
  - Cogent will provide clear guidelines and standardized templates to all partners, ensuring they understand the required data, formats, and deadlines. This will help maintain consistency across all submissions.
  - We will utilize a real-time reporting platform where partners can submit their sales data. This system will feature Automatic Validation to ensure data accuracy before submission. It will also feature Data Aggregation for automatically compiling summary and detailed reports for internal review and submission to NASPO ValuePoint.
  - Cogent will provide initial training on how to submit data and use the reporting system. A dedicated support team to assist partners with any questions or issues during the reporting process.

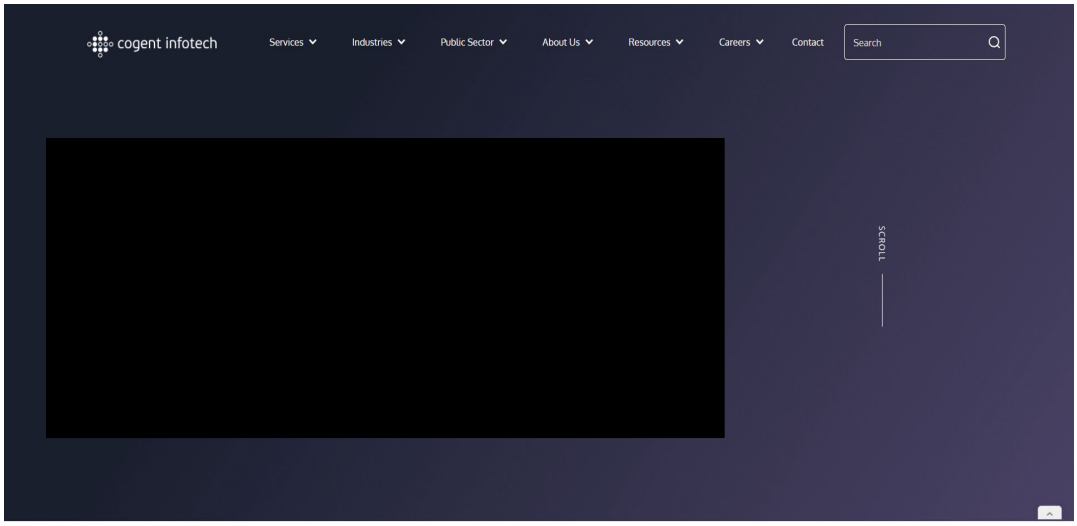
- To ensure accuracy, Cogent will perform regular audits of reported data. We will conduct random checks and address discrepancies with partners, providing feedback for continuous improvement.
- Sales data will be aggregated and submitted on time to NASPO ValuePoint. Our automated system ensures that all reports are formatted according to NASPO's specifications for easy submission.
- Cogent will introduce an incentive system for partners who consistently submit accurate and timely reports. Rewards may include recognition, priority support, and discounts on future services.
- We will maintain a feedback loop to optimize the reporting process. Partner surveys will help refine our systems and ensure that we continue to meet NASPO's standards effectively.

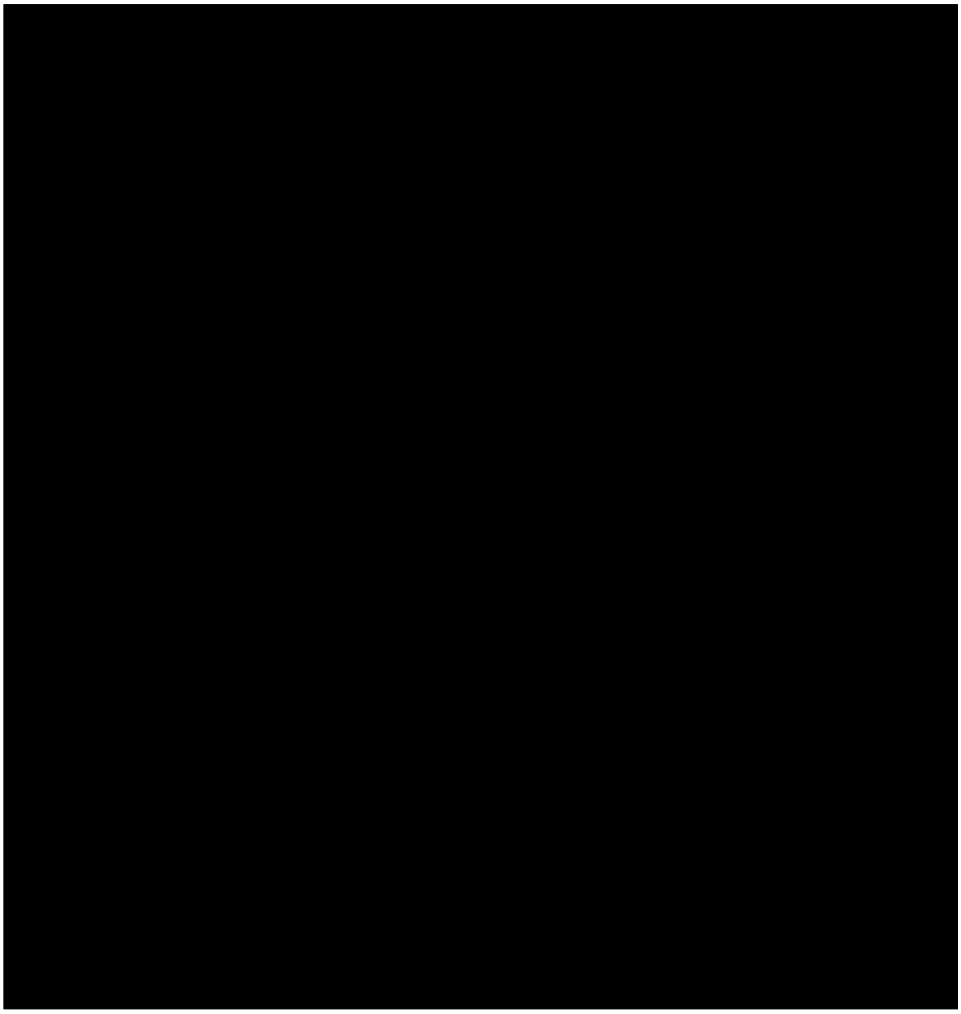
Conclusion and Proven Success in Delivering High-Quality Services

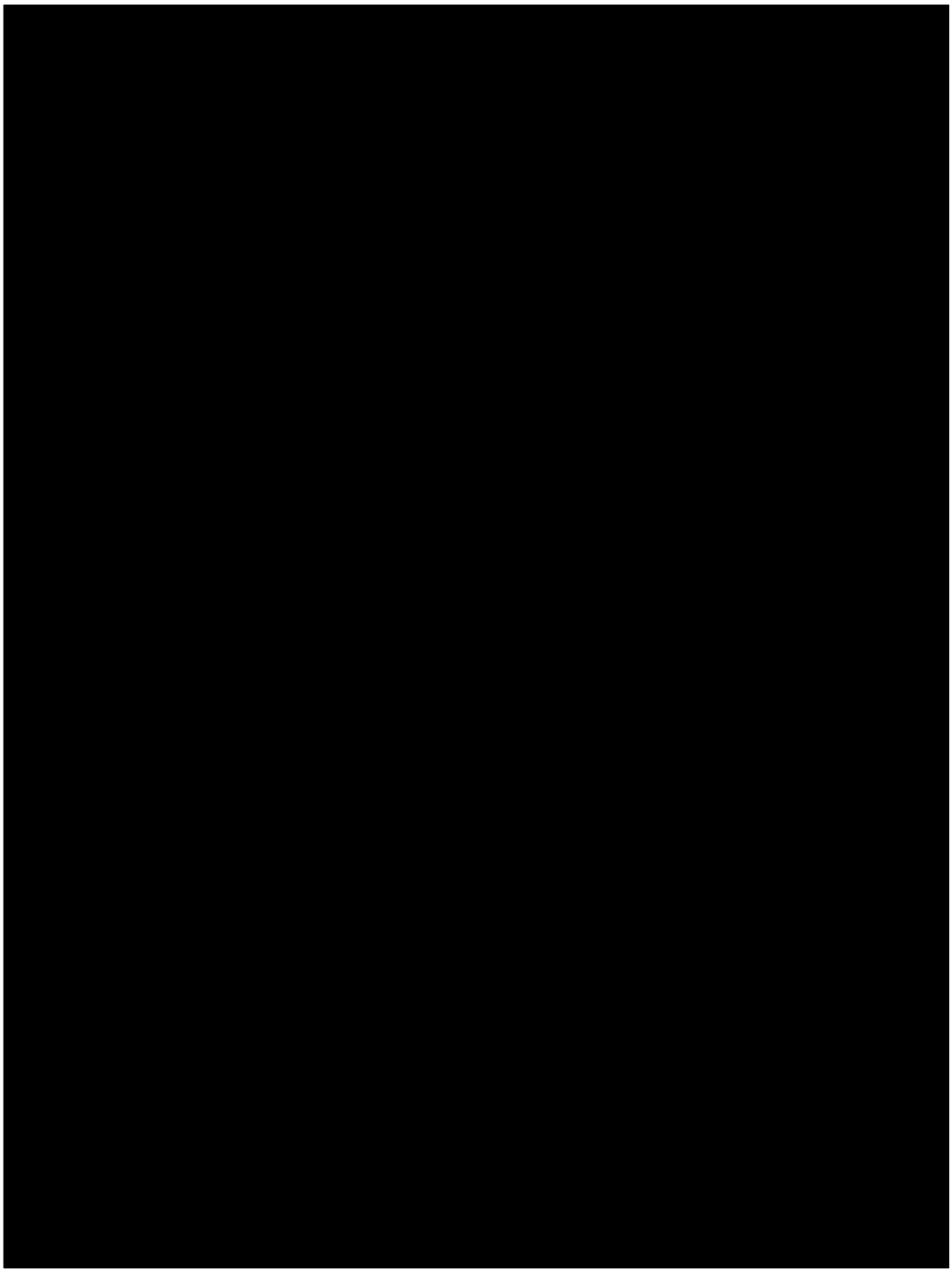
Cogent's comprehensive approach to managing cooperative agreements, including our experience with contracts such as [redacted], demonstrates our capability to efficiently meet the needs of Participating Entities. Our success with these contracts is a testament to our ability to deliver high-quality services, maintain compliance, and ensure transparency throughout the entire contract lifecycle. Whether it's through tailored marketing strategies, flexible negotiation practices, seamless onboarding, or immediate service delivery, Cogent consistently provides value to our clients by aligning with their specific needs and operational goals.

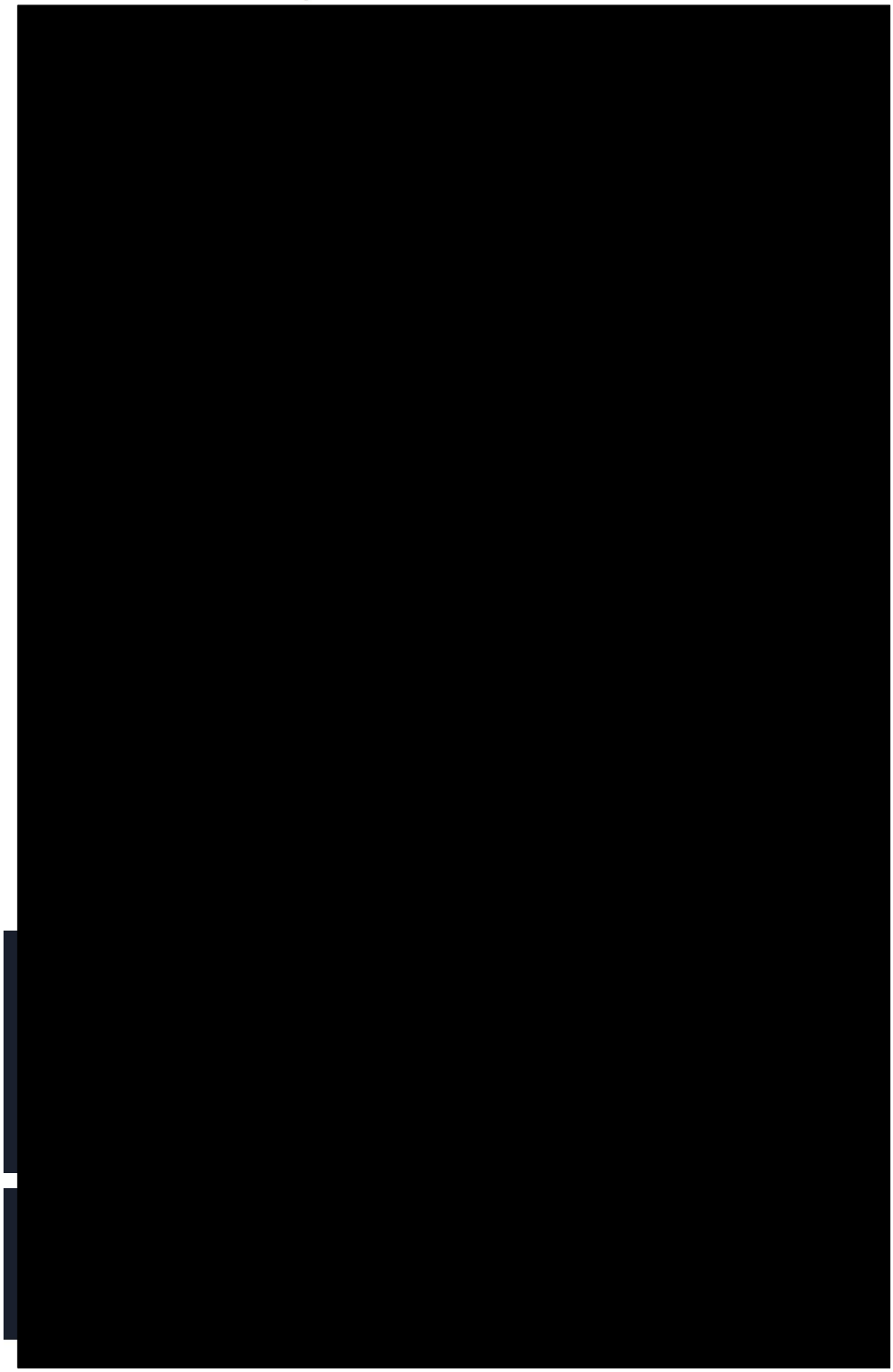

cogent infotech
Services
Industries
Public Sector
About Us
Resources
Careers
Contact
Search
SCROLL




cogent infotech
Services
Industries
Public Sector
About Us
Resources
Careers
Contact
Search
SCROLL







By leveraging our proven systems, dedicated resources, and strong relationships with public sector organizations, Cogent ensures that each Participating Entity receives not only the best

products and services but also the support and expertise necessary to maximize the value of the Master Agreement. We remain committed to fostering long-term partnerships, supporting seamless contract execution, and driving the success of every Participating Entity throughout the term of the agreement.

G. (ME) **Customer Service**

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

  At Cogent, we prioritize our clients' needs through proactive service and responsive communication. We believe that building strong relationships with clients and consultants is essential to identifying and resolving potential challenges early—before they escalate. Our emphasis on regular, transparent communication enables us to address concerns quickly and effectively.

  For this contract, Cogent will assign a dedicated ***account team led by the designated Contract Manager***, who will serve as the primary point of contact for the Lead State and all participating entities. This individual will be responsible for ongoing coordination, issue resolution, and performance oversight. Weekly feedback will be collected from participating clients to ensure service consistency and timely improvements.

  Our customer service team operates during regular business hours, Monday to Friday, from 9:00 AM to 5:00 PM (local time). For urgent issues outside these hours, we offer extended support options during evenings and weekends to address critical matters. Key account representatives are available during these hours and can be reached directly through dedicated contact information that will be provided to your team.

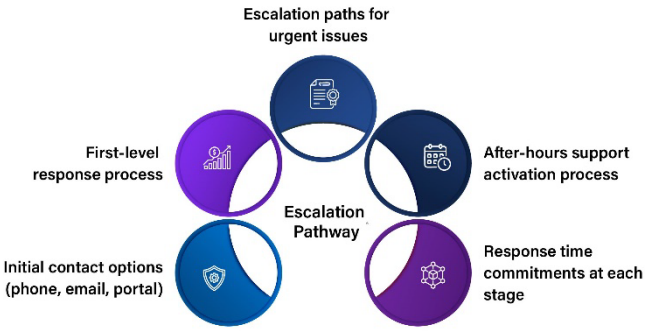


Figure 9 Escalation Pathway

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

  Cogent takes a proactive approach to problem identification and resolution, ensuring that any potential issues are addressed swiftly and effectively. Our Contract Manager leads a dedicated team that will be assigned to this contract, ensuring direct and continuous communication with the Lead State and all potential clients. By fostering open lines of communication, we aim to identify issues early, before they escalate into larger problems.

  To ensure that we stay ahead of any challenges, we will actively solicit written feedback from our clients on a weekly basis. This feedback loop allows us to identify concerns or service gaps early, providing us with the opportunity to address them before they become significant obstacles.

  Once an issue is identified, we will assess the situation in collaboration with the client and create a customized resolution plan that aligns with the client's needs and priorities. Our resolution strategy is tailored to each unique situation, ensuring that the solution is both effective and acceptable to all parties involved. Our Contract Manager will work closely with

the client's Contracting Officer (CO) throughout the resolution process to ensure that the solution is executed to satisfaction.

In the rare event that a service issue or complaint arises, we will follow our structured escalation protocol to resolve it quickly. Our customer service team is trained to handle service complaints with professionalism, ensuring that all issues are addressed in a timely and satisfactory manner. The Program Manager will oversee the entire resolution process, keeping the client informed and involved until the issue is fully resolved.

- Describe how you will assess customer satisfaction.

Customer satisfaction is the key priority of our firm and we actively seek to measure and improve it throughout the duration of our engagements. We use a multi-faceted approach to ensure that our services consistently meet or exceed client expectations.

Figure 10 Cogent's Customer Satisfaction Model

Regular Customer Satisfaction Surveys: To gauge client satisfaction, we conduct regular surveys to collect feedback on key service areas such as responsiveness, quality of work, communication, and overall satisfaction. These surveys are distributed periodically, typically following the completion of significant milestones or projects, allowing us to capture insights into the client's experience at various stages of the engagement.

Ongoing Feedback and Communication: Beyond formal surveys, we maintain open lines of communication with our clients to encourage real-time feedback. Our Program Manager will regularly check in with clients to solicit informal feedback, ensuring that any concerns are addressed promptly. This allows us to identify potential issues before they develop into more significant problems, fostering a positive and transparent relationship.

Post-Resolution Follow-Ups: After addressing any issues or service complaints, our customer service team will proactively follow up to ensure that the resolution was satisfactory and that the client's expectations were met. This feedback helps us continuously improve our problem-solving approach and ensures that our services remain aligned with client needs.

KPI Tracking and Performance Reports: We track key performance indicators (KPIs) related to service delivery, including response times, resolution times, and overall client satisfaction. These metrics are reviewed regularly to monitor our performance and identify areas for improvement. We also provide clients with performance reports that highlight how we are meeting agreed-upon service levels.

Client Satisfaction Reviews: At the end of each engagement or project phase, we conduct formal reviews with clients to assess overall satisfaction. This review involves discussing the client's experience, identifying strengths, and addressing any opportunities for improvement.

The results from these reviews inform our future service delivery and help us fine-tune our approach for ongoing and future projects.

By using these strategies, Cogent ensures that we are always in tune with our clients' needs, continuously improving our services based on their feedback, and delivering the highest level of satisfaction possible.

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.

Cogent is ISO 27001 certified, demonstrating our adherence to international standards for information security management. Our ISO 27001 certification ensures that we manage and protect sensitive client data, with a comprehensive information security management system (ISMS) in place. We also hold CMMI Level 3, ISO 9001, ISO 20000 to further strengthen our security and management systems.

Attached, you will find the certificate validating our ISO 27001 certification, along with additional certifications, further attesting to our dedication to robust security and service excellence.

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.

At Cogent, our approach to artificial intelligence (AI) in cybersecurity and information security is guided by a robust ethical framework. As illustrated in Figure below, we follow seven key dimensions of ethical AI, adapted from the European Commission’s principles. These dimensions ensure that our use of AI is transparent, responsible, and always underpinned by strong human oversight and governance.

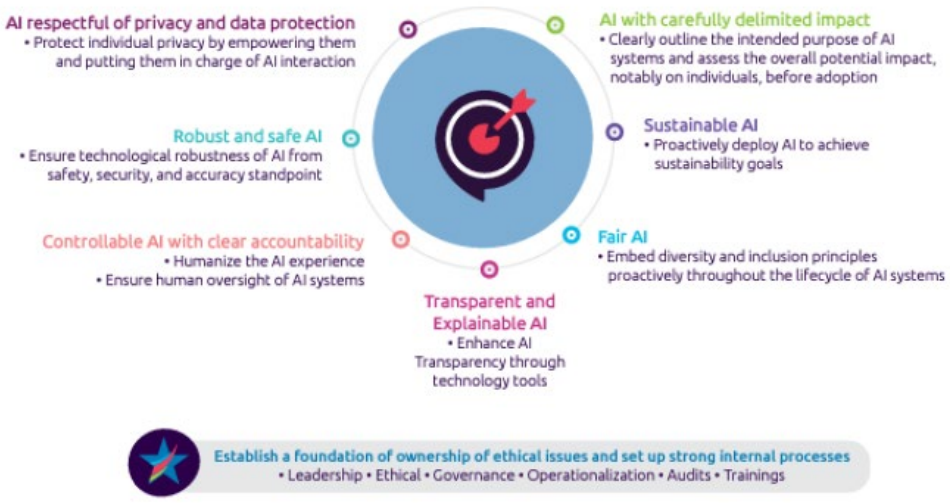


Figure 11 Cogent's Seven Key Dimensions of Ethical AI

By embedding these principles into every stage of our AI deployment from threat detection to risk analysis and reporting, we ensure that all AI-generated findings are subject to rigorous human review, data is protected according to the highest standards, and clients are empowered with clear explanations and privacy controls. This approach provides the State of Idaho and all NASPO ValuePoint entities with the assurance that AI is used ethically, securely, and in full alignment with public sector values.

AI Technologies and Their Purposes:

- We deploy AI-driven security information and event management (SIEM) tools to monitor and analyze large volumes of network data, enabling rapid identification of unusual patterns, behaviors, or potential security incidents.
- Machine learning models are used to assess and prioritize risks and vulnerabilities, ensuring that our teams focus on the most critical threats.
- Natural language processing (NLP) is leveraged to translate complex technical findings into clear, actionable reports for client stakeholders.

Safeguards, Protocols, and Interpretive Reviews:

- All AI-generated findings and recommendations are subject to review and validation by qualified security analysts; AI is never the final decision-maker.
- Data processed by AI tools is encrypted in transit and at rest, in full compliance with all applicable federal, state, and NASPO ValuePoint privacy and data residency requirements.
- Our protocols include documenting and learning from false positives, maintaining transparent communication with clients about the capabilities and limitations of AI tools, and providing interpretive reviews upon request.
- We adhere to a comprehensive ethical AI framework, based on seven key principles: clear purpose, sustainability, diversity and inclusion, transparency, human oversight, technological robustness, and customer privacy controls. These principles guide every aspect of our AI implementation and ongoing operations.

Commitment to Responsible AI:

AI at Cogent is a force multiplier for our security teams, never a replacement for expert human judgment. Our safeguards, governance, and transparency ensure that AI is always used responsibly, securely, and in the best interests of our public sector clients.

VII. ACKNOWLEDGEMENTS AND CERTIFICATIONS

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

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

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

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

B. Non-collusion.

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

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

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

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

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

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

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

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

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

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

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

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

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

K. **Understanding of the RFP.** Offeror has read the RFP in its entirety and understands and agrees to comply with all requirements set forth therein. Any conflicts in the materials composing the RFP and any issues relating to the content of the RFP, including instructions, requirements, or specifications Offeror believes to be ambiguous, unduly restrictive, erroneous, anticompetitive, or unlawful, have been brought to the attention of the Lead State using the process described in the RFP for asking questions or, if applicable, by filing a protest. In accordance with Attachment 01, RFP Terms and Conditions, Offeror acknowledges and understands that any protest, claim, dispute, or action based upon a conflict or issue described herein must be filed no later than the RFP Close Date, and Offeror waives the right to file any protest, claim, dispute, or action based upon a conflict or issue described herein if not filed by the RFP Close Date.

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.

Cogent hereby acknowledges receipt and understanding of the instructions outlined in AMD 2 L. IPRO Cost Submission.

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:

[redacted]

Signature

June 26, 2025

Date

Manu Mehta

Printed Name

President

Title

[redacted]

Email Address

[redacted]

Phone Number