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: Gartner Inc.
B. Primary Business Address: 56 Top Gallant Road, Stamford, CT 06902-7700
C. Federal Tax Identification Number: 04-3099750
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.

www.gartner.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.

Gartner delivers actionable, objective insight to executives and their teams. Gartner was originally incorporated in 1979 (46 years in business) under the name Gartner Group, Inc. In 2001, the company changed its name to Gartner, Inc. Gartner joined the S&P 500 in April 2017.

Since its inception, Gartner has made many acquisitions and investments. The acquired businesses, people and products have broadened our comprehensive suite of product solutions to business and IT professionals worldwide. Key acquisitions in the last 10 years are set forth in the table below.

Table 1. Gartner Acquisitions

Acquired Organization	Acquisition Date	Description of acquired business
UpCity	October 2022	Marketplace connecting small businesses to ratings and reviews of B2B service providers
Topo	October 2019	Subscription-based research and advisory business
CEB	April 2017	Best practices and talent management business
L2	March 2017	Marketing benchmarking business
Machina Research	November 2016	Provides strategic insight and market intelligence related to Machine-to-Machine, Internet of Things, and Big Data
SCM World	June 2016	Supply Chain research and events business
Capterra, Inc.	September 2015	Provider of software products lead generation for small enterprises
Nubera eBusiness	June 2015	Provider of software products lead generation for small enterprises
Marketvisio	May 2014	Former Gartner sales agent and research firm in Finland with a subsidiary in Russia
Software Advice	March 2014	Provider of software products lead generation for small enterprises

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

Gartner has more than 21,000 associates around the world, including 2,500+ research and advisory experts and 950+ consultants.

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

Gartner is a publicly traded corporation (NYSE: IT) incorporated in the state of Delaware in 1979.

Gartner is overseen by an 11-person Board of Directors, including CEO and Chairman, Eugene Hall. The following chart depicts Gartner's management team and structure. Gartner's management team operates under the oversight of the Board of Directors.

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.

Gartner is involved in legal proceedings and litigation arising in the ordinary course of business. Gartner believes the outcome of all current proceedings, claims and litigation will not have a material effect on the company's financial position or results of operations when resolved in a future period, nor impact our ability to provide the services contemplated in this Proposal.

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.

Contract Manager

Name: Amanda Fales	Title: VP Consulting
Email: amanda.fales@gartner.com	Phone: +1 619 819 0368

Gartner's dedicated state and local government (SLG) contracting Vice President (VP), Amanda Fales, specializes in government contracting. Amanda supports the management and tracking of our existing statewide contracts and cooperative agreements, such as NASPO Procurement Acquisition Support Services (PASS) and NASPO IT Research, Advisory and Consulting Services (IT RAC). Her support which includes contract vehicle marketing, establishing Participating Agreements with Participating Entities (PE), and participating in joint government-industry events aimed at cooperative contracting improvements.

Amanda Fales brings more than 20 years of experience in government contracting serving federal, state, and local clients. Amanda and her team are experienced and equipped to handle the different needs and difficulties the Lead State and any Participating Entities may face.

Following presents our proposed Contract Manager's resume:

Amanda Fales

Role: Contract Manager **Experience**: 20+ years **Highest Level of Education**: M.S.

Summary

Amanda Fales is a government contracting professional with over 20 years of experience serving federal, state, and local clients. Amanda leverages her extensive background in public sector contracts and consulting to guide Gartner Consulting sales teams and their clients through contracting strategies, negotiation of new and existing contracts, identification of new contract vehicles, while also providing advice and consultation as a procurement subject matter expert.

Amanda is proficient in MS Office and has a strong technical writing background with effective oral and written communication skills. In addition to her education and credentials below, Amanda has access to the breadth of Gartner Research and is regularly apprised of updated methodology guidance, regulatory issues and emerging technologies.

Prior to joining Gartner, Inc., Amanda worked at Teradata Corporation in San Diego, CA where she led the Americas Sales Operations team. As the Director of Americas Sales Operations, Amanda drove complete revenue reporting fidelity (in partnership with Finance and Administration) and enablement of her sales leaders who were delivering on top-line growth and bottom-line profitability.

Prior to that role, she served as the Teradata Government Enterprise Deal Management where she supported the Federal and State Government sales territory by navigating and managing enterprise transactions from a business standpoint with an overall goal of optimizing transaction deal structure to maximize revenue and profit. She partnered with the Pricing Manager and the Account Team to provide vital counsel to Sales and Sales Management concerning the most appropriate purchasing structure for a customer transaction given the customer's purchasing and budgeting requirements and Teradata's preferred revenue recognition treatment.

Before joining Teradata Corporation, Amanda served as a civilian Navy Contracting Officer in San Diego, CA where she did cradle-to-grave contracting for large research and development systems as well as professional services. In this role, she served as the Contracting Officer on complex multiple award contracts valued at over $950M; for contractor support services task orders valued at over $160M; for Small Business Innovation Research Phase II contracts valued at over $19M; and for commercial item contracts valued at over $5M.

Amanda started her career as a contracts management consultant with Booz Allen Hamilton. She provided senior contracts management consulting expertise to various clients within Naval Information Warfare Systems Command in San Diego, CA. Amanda provided consulting expertise to numerous multi-million-dollar programs where she provided procurement planning, contract execution, and contract closeout expertise. She also engaged in pre-sales and sales activities while managing and mentoring assigned client delivery teams.

Education and Credentials

- M.S., Contract Management, Naval Postgraduate School
- B.S., Management Science (formerly Quantitative Economics and Decision Sciences), University of California at San Diego
- Certified Project Management Professional (PMP)
- Certified Federal Contracts Manager (CFCM)
- Lean Six Sigma Green Belt
- Beta Gamma Sigma (business honor society), member
- Project Management Institute (PMI) and the National Contract Management Association (NCMA), member
- Expert user of Microsoft Suite, Salesforce, and CPQ
- Accredited AWS Technical Professional

Publications and Presentations

- “Streamlining Task and Delivery Order Competitions Within Federal Acquisition Regulation Subpart 16.5 Flexibilities” (https://calhoun.nps.edu/handle/10945/59592)
- NCMA Contract Management magazine article titled "Nondevelopmental Item Procurements: Achieving Results Through Design Re-Use" published in July 2013

Relevant Experience

- Negotiation and Contract Award Support for the County of Los Angeles Registrar/Recorder’s Election Management System (EMS) — Project managed and facilitated cross-functional subject area workshops across multiple internal departments, the County’s attorney, and the system integrator to successfully negotiate the contract for the County’s EMS. This included finalizing statements of work, payment tables, delivery schedules, terms and conditions, SLAs, hosting agreements, etc. The County client was so pleased with Amanda’s performance on the EMS project that they requested she return to support them with another contract negotiation engagement with their team.
- Procurement SME for Lake County, IL — The Gartner Managing Partner and Ms. Fales first met with Lake County in January 2023 to discuss the phased ERP implementation program that Gartner would be assisting with and the associated contracting vehicle challenges. Lake County had a vehicle to cover the scope of the initial phases but not the latter ones. Amanda then met with Lake County’s procurement staff in February 2023 to present contracting options for the latter phases. Lake County procurement was thrilled to learn about Gartner’s NASPO PASS contract which they ultimately used for this engagement. Their procurement lead was extremely grateful for the contracting counsel and commented that she “just needed to ask the right person.”

  Procurement SME for Orange County District Attorney (OCDA) —The Gartner Managing Partner requested Ms. Fales assist with the pre-sale’s activities for this new client in April 2023. OCDA was interested in hiring Gartner for a CMS modernization engagement but needed a contract to do so. Ms. Fales and the MP met with OCDA to discuss potential cooperative vehicles as well as options for piggybacking off locally competed contracts. Based on their discussions with OCDA procurement and legal counsel, they were able to successfully enter into a contract with OCDA and provide them with the modernization they need in a timely manner.

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.

For 46 years, Gartner has been the leading source of independent insight and advice regarding information technology. We are solely focused on the objectives of this engagement and the current and long-term goals of our clients.

Recommendations without Influence

Our recommendations are produced without the influence or approval of outside investors, shareholders, organizations, or directors. We possess no relationships or biases toward any vendor, service provider, or third-party organization, and no downstream technology implementation or service work is performed.

This means there are no conflicts or commercial factors that would unduly influence our work. The recommendations we make are based solely on what we believe will satisfy our client's mission-critical priorities and achieve the greatest success for our client's organization.

Independent Advice from Strategy to Execution

Our consulting solutions provide specific, practical, and impartial advice at all points of the journey from strategy to execution.

Recommendations detailed within the project deliverables clearly articulate how we arrived at our conclusions. Each recommendation answers the specific questions asked of us and enables maximum benefit to the client.

Avoidance of Conflicts of Interest

We leverage a consistent and proven risk management process on a global basis to avoid conflicts of interest on engagements.

Our strict, companywide Conflict of Interest policy ensures associates are aware of their responsibilities regarding their professional conduct. Gartner is the only research organization of its kind equipped with an Ombuds Office designed to protect independence, objectivity, and accuracy.

In today's rapidly evolving digital landscape, organizations face an unprecedented array of cyberthreats. As a cybersecurity consultancy, we understand the critical importance of developing a defensible cybersecurity program. Such a program is not just about deploying the latest technologies; it’s about creating a comprehensive strategy that integrates risk management, technological defenses, employee training, incident response, and regulatory compliance.

A defensible cybersecurity program requires a holistic approach integrating risk management, layered defenses, employee training, incident response, and compliance. By focusing on these key areas and leveraging insights from Gartner, organizations can build a robust cybersecurity strategy capable of defending against evolving threats. Our commitment is to provide a security program that meets immediate needs and adapts to future challenges, ensuring ongoing protection and peace of mind.

Our Approach

To assist eligible entities in the U.S. and its territories with Risk Assessment and Mitigation Services, Gartner’s approach is designed to be scalable and adaptable to meet a diverse range of maturity and needs. Services will include:

1. **Initiate and establish the project approach** to set the foundation for a successful engagement that is delivered on time, within budget and meets/exceeds objectives

2. **Detailed assessment of the current state** of the InfoSec environment (people, process and technology) for contracted entity in alignment with the solicitor's cybersecurity framework including, NIST CSF 2.0, NIST 800-53/171, ISO27001, and/or other security frameworks.
3. **Identify and prioritize** cybersecurity risks and specific gaps based on impact, enterprise risk appetite, and compliance requirements. Develop Current State & Gap Assessment Report to support analysis.
4. **Evaluate and benchmark the cybersecurity program** against peer organizations to identify how the program is performing relative to similar organizations, including spending and personnel benchmarks.
5. **Develop prioritized Recommendations Roadmap report** with essential time sequenced activities to address risks and gaps. **Includes Rough Order of Magnitude (ROM) cost estimates** for each recommended initiative.
6. **Develop a time sequenced roadmap** that aligns recommendations into key initiatives for a phased approach to planning and implementation of the recommendations.
7. **Executive Presentation(s)** of Current State & Gap Assessment, Recommendations & Roadmap, Risk Identification& Mitigation Strategy.
8. **Establish program assurance and measure progress** to ensure Risk Mitigation and cyber modernization strategies are executed as designed and are effective to adapt to changing circumstances.

Approach Overview

A synopsis of Gartner's approach, which is incorporated into this response and is later elaborated upon in greater detail with technical methodology, schedule, staffing, pricing and legal terms:

Risk Assessment & Mitigation Services

- Assess the current-state of the InfoSec environment, including the skills, capabilities, processes and technologies security framework(s) and peer performance
- Develop baseline Current State & Gap Assessment of security and risk management posture compared to cross-industry best practices
- Identify and prioritize specific gaps and risks based on evaluation of current capabilities
- Develop prioritized Recommendations & three-year Roadmap report with essential time sequenced activities to address risks and gaps.
- Develop Mitigation Strategy for High Risk and/or large impact issues; includes preventive measures, contingency plans, and risk transfer options.
- Provide implementation & monitoring services for Risk Mitigation Strategy
- Provide Executive Brief(s)

Scope

People (Organization)

- Members of eligible entity's enterprise information security program, SMEs, and key stakeholders.

Process (Mission and/or IT)

- The in-scope processes and controls of the proposed assessment are defined per a chosen security framework (e.g., NIST CSF 2.0).

Technology (Application, Infrastructure and Data)

- The assessment will include supporting security technologies within the defined security framework (e.g., NIST CSF 2.0 and NIST SP 800 -53 rev 5).

Outcomes/Benefits

- Strategic Planning — Assist security leaders with understanding with a baseline assessment of the current state against controls and provide a prioritization of control areas for focus
- Executive Communication — Provide Executive-ready visuals to support and resource business cases equally, with easy-to-read graphics to open dialogue with team members
- Audit Preparation — Provide readiness assessments for audits or ISO certifications
- Governance Oversight — Provide governance over business lines or entities

Key Deliverables

- Project Planning Materials and Kick-off Presentation
- Current State & Gap Analysis
- Cyber Maturity Benchmark Report
- Strategic Recommendations Report & Three-year Roadmap
- Risk Mitigation Strategy
- Periodic Implementation & Monitoring Report(s)
- Executive Summary

Gartner's Differentiated Approach

Gartner has extensive experience assisting governments at all levels with understanding their current cybersecurity risk posture and developing innovative strategies to improve and mature their Cybersecurity programs. Gartner delivers actionable and unbiased insights and recommendations — free from IT vendors and

integrators — to help our clients achieve their most critical objectives. Gartner maximizes access to Subject Matter Experts (SMEs) by blending Research Analysts and Consultants to provide thought leadership and support innovation.

During Risk Assessment and Mitigation Services engagements Gartner will utilize a standard approach across all entities for assessing maturity, developing a Current state & Gap Assessment, identifying Risk and Mitigation services, as well developing Recommendations & Roadmap. This consistent approach will allow assessed organization to track reductions in cybersecurity risk and improvements in program security year-to-year over, justifying investments in the cybersecurity and IT programs.

Assessing Maturity to inform Risk Mitigation: As security maturity increases, reducing additional risk requires exponential increases in cost and effort. Therefore, organizations in any industry must identify their ideal return on investment

Figure 1. Security Maturity Assessment Sample

Identifying Risk Areas: An entity's maturity is mapped to the desired target state across selected security framework (e.g., NIST CSF). This mapping occurs at multiple levels first at the functional area, then further drill down at the capability level to identity areas of risk consistently. Illustrative examples include:

Figure 2. Sample Entity Assessment Deliverables

Benchmarking Against Peers: An entity's maturity is benchmarked against peer organizations, including spending and staffing models. Enabling strategic planning to consider performance against peer organizations while considering differences in staffing and spending levels.

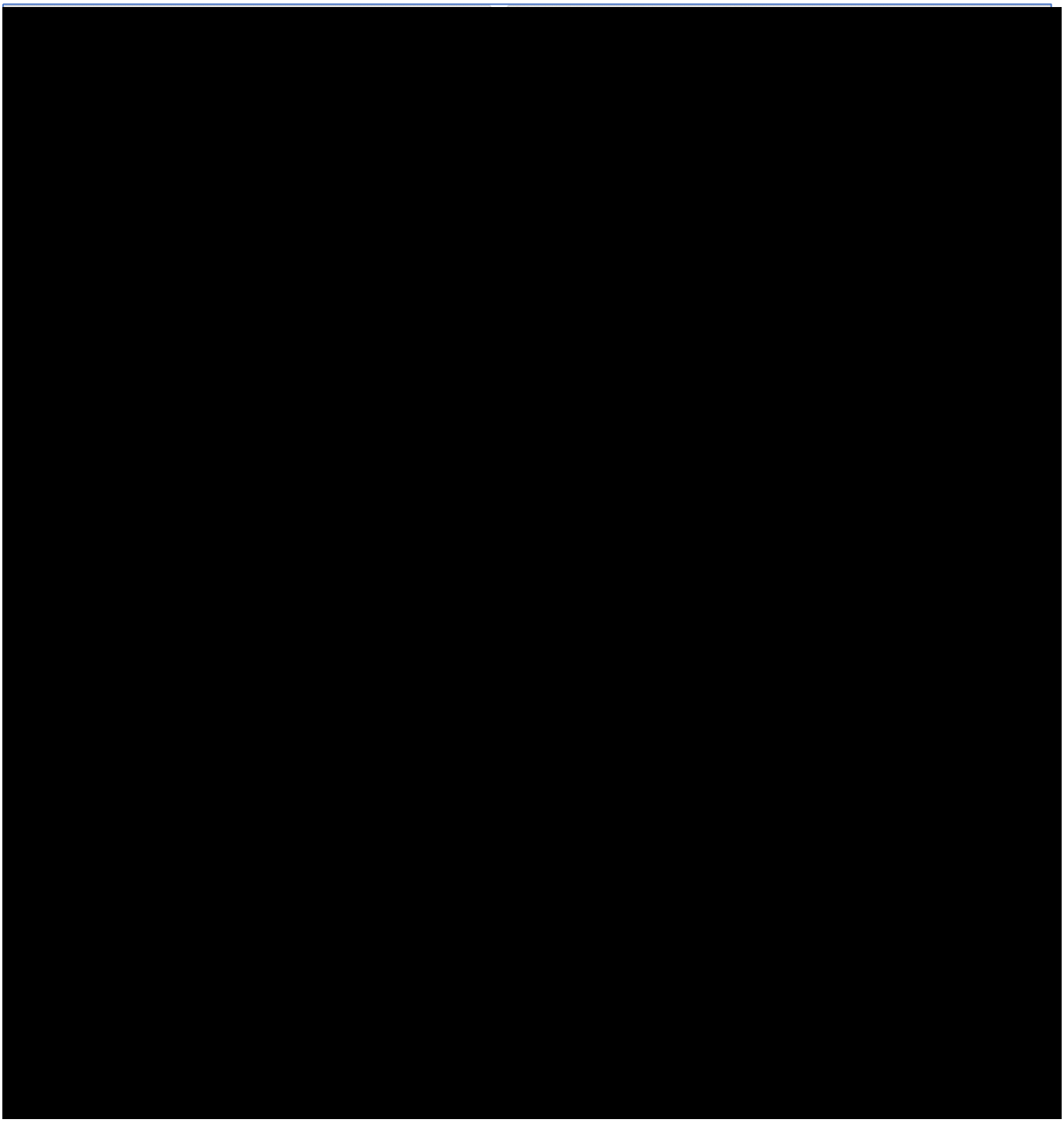
Figure 3. Sample Security and IT Spend Analysis

Current State & Gap Assessment: Each entity's current capabilities, processes, resources and performance will be evaluated against its desired target state for identifying discrepancies or "gaps" between them. This analysis is codified in a Current State & Gap Assessment report. The following provides an Illustrative excerpt from a report:

Figure 4. Sample Vulnerability Gap Assessment Report Excerpt

Recommendations & Roadmap: Each entity will receive a Recommendations & Roadmap report contextualized to their organization, clearly identifying the challenges, risks and gaps and time sequenced activities with estimated ROMs for how to address these gaps.

Figure 5. Sample Recommendations and Roadmap Report Deliverables



Mitigation Services: Cybersecurity modernization programs are high risk and must be properly supported throughout planning, design, and execution phases. Gartner provides program assurance to support Cyber transformation and risk mitigation initiatives. Our approach helps clients to monitor, assess and implement project and program governance capabilities aligned to strategic cybersecurity objectives and risk mitigation activities.

Figure 6. Gartner's Value Realization

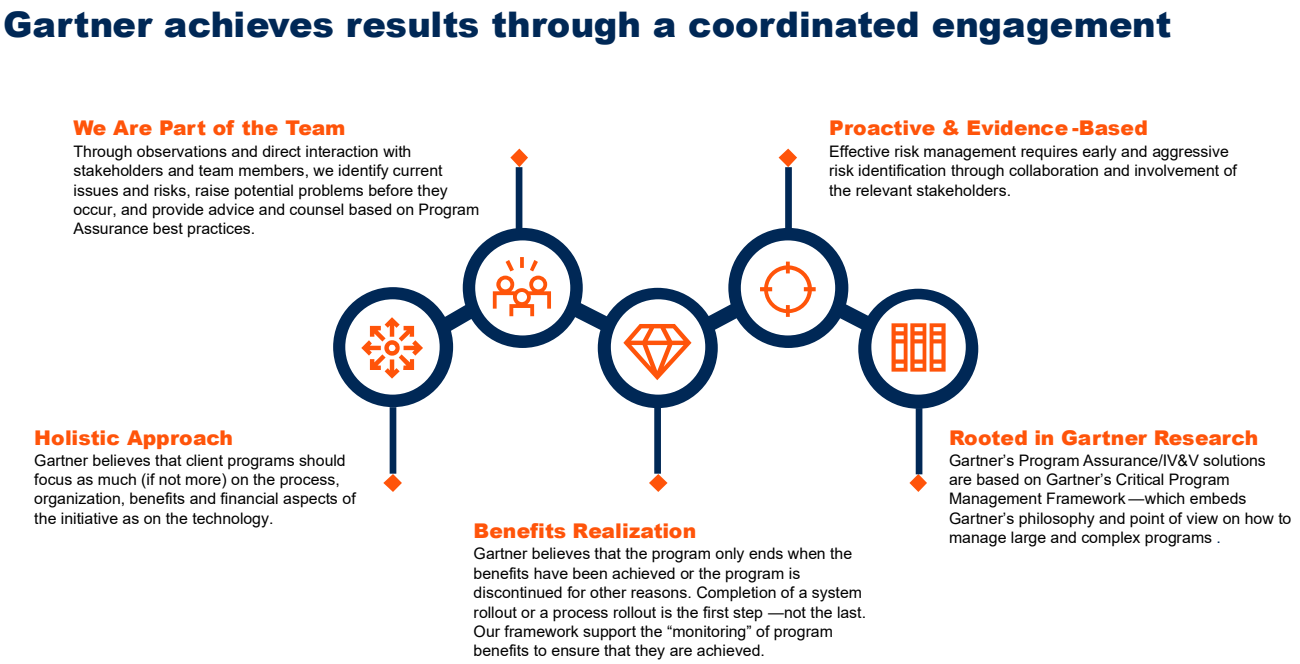
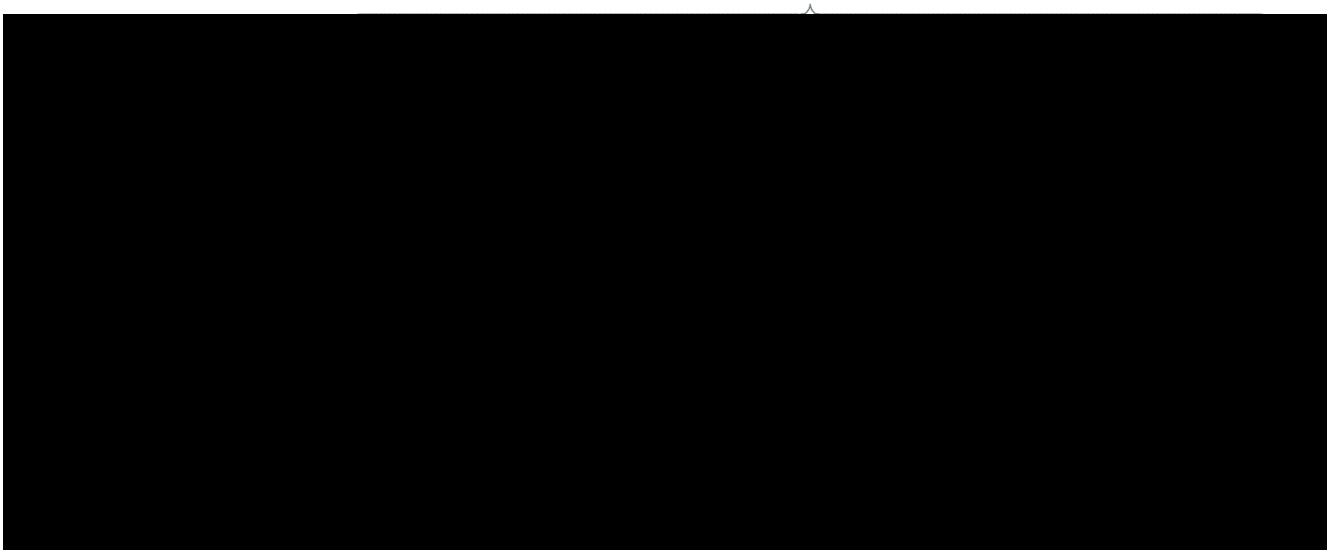


Figure 7. Program Assurance Approach

[redacted]

Figure 8. Program Assurance Risk/Readiness Methodology



Tools and Frameworks: The following frameworks are embedded in Gartner's Cybersecurity and Controls Assessment (CCA) will be utilized to measure maturity for each entity against industry standards (e.g., NIST 2.0, ISO/IEC 27002.2013, NIST SP 800-52). These frameworks support risk assessment and analysis, including detailed narrative, gap analysis and recommendations.

Figure 9. Gartner Security and Risk Management Framework

Engagement Approach

Proposed Engagement Approach: Gartner proposes the following approach to assess the Entity's current security program, identify risks and mitigation strategy, as well as define future-state capabilities with recommendations and a time-sequenced roadmap.

Approach Detail: Gartner's approach is composed of six (6) steps as outlined in Table 2 below.

Table 2. Approach Detail

Phase 1. Project Initiation	
Objective	▪ Work closely with the entity to set the foundation for a successful engagement that is delivered on time, within budget and meets/exceeds objectives.
Activities Performed by Gartner	▪ Host a kickoff meeting to validate the understanding of the project objectives, scope, schedule, and milestones, roles, responsibilities and required resources for Gartner and the entity. ▪ Establish a weekly cadence for status calls to review and monitor the progress of the engagement. ▪ Jointly identify participants for interviews and workshops to solicit input on both current and future-state Security program. ▪ Identify and collect discovery artifacts to support current state understanding of the InfoSec program. ▪ Distribute and review Cybersecurity Controls Assessment (CCA) Survey and validate inputs.
Deliverable(s)	▪ Kick-off Presentation (PowerPoint) ▪ Project Planning Materials (including Status Reporting Template) (PowerPoint)
Phase 2. Discovery	
Objective	▪ Obtain an understanding of the current-state InfoSec function focused on skills, capabilities, processes, plans, technologies and program.
Activities Performed by Gartner	▪ Conduct up to ten (10) virtual conference interviews to gather input from Executive, Managerial and technical stakeholders about: business and regulatory environment; current InfoSec capabilities; business and IT strategies; projects in flight; and gaps between current and desired capabilities. ▪ Provide a secure file transfer service for background documentation. ▪ Review background documentation provided by Entity. ▪ Review completed CCA Survey.
Deliverable(s)	▪ Completed interviews ▪ Completed survey
Phase 3. Current State and Gap Analysis	
Objective	▪ Assess the baseline InfoSec function, develop gap assessment between current state and desired target-state for the security program.
Activities Performed by Gartner	▪ Analyze discovery information to assess current-state InfoSec function in the context of strategies, skills, capabilities, and industry trends in information security. ▪ Identify and prioritize specific gaps and risks: ▪ Identify gaps between cross-industry best practices and peers for information security. ▪ Organize and prioritize gaps according to their potential risk or exposure.

	▪ Validate CCA Security Benchmark Survey responses. ▪ Draft a Current State & Gap Analysis report for review and validation with key stakeholders. ▪ Conduct a workshop to review and validate the draft reports. ▪ Update the Current State & Gap Analysis and Penetration Test reports based on validation workshop(s).
Deliverable(s)	▪ Current State & Gap Analysis Report (PowerPoint)
Phase 4. Cybersecurity Benchmarking	
Objective	▪ Compare security spending to that of organizations with similar industry (e.g., State and Local Government), size (annual revenue, total assets, constituents served, etc.) and risk profile (e.g., highly regulated, critical infrastructure, etc.) ▪ Analyze how current investments in IT Security impact the organization's risk posture and mitigation strategies.
Activities Performed by Gartner	▪ Conduct working sessions to answer questions related to Gartner's spending model. ▪ Obtain security spending data from your finance / cost accounting team for the last 12 months. ▪ Compare security spending to a cohort from the insurance sector. ▪ Compare security spending to maturity. ▪ Draft and validate spend analysis report.
Deliverable(s)	▪ Staffing and Spending Analysis Report (PowerPoint)
Phase 5. Risk Mitigation Strategy	
Objective	▪ Develop a set of recommendations to reduce cybersecurity risk, improve the Information Security program maturity, and meet strategic objectives established for the entity's cybersecurity program. ▪ Identify areas of investment and rough order of magnitude (ROM) to meet risk mitigation goals.
Activities Performed by Gartner	▪ Analyze risk profile and develop an overall approach for managing potential risks. Prioritize risks based on likelihood, severity and impact. ▪ Outline the high-level plan(s) to better manage and control risks. ▪ Develop Risk Mitigation Strategy focused on the "what," "why" and the "how" to resolve identified risks. ▪ Conduct workshop(s) with key stakeholders to review and validate draft Risk Mitigation Strategy, goals and objectives of risk mitigation efforts.
Deliverable(s)	▪ Recommendations Report (PowerPoint)
Phase 6. Strategic Roadmap	
Objective	▪ Develop a time sequenced roadmap that aligns recommendations into key initiatives for a phased approach to planning and implementation of the recommendations.
Activities Performed by Gartner	▪ Draft Roadmap report based on research-identified best practices needed to mitigate risks, close gaps, improve maturity level, optimize operating model and capabilities. Organize the recommendations into a three-year roadmap depicting the sequence and dependencies of actions required to address gap mitigation and improve information security maturity.

	▪ Conduct a workshop to review and validate draft Recommendations & Roadmap with key stakeholders. ▪ Update and finalize the Recommendations & Roadmap Report based on feedback.
Deliverable(s)	▪ Strategic Roadmap (PowerPoint)
Phase 7. Executive Summary	
Objective	▪ Present an integrated overview of the project and a summary of the results to an audience of senior management and key stakeholders for this initiative.
Activities Performed by Gartner	▪ Develop an Executive Summary presentation. ▪ Meet with Entity's Project Sponsor and key stakeholders to review the draft and refine the messaging for the Executive Summary. ▪ Present the Executive Summary to Entity's leadership. (Limited to no more than three presentations)
Deliverable(s)	▪ Executive Presentation (PowerPoint)
Phase 8. Risk Mitigation — Program Assurance Support	
Objective	▪ Support the Entity through risk mitigation activities, implementation, and cyber improvements
Activities Performed by Gartner	▪ Oversee cybersecurity program and governance enhancements. ▪ Maintain risk and action log(s) related to cybersecurity roadmap initiatives. ▪ Provide update(s) to risk log and risk posture based on initiative implementation milestones. ▪ Support entity through technology/vendor procurement, contracting, and oversight.
Deliverable(s)	▪ Monthly Roadmap Status ▪ Cyber Risk Log ▪ Executive Summary/Briefing (Quarterly)

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.

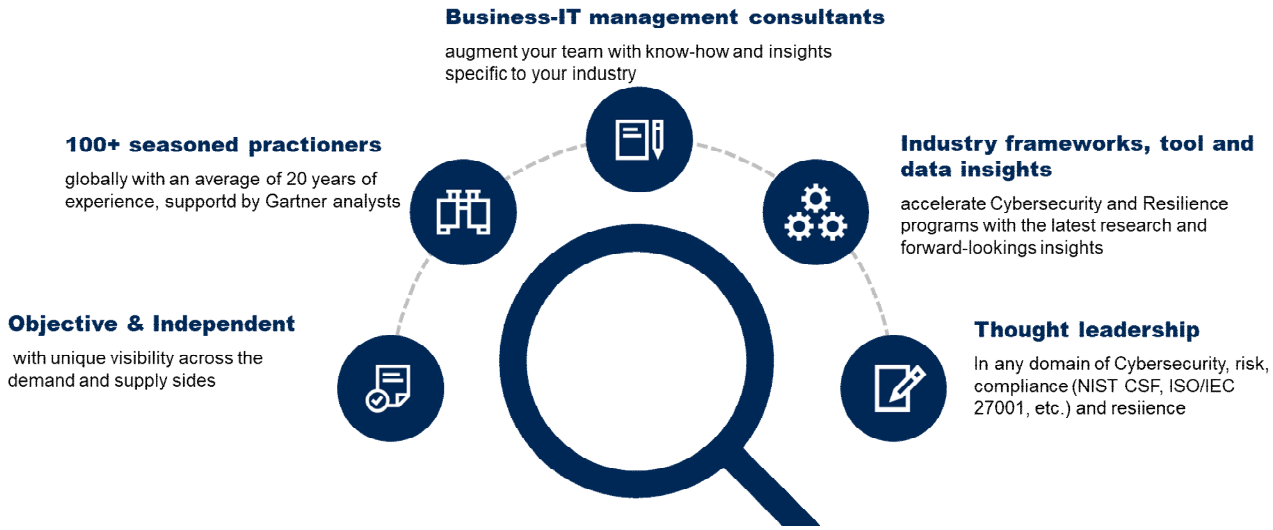
A. Category 1 — Risk Assessment and Mitigation Services — Experience and Qualifications

- **(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.

Gartner has provided information security and cybersecurity risk assessment and mitigation services for more than 25 years. By the early 2000s, Gartner was recognized for its expertise and consulting services in information security, helping organizations address emerging cybersecurity threats, develop security strategies, and apply best practices.

Gartner extensively covers the cybersecurity market with +100 dedicated industry experts, routinely advising and gathering insights from clients, vendors and customers in 600+ calls and interactions each year.

Figure 10. Gartner's Cybersecurity and Resilience Practice Overview



In addition, **Gartner has provided services to public sector clients for nearly 40 years.** Including national, federal, state, regional and local government agencies (cities, counties, municipalities, etc.) and organizations around the world, our dedicated public sector practice delivers deep understanding across multiple government programs, including:

- revenue and taxation
- health and human services
- public safety and justice
- transportation
- pensions and retirement
- environmental
- defense

Gartner has an expansive and successful track record of helping federal, state, and local government organizations maximize their returns on mission-critical projects and initiatives. We have a deep understanding of the complex and often competing challenges facing government organizations, given their unique environment, pressures and orders of magnitude in terms of resources and service requirements.

These experiences have resulted in robust and reliably executed methodologies. Gartner's breadth of clients and engagements has allowed us to develop the deep understanding of the challenges, practices, and dynamics within State and Local Government organizations.

Gartner has provided examples of our Risk Assessment & Mitigation Services project experience in the table below. To assist with the review, we have also provided the following summary matrix which delineates the Category 1 requirements covered by the project experience example.

Projects listed are a representative sample of Gartner's overall experience. With 14,000 clients worldwide, including more than 1,000 public sector organizations, Gartner has substantial experience performing the services identified in Attachment 07 — Scope of Work spanning Category 1 'Risk Assessment & Mitigation Services'.

Category 1 — Risk Assessment & Mitigation Activities:

1. Risk Identification
2. Risk Analysis
3. Risk Prioritization
4. Mitigation Strategy Development
5. Implementation and Monitoring

Table 3. Project Experience: Category 1 — Risk Assessment & Mitigation Services Matrix

	Risk Assessment & Mitigation Activities				
Client Organization	**1**	**2**	**3**	**4**	**5**
[redacted]	X	X	X	X	X
[redacted]	X	X	X	X	
[redacted]	X	X	X	X	X
[redacted]	X	X	X	X	X
[redacted]	X	X	X	X	X
[redacted]	X	X	X	X	X
Multinational Food Corporation	X	X	X	X	
A Global Financial Services Firm	X	X	X	X	X
A Global Payment Processor	X	X	X	X	X

Table 4. Project Experience: Category 1 — Risk Assessment & Mitigation Services

Client Name	Project Title	Project Duration	Key Activities	Outcomes
[redacted]	▪ Network & Security Modernization Program ▪ Identity Access Management Consolidation Strategy	Phase 1: 09/2021-12/2023 Phase 2: 02/2024-06/2025 Phase 3: 01/2025-06/2025	▪ Developed a strategy for the State's Centralized Network and Security modernization goals, including detailed state-wide network & security roadmap, initiative timelines, architecture guidance, and detailed implementation plans for 24 key initiatives. ▪ Supported leadership and stakeholder biennium budgeting efforts for initiative funding requests ▪ Revised and updated strategy and guidance based on emerging cyber and networking market trends, changes in State priorities, and interim progress. ▪ Designed a State-wide identity management program & consolidation program to support whole-of-state Identity Management approach.	▪ A roadmap and detailed architectural recommendations tailored to the State's centralization and cyber risk reduction goals. ▪ An approach to State-wide consolidation of Identity and Access Management. ▪ Independent and unbiased support to justify budgetary needs for modernization initiatives.
[redacted]	▪ Cybersecurity Risk and Maturity Assessment ▪ Cybersecurity Mitigation Recommendations & Roadmap	01/2023-11/2023	▪ Performed security assessments of 18 cities, counties and school systems using a NIST CSF to determine their security maturity across over one hundred NIST CSF subcategories. ▪ Benchmarked organizations against peers for a systematic comparison of capabilities to identify strengths and weaknesses, areas for improvement and setting higher standards. ▪ Assessed the State's central security program using the same NIST CSF approach to determine which areas were strong for the State. This formed the basis for matching State strengths with municipality weaknesses, to determine which services the State could offer the municipalities to help them improve their security posture.	▪ Provided each of the 18 entities with security maturity assessment and targeted recommendations for improvement. ▪ Developed evidence of need for improving the security posture of municipalities across the State. ▪ Provided the State's central IT service organization with an assessment of their security posture. ▪ Partnered with the State to develop a Catalog with cybersecurity services and recommended Plan to improve the security posture of the 18 entities within the State.

Client Name	Project Title	Project Duration	Key Activities	Outcomes
[redacted]	▪ Cybersecurity Risk and Maturity Assessment	12/2021-04/2022 05/2022-10/2022 01/2025-03/2025	▪ Conducted multiple assessments across different departments (e.g., Traffic Management, Utilities). ▪ Evaluation of risk posture spanned OT and IT systems over time. ▪ Benchmarked the security maturity of the acquired entity for comparison with peers and the parent organization. ▪ Identified gaps and opportunities for maturity across the Security Program. ▪ Developed prioritized recommendations and 3-year Roadmap for achieving a target level of security maturity and address future security risks.	▪ Prioritize limited resources for improved security risk reduction and ultimate cost optimization.
[redacted]	▪ Cybersecurity Risk and Maturity Assessment ▪ Cybersecurity Mitigation Recommendations & Roadmap ▪ Election Security Assessment & Penetration Testing	Phase 1: 10/2020-02/2021 Phase 2: 06/2022-10/2022 Phase 3: 07/2023-12/2023 Phase 4: 09/2024-12/2024	▪ Conducted annual cybersecurity program maturity & risk evaluation to track improvements over 4 years. ▪ Developed roadmaps, strategies, and programs to improve the cybersecurity posture of the county-wide security services team. ▪ Executed annual threat-based cybersecurity assessment of the Elections related infrastructure and agency personnel.	▪ A multi-year plan to enhance county-wide cybersecurity. ▪ An objective measurement against strategic and mandatory cybersecurity risk reduction efforts. ▪ Threat mitigation plans to instill confidence in the security of election system(s) and key election personnel.
[redacted]	▪ Security Risk Assessment & Strategy	Phase 1: 01/2018-04/2018 Phase 2: 01/2021-04/2021	▪ Conducted multiple tri-annual security assessments for the Department across IT and OT environments. ▪ Identified gaps and opportunities for maturity across the Security Program. ▪ Benchmarked security maturity of the acquired entity for peer comparison. ▪ Developed prioritized Recommendations and 4-year Roadmap for achieving a target level of security maturity and address future security risks.	▪ Regularly updated insights into the organization's security maturity across IT and OT environments with peer comparisons to contextual findings. ▪ Justified a prioritized remediation investment of approximately $3M over 4 years in areas of security governance, data security, IAM, mobile security, security analytics, and network security for the IT and OT organizations.

Client Name	Project Title	Project Duration	Key Activities	Outcomes
[redacted]	▪ Cybersecurity Risk and Maturity Assessment	07/2015-09/2015 08/2019-11/2019 09/2022-12/2022	▪ Conducted tri-annual Risk Assessments with process rigor, intensity, and breadth of coverage for the overall organization in a consistent and standardized manner. ▪ Evaluated current state and progress made in the development of security capabilities and execution of recommended Roadmap, after initial assessment and for all follow up assessments. ▪ Developed new Recommendations to mature security functions, guidance on what industry trends to consider for continued improvement, an updated forward-looking strategy for the security organization. ▪ Developed Comparative metrics and dashboard for visibility across each security domain. ▪ Gained insight into Security Organization's progress made since previous assessments. ▪ Informed prioritized investment for a three-year horizon. ▪ Reduced risk exposure through Recommendations and mitigation strategies.	▪ Gained insight into Security Organization's progress since previous assessments. ▪ Informed prioritized investment for a three-year horizon. ▪ Reduced risk exposure through Recommendations and mitigation strategies.
Multinational Food Corporation	▪ Cybersecurity Risk and Maturity Assessment	04/2021-08/2021	▪ Conducted Risk Assessment across Enterprise's global footprint. ▪ Leveraged industry standards to evaluate organizational capabilities in a transparent and verifiable manner. ▪ Benchmarked security maturity and spend to peer organizations. ▪ Developed Current State Assessment and identified gaps across the Organization's global footprint.	▪ Insight as to the security posture across the Enterprise's global footprint. ▪ Clear path forward with a prioritized Roadmap and Recommendations for a more harmonized Security Global Program to support sustainable growth.

Client Name	Project Title	Project Duration	Key Activities	Outcomes
			▪ Developed prioritized recommendations with time sequenced roadmaps (three- year horizon) for each region's security program to harmonize and standardize security practices and address gaps.	
A Global Financial Services Firm	▪ Cybersecurity Risk and Maturity Assessment ▪ Cybersecurity Mitigation Recommendations & Roadmap ▪ Cybersecurity Policy & Standards Modernization ▪ Cybersecurity Centralization & Integration Operating Model	Phase 1: 09/2022-01/2023 Phase 2: 02/2023-07/2023 Phase 3: 09/2023-01/2024 Phase 4: 09/2024-01/2025	▪ Conduct annual NIST CSF based cybersecurity risk, technical threat assessment, and spend benchmarking. ▪ Developed, tracked, and maintained multiple 3-year cybersecurity roadmaps to meet cybersecurity modernization and risk reduction goals. ▪ Developed a centralization and integration strategy for	▪ An objective view of cybersecurity risk and spending relative to peer organizations. ▪ An actionable roadmap and activities to meet CIO, CISO, and board-level risk reduction efforts. ▪ A consensus-based design to enable centralized cybersecurity and IT service delivery. ▪ Consistent progress reviews against cybersecurity maturity and risk reduction efforts.
A Global Payment Processor	▪ Cybersecurity Risk and Maturity Assessment ▪ Cybersecurity Mitigation Recommendations & Roadmap ▪ Pre-M&A Cybersecurity Assessments	09/2011-06/2025 (ongoing annually)	▪ Conduct annual NIST CSF based cybersecurity risk and program maturity assessment. ▪ Benchmark against peer organization for risk profile, program maturity, and cybersecurity spend.	▪ Unbiased evaluation of risk and program maturity efforts. ▪ Validation of sustained investment in cybersecurity resources and program improvements. ▪ Board-level reporting against key cyber initiatives.

- **(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.

Gartner has a strong, deep bench of 950 experienced professionals to meet the service needs of the Lead State and Participating States. Our deep expertise in public policy, regulation and the special missions of government agencies balanced with our own efficiency, effectiveness, ethics, and equity enable project success and achievement across all dimensions. Our collective experience across state, local and federal government serves as the foundation for our ability to provide cybersecurity and IT security services that can benefit all NASPO users.

We affirm Gartner has associates with substantial experience and qualifications, both domestically and off-shore (if desired), to fulfill the minimum requirements for Category 1. Risk Assessment and Mitigation Services, as reiterated from Attachment 02 — Scope of Work, section 2.3 below.

Table 5. Category 1 Roles and Minimum Qualifications Description

Role	Description
Security/Technology Senior Analyst (5+ years of professional experience)	Strong technical and/or security skills. Experienced in specific areas, relative to the project. Able to plan and coordinate the technical tasks and work necessary for delivery of services. Able to design and oversee completion of deliverables. Can manage and coach staff and provide QA over the process and work product, as it relates to risk, security and/or technical matters. Strong communications, analysis skills, troubleshooting, and issue resolution skills. Security or technology certification.
Business Process/ Risk Management Senior Consultant (5+ years of professional experience)	Deep knowledge of business processes, industry issues, and/or risk management. Understands big picture and able to prioritize issues, based on data discovery and experience. Can provide recommendations related to security and technology matters. Able to supervise large and diverse teams and provide QA over the process and work product. Often serves as a technical subject matter specialist. Strong communication and facilitation skills.
Project Manager (5+ years of professional experience)	Project Management and Business process subject matter experts. Skills and experience in managing engagement work efforts, scoping and assigning work, and managing engagement budgets. Tracks and communicates project status and demonstrates project value. Project management certification.

In addition to the three labor categories identified above for Category 1, Gartner has a variety of Value Add roles with a breadth of experience to handle the different needs and difficulties associated with public sector cybersecurity and IT security engagements. The description and qualifications of these roles are presented in the table below.

Table 6. Gartner Value Add Roles Description

Role	Description
Principal (15-20 years of professional experience)	Leads Gartner's relationship with the contracted entities and NASPO, including its current and past work under NASPO contract vehicles. Extensive experience in helping clients with assessment, planning and implementation around IT and Cybersecurity Risk Management, strategy, governance, communications and organizational change management.

	May possess applicable industry credentials such as: ▪ Project Management Professional (PMP) ▪ Certified Federal Contracts Manager (CFCM) ▪ Lean Six Sigma Green Belt ▪ National Contract Management Association (NCMA) member
Cybersecurity and Resilience Senior Expert (15-20 years of professional experience)	Provides oversight for Risk Assessment and Mitigation Services for all contracted entities. Supports scoping activities and Quality Assurance (QA) review of the Gartner's Project Plans and deliverables. Promotes outcome driven results and leverages Gartner's methodologies and tools for standardized and consistent delivery to contracted entities. May possess applicable industry credentials such as: ▪ PMP ▪ Certified Information Systems Auditor (CISA) ▪ Certified Data Privacy Solution Engineer (CDPSE) ▪ Certified in the Governance of Enterprise IT (CGEIT) ▪ Certified in Risk and Information Systems Control (CRISC) ▪ Certified Information Systems Security Professional (CISSP) ▪ Amazon Web Services (AWS)-Certified Solution Architect Professional
Cybersecurity Specialist (10-15 years of professional experience)	Leads team of security professionals in completing Risk Assessment and Mitigation activities, including identifying and assessing risks and vulnerabilities; the development and implementation of Cybersecurity Risk and Mitigation strategies, program security policies and protocols, ensuring compliance with relevant security, regulatory, and legal framework(s). Advises senior management and stakeholders on Risk Assessment and Mitigation strategies. Identifies and leads implementation of continuous program enhancements and evaluating existing processes. Supervises large and diverse teams and provides QA over process and work products. Serves as technical subject matter for Cybersecurity Risk Assessments and Mitigation Strategies. Strong communication and facilitation skills.
Cybersecurity Engagement Manager (5-10 + years of professional experience)	Bridges technical cybersecurity knowledge with client's business needs. Provides day to day design and delivery of cybersecurity solutions, including Risk Assessments and Mitigation services ensuring alignment with customer strategies and promoting secure practices. Serves as the Project Manager and cybersecurity business process subject matter expert. Experienced in managing and delivering Cybersecurity engagements, including Risk Assessments and Mitigation services. Manages project lifecycles and delivery teams, scopes and assigns work, as well as manages engagement budgets. Strong communication and facilitation skills.
Cybersecurity Risk Analyst (5+ years of professional experience)	Analyzes data, business processes, and other reference material to identify security risks, develops mitigation strategies, and ensures compliance with industry regulations and internal policies. Experienced implementing industry best practices in alignment with security frameworks and aligning clients' governance, processes, controls, etc. to meet legal and regulatory requirements for compliance.

Table 7 below presents representative examples of the qualifications and experience of Gartner personnel who may be assigned to a project. Actual personnel assigned to a project will depend on the scope of services and expertise required. Additional resources across Gartner Consulting with similar skills and experience may be called upon to deliver services as needed.

Table 7. Representative Sample of Gartner Personnel Qualifications and Experience

Personnel	Years of Experience	Cybersecurity and IT Security Experience	Public Sector Experience	Strong Communication Skills	Ability to Work With and Manage Diverse Teams	Education	Certifications
Amanda Fales (Key Person: Contract Manager)	20	✓ (contracting and procurement)	✓	✓	✓	▪ M.S., Contract Management ▪ B.S., Management Science	▪ Project Management Professional (PMP) ▪ Certified Federal Contracts Manager (CFCM) ▪ Lean Six Sigma Green Belt ▪ National Contract Management Association (NCMA) member
Michael Orozco	20+	✓	✓	✓	✓	▪ B.A., Finance ▪ B.A., Psychology	▪ PMP ▪ CISA ▪ CDPSE ▪ CGEIT ▪ CRISC ▪ CISSP ▪ AWS Certified Solution Architect Professional
Christopher Thomas	30+	✓	✓	✓	✓	▪ M.A., Computer Resource and Information Management ▪ B.S., Computer Science	▪ CISSP ▪ Certified Information Security Manager (CISM) ▪ Certified Ethical Hacker (CEH) ▪ Certified Network Defense Architect (CNDA) ▪ Certified in Information Technology Infrastructure Library (ITIL) Foundation

Personnel	Years of Experience	Cybersecurity and IT Security Experience	Public Sector Experience	Strong Communication Skills	Ability to Work With and Manage Diverse Teams	Education	Certifications
Brian Massa	15+	✓	✓	✓	✓	▪ Doctor of Information Systems and Communications (D.Sc.) ▪ M.S., Engineering Management ▪ B.S., Systems Engineering Management	▪ CISSP ▪ PMP
Heidi Schmidt	25+	✓	✓	✓	✓	▪ M.S., Telecommunications Management	▪ CISSP ▪ CISM ▪ Certified in ITIL V3 Foundation
Michael Love	10+	✓	✓	✓	✓	▪ Bachelor of Science; Finance, Accounting, and Information Systems	▪ AWS Certified Solutions Architect — Professional ▪ AWS Certified Security Specialty ▪ ITIL V3 Foundations certifications ▪ Certified Scrum Master
Jed Chapin	10+	✓	✓	✓	✓	B.A., Information Technology Management	

- **(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.

Gartner recognizes that services from Categories 2-4 for Incident Response, Breach Coaching, and Notification and Credit Monitoring Services require specific types of service levels for detection, response, notification, and reporting (e.g., four-hour time to respond to incidents, etc.) However, for Category 1: Risk Management and Mitigation services, these types of traditional service levels are not relevant, and appropriate service level measures vary widely based on the specific scope of work and client environment. As such, we will work with the Lead State/Participating Entities to define SLAs that will guide the delivery of our services.

Upon receiving a scope of work from the Lead State/Participating Entity, Gartner initiates various scoping and planning activities, including the establishment and mutual agreement of timelines, budget, metrics, deliverables, etc.

The first 2 phases of any new project with Gartner are described below:

PHASE 1: Project Initiation

Gartner Activities and Results

- Create customized approach based on the client environment, requirements and challenges.
- Conduct preparation including internal kickoff meeting with subject matter experts, identification of relevant Gartner research, and establishing an online project repository.
- Create collaborative approach by using the most appropriate collaborative tools.
- Conduct a client kickoff meeting to confirm understanding of the project objectives, scope, schedule, milestones, roles and responsibilities of required resources, and anticipated risks and mitigation strategies.

Value to the Client

- Increased project success through customized approach — not "cookie cutter."
- The client does not pay for learning curve; project team "hits the ground running." Increased efficiency through use of a project repository tool.
- Open lines of communication between Gartner and the client throughout the entire project life cycle.
- Project that is delivered on time and within budget; ability of the client to plan for its involvement.

PHASE 2: Discovery

Gartner Activities and Results

- Build project management plans, baseline schedule and risk list that is updated throughout the duration of the project.
- Apply project management tools and leading techniques, customized based on the client requirements and characteristics.
- Define governance model to formalize key project processes and rules for making important project decisions.

Value to the Client

- Increased value and decreased project risk through proactive approach to identifying and mitigating risks.
- Rigor in project management, with more than 20% of all Gartner associates Project Management Institute (PMI) certified.

- More-efficient execution of decision making and recurring tasks.

- **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.

Gartner Consulting offers a comprehensive suite of cybersecurity and resilience solutions and capabilities:

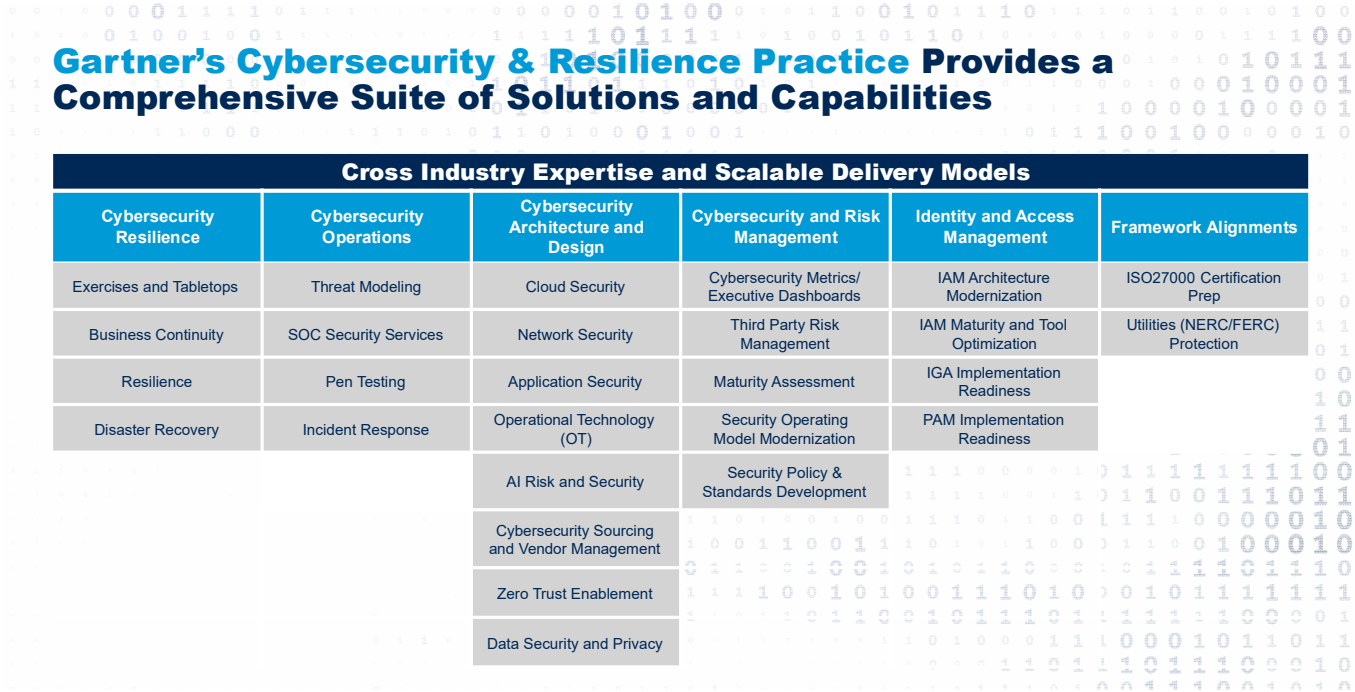


Table 8. Gartner Value Add Services

Cybersecurity Capability	Value Added Service	Description
Cybersecurity Resilience	Tabletop Exercises	Evaluate the effectiveness of these plans in real-world scenarios and their integration with broader organizational security policies. Design and conducting tabletop exercises with meticulously crafted scripts and relevant injects to test and enhance plan effectiveness.
	Business Continuity	Assess, establish or optimize the Business Continuity Program by helping clients establish a sound risk management practice well integrated with established decision-making processed and aligned to industry standards such as ISO 22313.
	Disaster Recovery Resilience	Assess existing IT Resilience or Disaster Recovery Program against best practices. Recommend a course of action to mature the IT Resilience or Disaster Recovery Program.

Cybersecurity Capability	Value Added Service	Description
		Formulate a strategy for IT Resilience structured around data protection, workload recovery and location/facilities. Develop resilience patterns based on business requirements, in order to guide IT architecture. Assess hosting and service delivery models to identify operating model gaps that have implications for technology resilience. Provide data center and networking architecture reviews.
Cybersecurity Operations	Threat Modeling	Conduct comprehensive technical reconnaissance from both external and internal perspectives to identify vulnerabilities and cyber hygiene risks. Execute targeted phishing simulations aimed at employees and executives to assess susceptibility to social engineering attacks. Evaluate security controls through hypothesis-driven campaigns, simulated data exfiltration, and attempted compromises, ensuring client operations remain unaffected. Develop a tailored threat model using attack techniques from the MITRE ATT&CK Framework, relevant to the client, and formulate a monitoring and response strategy to address identified gaps. Provide detailed reports outlining specific vulnerabilities, at-risk assets, prioritized threats, threat actor profiles, and actionable recommendations for enhanced security posture.
	Penetration Testing (PenTesting)	Coordinate penetration testing services cover both IT and operational technology (OT) environments. Follows the Penetration Testing Execution Standard (PTES). Structured, methodical approach to security testing while minimizing operational disruptions.
	Incident Response	Review current Security Operations and Incident Response Plans to ensure alignment with industry best practices. Evaluate the effectiveness of these plans in real-world scenarios and their integration with broader organizational security policies. Scrutinize escalation procedures to ensure clarity in roles, responsibilities, communication channels, and decision-making processes. Design and conduct tabletop exercises with meticulously crafted scripts and relevant injects to test and enhance plan effectiveness.
Cybersecurity & Risk Management	Cybersecurity Metrics/ Executive Dashboards	Engage business, cyber and IT teams in establishing shared understanding of acceptable risk thresholds and targets for mission-critical services.

Cybersecurity Capability	Value Added Service	Description
		Identify 'right fit' outcome driven metrics for dashboards and reports to support desired data driven insights to enable risk-based decision-making by defining target levels in the form of Protection Level Agreements (PLA). Develop dashboards and reports for the Board, C-Level and Operations teams.
	Third Party Risk Management	Design and establish a Third-party Risk Management function: Develop policy, framework and tools to identify and manage Cyber and Resilience risk of managing third parties. Categorize third-parties by criticality to you supply chain: Based on criteria that we co-develop (e.g., criticality of the business processes, information shared or created by the third-party, etc.) with the client organization, categorize third-parties by criticality. Conduct assessments of third-parties to identify cyber and resilience issues: Based on industry standards we can conduct cybersecurity and resilience assessments of third parties to identify and rank issues or risks. Design and develop a dashboard to view third-party issues and risks: Design and develop a dashboard that displays known issues and risks across your supply chain/third-parties.
	Operating Model Modernization	Bring Business, IT and Security stakeholders together toward your Security vision. Define accountability/decision rights, measures of performance, location strategy, skills and sourcing of talent. Defined security governance processes (Steering committee charter, Key risk/performance indicators RACI, responsibilities across three lines of defense). Review staff and organizational structure to determine fit with security objectives. Inventory skills to identify opportunities to align talent with your current and forecasted needs. Review sourcing model to identity opportunities to realized talent and location strategy.

Cybersecurity Capability	Value Added Service	Description
Identity and Access Management	IAM Architecture Modernization	Identify business level objectives for IAM by understanding business priorities. Develop vision and strategy for IAM modernization by addressing the needs to support the journey of customers, partners and workforce. Define the target picture with tangible objectives, improvements needed and investment priorities. Define a clear and efficient roadmap with actionable steps, while setting priorities to activities and investments needed. Execute the strategy by driving the IAM program to success.
	IAM Maturity and Tool Optimization	Develop a robust strategy for IAM modernization that effectively addresses urgent business scalability needs, ensuring organizations are equipped to handle growth and evolving demands. Deliver a comprehensive analysis of existing IAM processes and technology architecture, highlighting gaps and areas for improvement, while offering insights into industry trends and leading IAM methodologies. Craft a detailed roadmap for IAM modernization, complete with actionable recommendations that cater to immediate priorities and support the management of scalable processes aligned with future business objectives. Prepare clients for vendor negotiations by creating well-structured RFP packages, ensuring they are informed and ready to procure new IAM technologies or operational services that best meet their needs.
	IGA Implementation Readiness	Evaluate the current state of a client's IAM governance, processes, and technologies to determine how an IGA platform will fit within the architecture. Document current IGA architectural alignment, gaps, and desired use cases for the IGA platform. Facilitate workshops with client stakeholders and subject matter experts to identify and discuss relevant use cases for the client's particular user populations and target systems, operational processes that are ideal for automation, and key IGA controls and requirements for prioritization. Develop a set of prioritized recommendations for initiatives necessary to implement and support an IGA platform now and in the future. Craft requirements for an IGA platform that meet the client's objectives which can be included in a Request For Proposal (RFP) used to procure a new IGA platform.
	Cloud Security	Identify the cloud security business and skills requirements required to support the cloud strategy.

Cybersecurity Capability	Value Added Service	Description
Cybersecurity Architecture and Design		Develop an organizational cloud risk framework and responsibilities model. Design and prioritize the cloud security controls and policy guardrails to mitigate to security challenges. Build a cloud security architecture that aligns business needs to control requirements and security capabilities showing preference for existing investments and cloud-native. Enhance supporting across capabilities across cybersecurity and IT to enable the cloud strategy objectives.
	Application Security	Evaluate and prioritize programmatic risks including architectural practices, supportability, resiliency areas, collaboration, and integration. Seamlessly embed security as part of development life cycle to reduce security risks and build secure by design applications. Improve collaboration between development and security siloes to minimize exposure to cyber threats and deliver DevSecOps efficiencies. Deliver strategy roadmaps to support Application Security modernization initiatives.
	AI Risk and Security	Conduct thorough evaluations of AI risks and devise a roadmap to mitigate potential threats and vulnerabilities. Analyze the market to identify best tools and features to better enable AI trust and manage risk and security. Conduct security controls assessments in AI enabled environments. Developing protocols for enhancing defensive behavior when attack is detected to be AI enhanced. Implement a pilot or proof of concept to test and validate security measures, features, and tools for AI systems and security capabilities. Leverage AI technologies (to include agentic AI) to enhance and expedite security operations, threat detection, Identity and Access Management (IAM), and overall defensive security measures.

Cybersecurity Capability	Value Added Service	Description
	Zero Trust Enablement	Baseline Zero Trust maturity against existing capabilities and processes based on relevancy and importance to organization's business objectives. Define targeted recommendations for improved security posture based on prioritized uses cases for improvements across: User, Device, Data, Network, Applications, Automation and Visibility. Refine IT and Security Strategy to align with Zero Trust principles for proactively mitigating threats with an achievable, time sequenced roadmap. Identify controls, processes and technologies to improve security posture and limit attack surface. Demonstrated improvements with 'right fit' metrics.

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.

Not applicable. Gartner is not responding to Category 2.

- **(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.

Not applicable. Gartner is not responding to Category 2.

- **(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.

Not applicable. Gartner is not responding to Category 2.

- **(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.

Not applicable. Gartner is not responding to Category 2.

- **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.

Not applicable. Gartner is not responding to Category 2.

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.

Not applicable. Gartner is not responding to Category 3.

- **(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.

Not applicable. Gartner is not responding to Category 3.

- **(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.

Not applicable. Gartner is not responding to Category 3.

- **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.

Not applicable. Gartner is not responding to Category 3.

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.

Not applicable. Gartner is not responding to Category 4.

- **(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.

Not applicable. Gartner is not responding to Category 4.

- **(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.

Not applicable. Gartner is not responding to Category 4.

- **(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.

Not applicable. Gartner is not responding to Category 4.

- **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.

Not applicable. Gartner is not responding to Category 4.

AMD 2 E. (M) Subcontractors.

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

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

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

Gartner has substantial experience, knowledge, skills and resources specific to the services identifying in the NASPO Cybersecurity and Information Security Services RFP, as well as the resources and capacity to perform the services.

Should the need for additional specialized skills, knowledge or local resources arise for a particular assignment, we will work with the client and seek approval prior to engaging any subcontractors. We do not engage subcontractors without prior approval of our client.

Gartner has a Subcontractor division dedicated to vendor identification and onboarding. Gartner utilizes its vast network to identify qualified subcontractors. In the event that Gartner's Subcontractor division is unable to identify the right resource in a timely manner, Gartner utilizes two contracted third party staffing firms to assist in rapid identification.

Gartner maintains a Consulting Subcontractor policy designed to optimize procedural compliance and reduce risk. All Gartner's subcontractors are bound by a Master Services Agreement approved by Gartner's Legal Team, which includes provisions for confidentiality.

Gartner is committed to conducting business in an ethical and honest manner and in compliance with all applicable laws and regulations. Toward that goal, Gartner endeavors to work with reputable subcontractors which conduct their business in a manner that shows such a commitment. We view our suppliers and subcontractors as partners in delivering on our commitments and, just as we hold ourselves to the highest standards of ethics and compliance, we expect the same from each of our subcontractors.

In fact, we pride ourselves on the strong relationships we build with suppliers and our shared focus on ethics, compliance, fair practices, integrity, safety and quality. To confirm consistency and mutual commitment, Gartner

requires that our suppliers (including their employees, representatives and subcontractors) comply with the Gartner Supplier Code of Conduct.

While not anticipated, should the need to engage subcontractors arise, Gartner confirms that we will obtain written approval from the Lead State or Participating Entity and that any subcontracted resources will meet or exceed all minimum requirements established in this RFP.

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.

1. [redacted]

Sales under contract in last 5 years: $[redacted]

Gartner was awarded a [redacted] contract for multiple service categories; one of which is IT Assessments, Planning, Independent Verification and Validation (IV&V), and Market Research, Procurement Advisory, and Contract Implementation Services that aligns to this procurement.

IT Assessments and Planning may include IT effectiveness, maturity, governance, and architecture. Strategic planning activities may include mission statement development, visioning and goals, objectives, and strategy development. Assessment of staff knowledge, skills and abilities, bandwidth, time and motion studies, and succession planning are included in this category. Strategic planning development and tactical planning may require the provisioning of actionable plans and roadmaps. Organization change management, enterprise architecture, cloud assessments, and network performance assessments are within scope as well. Also included in this category are the independent verification and validation procedures that are used together for in-depth analysis of a product, service, or system for compliance with requirements as well as the independent oversight of software (or systems) development life cycle (SDLC) processes and specifications.

2. [redacted]

Sales under contract in last 5 years: $[redacted]

[redacted]

Gartner was awarded a contract for several service categories, one of which is Category 7: Cyber Security. This category includes Cyber Security Analysis (Service 7.1) and IT Security Risk Assessment (Service 7.4). Services include:

Cyber Security Analysis — planning and security advisement for security related plans, training and other customer cybersecurity needs. Deliverables may include plans and recommendations for black box testing, gray box testing, credentialed testing, device/system configuration, external and internal scans, IT security controls audit, external and internal vulnerability assessments, security program review, security awareness training, social engineering and awareness testing, security plans, business continuity plans, disaster recovery plans, and incident response plans.

IT Security Risk Assessment — planning and security advisement for security related plans, training and other customer cybersecurity needs. Deliverables may include plans and recommendations for black box testing, gray box testing, credentialed testing, device/system configuration, external and internal scans, IT security controls audit, external and internal vulnerability assessments, security program review, security awareness training, social engineering and awareness testing, security plans, business continuity plans, disaster recovery plans, and incident response plans.

3. [redacted]

Sales under contract in last 5 years: $[redacted]

[redacted]

Gartner was awarded a contract for several service categories, including procurement strategy and planning, independent government cost estimates, specifications/scope of work review, market research, cost & pricing analysis, solicitation review and preparation, source selection, cost realism analysis, contract development & management, completion & closeout, contract management, vendor performance evaluation program, procurement policy and digital procurement transformation, category management, change management and procurement transformation assistance, training, project management, and grants assistance, as well as a variety of value add services including cybersecurity and risk assessment consulting, IT governance, program assurance and independent validation and verification (IV&V), etc.

In addition, Gartner holds a variety of cooperative contracts for use by public entities (state agencies, local governments, independent school districts, public universities) in other states and jurisdictions for the service categories requested in this solicitation.

The following table presents additional examples of Gartner's cooperative contracts in the U.S.

Table 9. Other Cooperative Contracts

Coop. Contract	Contract Number	Approx. Sales Volume	Link to Contract Page
[redacted]	[redacted]	Confidential	[redacted]
[redacted]	[redacted]	$[redacted]	[redacted]
[redacted]	[redacted]	Confidential	[redacted]
[redacted]	[redacted]	Confidential	[redacted]
[redacted]	[redacted]	Confidential	[redacted]

Gartner's GSA contract is entitled to the most favorable pricing.

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

Gartner attends the NASPO Exchange Conferences, where we actively work to meet with all states where Participating Addenda for our existing Master Agreements are not in place, and would continue this practice if awarded a Cybersecurity and Information Security Master Contract.

Gartner also employs a collaborative team across Sales and Consulting that are mutually responsible for marketing and managing the contract to deliver the most favorable outcome for each client. The team meets on a weekly basis to collectively align activities for managing the State's relationship.

- ***Marketing Initiatives:*** Gartner markets directly to State, Local and Education clients across the U.S. Our team works together with NASPO Participating Entities/eligible customers to understand their needs and provide products and services to support their organization's mission-critical priorities. Upon execution of

the Master Agreement, Gartner will inform our associates (e.g., Consulting Managing Partners) who work directly with State, Local, and Education clients across the U.S. of its availability to promote immediate use.

Gartner employs a multichannel strategy to market its available products and services to NASPO Participating Entities/eligible customers through webinars, conferences, consulting clinics, and complementary Research & Advisory and Consulting offerings where appropriate. Our marketing initiatives have resulted in great success for other cooperative contracts.

Similar to the NASPO Cybersecurity contract, eligible customers currently purchase acquisition support services from Gartner through our existing NASPO PASS and IT RAC contracts. Our strong market position and continued partnership with Participating Entities and other State and Local government agencies will help drive further use of the cooperative contract resulting from this RFP.

- ***Marketing Literature:*** Gartner plans to create a Marketing "Slick Sheet" for Gartner use, which would be approved by NASPO. For example, Gartner similarly created a 2-page NASPO PASS Marketing "Slick Sheet" that was approved by NASPO for Gartner use. The marketing literature is intended to be used by Gartner sales teams to educate potential customers on the contract, its benefits, scope, and ordering information. It is expected that this Sheet will be distributed at tradeshows or expos as well as emailed to existing and prospective customers who are candidates for using this contract.
- ***Webinars:*** Gartner produces and presents regular webinars available to NASPO Participating Entities/eligible customers eligible customers that cover a wide range of technology topics.
- ***Conferences:*** Gartner regularly hosts and participates at major public sector conferences to proactively identify and market opportunities for cooperative contracts, and would include NASPO Cybersecurity and Information Security services. A few key conferences include the Gartner IT Symposium/Xpo, Gartner Data & Analytics and Security & Risk Management Summit (among other IT role-focused Summit conferences) and the Gartner Supply Chain Symposium/Xpo.
- ***Consulting Clinics:*** Gartner offers complementary consulting clinics to all eligible consulting customers. These clinics offer eligible customers the opportunity to meet one on one with our industry and subject matter experts across a wide range of technology topics. The outcomes of these clinics provide customers with actionable next steps and create additional opportunities to promote contracting through NAPSO Cybersecurity and Information Security following state, local and education entities' procurement policies and guidelines.
- ***Customer Reach Out and Inquiries:*** Gartner account teams are also responsible for reaching out to customers and responding to their inquiries to actively market Gartner products and services available through cooperative contracts. These activities include:
  - Proactive marketing using POVs (Points of View) to illustrate trends, tools and solution benefits.
  - Needs analysis meetings with individual state, local and education organizations.
  - Extensive scoping, sizing and pricing methodologies to help develop SOWs.
  - Email and webinar campaigns based on areas of expertise and latest public sector trends (e.g., efficiency and modernization, AI, IT governance, sourcing, cybersecurity, etc.).

In addition, Gartner Consulting has over 40 full-time Consulting Managing Partners specifically focused on serving public sector and education organizations nationwide. These leaders meet on a regular basis to collectively align on properly leveraging and promoting our cooperative contracts. Further, Gartner's Contracts Manager is a dedicated state and local government Vice President (VP) who specializes in government contracting. The Contracts Manager supports the management and tracking of our existing statewide contracts and cooperative agreements, such as NASPO Procurement Acquisition Support Services (PASS) and NASPO IT Research, Advisory and Consulting Services (IT RAC). The Contracts Manager will continue this support which includes contract vehicle marketing, establishing Participating Agreements with Participating Entities (PE), and participating in joint government-industry events aimed at cooperative contracting improvements.

- 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.

In working with NASPO ValuePoint in the past, NASPO ValuePoint has maintained the customer website, which Gartner reviews to confirm information is accurate, current and accessible to clients. Should the Lead State and NASPO ValuePoint desire Gartner to establish and maintain a customer website, Gartner has the capability to do so, having successfully established and maintained customer websites for other cooperative agreements.

We intend to launch a comprehensive website, or link to the NASPO ValuePoint customer website (based on your preference), which will contain all pertinent contract information such as contract number, contract name, period of performance, contract description, Gartner point-of-contact, and a link to the contract on NASPO's website. We also plan to have this contract information accessible from our public-facing gartner.com website.

For example:

- Gartner information for our current NAPO PASS contract is available on the NASPO ValuePoint website (naspovaluepoint.org/portfolio/procurement-acquisition-support-services/gartner).
- Gartner information for the current NASPO IT Research & Advisory Services contract is also available on the NASPO ValuePoint website: naspovaluepoint.org/portfolio/it-research-advisory-services/gartner-inc.

- 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.

Gartner has consistently maintained several cooperative contracts over the past two decades and have processed a significant number of orders under the NASPO frameworks. Our associates are familiar with NASPO purchase order and administrative/reporting requirements for each SOW and regular reporting and payment requirements to NASPO. Each SOW agreement is assigned an Engagement/Project Manager that is responsible and accountable for the end-to-end processing of the order and the successful completion of the SOW deliverables.

Gartner's proposed Contracts Manager, Amanda Fales, supports the management and tracking of our existing statewide contracts and cooperative agreement, such as the NASPO Procurement Acquisition Support Services (PASS) and NASPO IT Research, Advisory and Consulting Services (IT RAC). She will also provide support in setting up new Participating Public Agency accounts.

To familiarize staff with Master Agreement terms and pricing and compliance, Gartner's Contracts manager, who specializes in government contracting, will provide training which includes detailed explanations of the Agreement's (and associated Participating Addenda) key provisions, a clear understanding of pricing structures, and interactive sessions to address questions and clarify where needed. Ongoing support, such as regular updates on changes to the Agreement (and associated Participating Addenda) will also be provided to maintain staff knowledge.

Initial Training:

- Comprehensive Overview: Provide a thorough explanation of the Master Agreement, including its purpose, scope, and key clauses.
- Pricing Structure: Clearly outline the pricing and how it applies to different situations or services.
- Interactive Sessions: Conduct Q&A sessions to address any questions or concerns regarding the agreement and pricing.

Ongoing Support:

- Regular Updates: Provide updates on any changes to the Master Agreement and/or PAs to maintain staff knowledge.
- Resource Materials: Make readily available relevant documents, guidelines, and examples for reference.

- Individualized Support: Offer personalized guidance and support to individual staff members as needed.

Compliance Monitoring:

- Regular Audits: Conduct periodic audits to ensure compliance with the Master Agreement's terms and pricing.
- Reporting and Feedback: Provide feedback to staff and management on any non-compliance issues and corrective actions needed.

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

Similar to our approach to market the Master Agreement and encourage participation among potential Participating Entities, including state governments, Gartner will encourage adoption and usage of the Master Agreement through:

- ***Customer Reach Out and Inquiries:*** Gartner account teams are also responsible for reaching out to customers and responding to their inquiries to actively market Gartner products and services available through cooperative contracts. These activities include:
  - Proactive marketing using POVs (Points of View) to illustrate trends, tools and solution benefits.
  - Needs analysis meetings with individual state, local and education organizations.
  - Extensive scoping, sizing and pricing methodologies to help develop SOWs.
  - Email and webinar campaigns based on areas of expertise and latest public sector trends (e.g., efficiency and modernization, AI, IT governance, sourcing, cybersecurity, etc.).
- ***Client Interactions:*** When contracting and negotiating terms and conditions with public sector clients, Gartner knows the value of a quick, seamless contracting experience. Where possible, we encourage our clients to utilize established cooperative contracting agreements because we know the value our clients receive from the comprehensive terms and conditions and pricing established cooperative contract master agreements, including transparency, reduced risk, and contracting efficiency.
- ***Marketing Initiatives:*** Gartner markets directly to State, Local and Education clients across the U.S. Our team works together with NASPO Participating Entities/eligible customers to understand their needs and provide products and services to support their organization's mission-critical priorities. Upon execution of the Master Agreement, Gartner will inform our associates (e.g., Consulting Managing Partners) who work directly with State, Local, and Education clients across the U.S. of its availability to promote immediate use.

  Gartner employs a multichannel strategy to market its available products and services to NASPO Participating Entities/eligible customers through webinars, conferences, consulting clinics, and complementary Research & Advisory and Consulting offerings where appropriate. Our marketing initiatives have resulted in great success for other cooperative contracts.

  Similar to the NASPO Cybersecurity contract, eligible customers currently purchase acquisition support services from Gartner through our existing NASPO PASS and IT RAC contracts. Our strong market position and continued partnership with Participating Entities and other State and Local government agencies will help drive further use of the cooperative contract resulting from this RFP.
- ***Marketing Literature:*** Gartner plans to create a Marketing "Slick Sheet" for Gartner use, which would be approved by NASPO. For example, Gartner similarly created a 2-page NASPO PASS Marketing "Slick Sheet" that was approved by NASPO for Gartner use. The marketing literature is intended to be used by Gartner sales teams to educate potential customers on the contract, its benefits, scope, and ordering information. It is expected that this Sheet will be distributed at tradeshows or expos as well as emailed to existing and prospective customers who are candidates for using this contract.

- ***Webinars:*** Gartner produces and presents regular webinars available to NASPO Participating Entities/eligible customers eligible customers that cover a wide range of technology topics.
- ***Conferences:*** Gartner regularly hosts and participates at major public sector conferences to proactively identify and market opportunities for cooperative contracts, and would include NASPO Cybersecurity and Information Security services. A few key conferences include the Gartner IT Symposium/Xpo, Gartner Data & Analytics and Security & Risk Management Summit (among other IT role-focused Summit conferences) and the Gartner Supply Chain Symposium/Xpo.
- ***Consulting Clinics:*** Gartner offers complementary consulting clinics to all eligible consulting customers. These clinics offer eligible customers the opportunity to meet one on one with our industry and subject matter experts across a wide range of technology topics. The outcomes of these clinics provide customers with actionable next steps and create additional opportunities to promote contracting through NAPSO Cybersecurity and Information Security following state, local and education entities' procurement policies and guidelines.

In addition, Gartner Consulting has over 40 full-time Consulting Managing Partners specifically focused on serving public sector and education organizations nationwide. These leaders meet on a regular basis to collectively align on properly leveraging and promoting our cooperative contracts.

- 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?)

Gartner has dedicated Contracts and Legal personnel responsible for reviewing and negotiating terms and conditions of all Participating Addenda requested by our clients. With multiple Contracts and Legal associates covering regions around the U.S., we are able to devote resources to simultaneous negotiation of multiple Participating Addenda.

Since Participating Addenda represent long-term relationships, Gartner strives to approach these negotiations collaboratively with the goal being a "win" for both parties. Collaborative negotiations require that Gartner understands the interests, motivations, and risks facing the Participating Entity (PE). This valuable expanded information about our customer allows us to give and take in an appropriate and informed manner. For example, where PEs are statutorily required to include specific language in the PA, Gartner is largely amenable to such inclusion since Gartner understands that its exclusion would likely pose an unacceptable risk to the PE.

In addition, our team is intimately familiar with previously negotiated terms and conditions across numerous jurisdictions. This large set of previously negotiated terms and conditions serves as an extremely useful data source to help initiate and guide negotiations with new PEs.

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

Upon execution of a Master Agreement and Participating Addenda for a specific scope of work, Gartner is able to quickly mobilize a delivery team to provide the services. Our deep bench of 2,500+ research and advisory experts and 950+ consultants allows us to identify personnel with the appropriate skills, background, knowledge and expertise to deliver exceptional value throughout each engagement.

We have an internal resource management function (Professional Development) that manages the number of projects that our consultants are assigned to at any given moment. This optimizes value to the clients and resource utilization, reducing the likelihood of competing client demands. The Resource management is a global function, sponsored at the most senior levels of Gartner Consulting, which sets consistent standards for people-related initiatives across the organization. The Professional Development function is a physical manifestation of

Consulting's commitment to individual growth and development, established in response to the needs of both associates and clients. Professional Development managers are based in hub offices, tasked with the objective of integrating these initiatives on a local/regional level as well as acting as the pipeline for providing feedback and input from associates to guide activity. Professional Development partners with other functions to promote a vibrant, enthusiastic local community that places priority on skill enhancement and growth.

Key advantages gained from Gartner's Professional Development function include:

- Offers local leadership to support all people-related initiatives.
- Enhances efficiency and effectiveness of associate staffing (i.e., matching client needs with associate availability, interests and development goals/opportunities).
- Promptly identifies associates with necessary skill sets, experience and credentials.

- 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.

Not applicable. Gartner is a sole source provider of Research, Advisory and Consulting services. Gartner does not utilize dealers, partners or resellers.

For any use and tracking of subcontractors in performance of Consulting services, we have the systems and processes in place to properly manage them throughout the project life cycle. For example, once a subcontractor is under contract with Gartner for a particular project, the company is entered into our Vendor Management System where the subcontractor can submit invoices and revenue forecasts. In this same system, Gartner can pay submitted invoices and run various reports on subcontractor data such as amount invoiced, amount paid, etc.

G. (ME) **Customer Service**

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

Gartner personnel meet with clients during a regular cadence of meetings and are also available on an as-needed basis to address any ad hoc questions/requests. Additionally, the Gartner interactive Client Support Team is available toll-free 24 hours a day, Monday to Friday, to support clients' general customer service and technical needs.

The assigned Gartner project teams will be made fully available based on the agreed upon project start date with the Participating Entity. Those associates designated as key personnel will be dedicated to the project based on the mutually agreed upon scope of work. At any time throughout the course of the engagement clients will be provided with contact information for the Project Manager and Managing Partner who can be reached 24/7.

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

For each project, Gartner assigns a dedicated Managing Partner and Project Manager. The Managing Partner is entrusted with the responsibility of monitoring and achieving client satisfaction as well as project oversight to provide an additional layer of assurance and quality. The Project Manager is responsible for the day-to-day management of overall project initiatives and acts as the primary point of contact for the Gartner Team through the project.

Our Project Managers, working closely with our Managing Partners, are entrusted with the responsibility of overseeing the assigned staff, achieving client satisfaction, and addressing any escalation that may arise. Key responsibilities of the Project Manager include:

- Aligning Gartner activities to support the client's goals.
- Building and maintaining a long-standing relationship with the client.
- Providing high-level oversight of the project.
- Taking action as needed to resolve issues.

Issue Escalation

Our issue escalation process aims to promptly address and resolve client concerns, achieving a high level of client satisfaction and successful project outcomes. While details of the process may vary depending on the nature and severity of the issue, we typically follow the process outlined below.

- **Initiate Communication** — The Client Project Manager communicates open risks/issues for meeting the project milestone to the Gartner Project Manager.
- **Assess and Investigate** — The Gartner Project Manager conducts a thorough assessment of the issue, gathering relevant information and investigating root causes; this may involve discussions with the client, internal team members and other stakeholders.
- **Escalate to Leadership** — If the issue cannot be resolved at the project level, it is escalated to the appropriate Client and/or Gartner leadership.
- **Resolve** — Gartner works closely with the client to develop a resolution plan, which may involve implementing corrective actions, revising project strategies or taking other appropriate measures to address the issue.
- **Close and Follow-up** — Gartner maintains open and transparent communication with the client throughout the resolution process, providing regular updates on issue resolution progress to adequately address the client's concerns. After the issue is resolved, Gartner Consulting may conduct a post-resolution review to identify any lessons learned and implement improvements for future projects.

- Describe how you will assess customer satisfaction.

Gartner is committed to delivering value for clients on all engagements. We regularly and consistently measure the outcome of our work with our clients via a formal **Client Satisfaction Survey** at the close of every engagement to monitor that our best practices and project approaches are fueled by continuous feedback. In addition, the Gartner Project Management Life Cycle includes activities to achieve and monitor client satisfaction as well as mitigation activities targeting any concerns or issues identified by the client. These activities include:

- Conducting a joint kickoff meeting to establish a common understanding of project scope and methodology, establish any metrics or KPIs by which quality will be measured, and to confirm Gartner deliverables are structured in accordance with the client's requirements and quality expectations.
- Providing regular status reports throughout the engagement that include an analysis of potential risks and appropriate mitigation actions.
- Maintaining open lines of communication with the client during each phase of the project so that any issues can be rapidly identified, communicated and resolved.
- Performing a close-out procedure after the engagement is completed which may include a Customer Satisfaction Questionnaire/Post-Engagement Review to assess the client's satisfaction and elevate satisfaction on future efforts with the client.

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

SSAE 16/SOC 2 Type II — Gartner uses third-party co-location facilities to support technology services in an environment that provides flexibility, scalability, and security. Our U.S.-based co-location data centers are SOC 2 Type II certified. The trust service principles on which SOC 2 is based are modelled on five principles: security, availability, processing integrity, confidentiality and privacy. Each of these principles have defined controls that must be met to demonstrate adherence to the principles and to produce an unqualified opinion during an independent audit.

Gartner requires execution of a Non-Disclosure Agreement to provide a copy of our SOC 2 Type II report and requests to provide a copy of the report upon apparent award.

National Institute of Standards and Technology (NIST) 800-171 — Gartner understands the importance of protecting Controlled Unclassified Information (CUI). We have established uniform policies and practices to align with NIST Special Publication 800-171. In addition to defining and implementing safeguard requirements for CUI, Gartner maintains an up-to-date System Security Plan (SSP) and Plan of Action and Milestones (POAM) to maintain compliance with NIST 800-171.

ISO 27001: Information Security — Gartner maintains certification with ISO 27001. We have developed and implemented a comprehensive Information Security Management System (ISMS). Gartner applies a systematic approach to securely managing sensitive, confidential information by implementing best-practice information security policies, systemized controls and risk management processes. We adopted an overarching management process for information security controls to meet our information security needs on an ongoing basis.

Sarbanes-Oxley (SOX) — As a publicly traded company, we have developed specific controls to protect our financial processes and reporting obligations. Our internal and external auditors perform an annual evaluation of SOX control effectiveness. This evaluation includes, but is not limited to, controls over Access Security, Change Management, Program Development and Computer Operations.

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.

Gartner is exploring generative AI (GenAI) tools to assist in routine and administrative tasks, creating opportunities for our associates to take on more interesting and challenging tasks that will enable us to get better, faster, stronger, every year. Gartner's opinion and insights continue to be human-led.

To ensure we use generative AI ethically, we have implemented the following guiding principles:

- Ethical Use: All GenAI-enabled tools must be developed and used in an ethical manner, respecting human rights, privacy and fairness.
- Transparency: We will be transparent about how we use GenAI. We are mindful of the importance of client trust in our research, products, and services.
- Accountability: We hold ourselves accountable for the outcomes of our AI-enabled tools.
- Compliance: GenAI use at Gartner must comply with relevant laws, regulations, and industry standards, including data protection and intellectual property laws. All Gartner associates, contractors, interns, and sales agents must complete mandatory training and sign a generative AI attestation showing that they understand this policy.

By leveraging our private GenAI tools, Gartner consultants can create customized deliverables with greater efficiency and quality to accelerate the timelines for desired outcomes. Highlights of Gartner's usage of GenAI include:

- **Safe and Secure** — Our private GenAI tool has features and functionality like ChatGPT, but only Gartner associates have access to our GenAI tool. Because Gartner private GenAI tools are not on the public internet, proprietary information is not shared externally and stays safely inside Gartner's secure environment. In addition, Gartner associates complete core compliance trainings at the time of hire on specific topics including GenAI and Data Protection.
- **Advice by and for Humans** — We do not outsource decisions to machines — our independent and objective advice is created by and for humans. Our recommendations are informed by our proprietary data and access to thousands of experts without bias toward a specific platform or product.
- **Governed by Gartner** — Use of Gartner private GenAI tools is restricted and governed by Gartner policies and procedures. For example, our private GenAI Chat is designed so that any client information entered within a session cannot be viewed by other users of the tool in a subsequent session. Gartner has established an AI Council to oversee the way we use GenAI across the organization. We also have a cross-Business Unit working group in place to monitor/report the use of GenAI across the organization, ensure that this use follows our guidelines, and ensure tie does not put our intellectual property or our client data at risk.

Gartner uses a combination of third-party software and proprietary tools that incorporate GenAI technology. These tools are designed to enhance associate productivity and deliver exceptional value to our clients. Gartner uses GenAI in various ways to help deliver value to our clients, including:

- Creating meeting summaries that identify action items
- Summarizing Gartner research
- Generating ideas and improving copy quality for marketing materials.

Gartner **does NOT** use any client data to train or inform internal or external GenAI models or allow third party services providers or subcontractors to do so either. Gartner also **does NOT** use GenAI to produce the insight that we provide to our clients. The insight is generated by our experts based on their knowledge and experience.

VII. ACKNOWLEDGEMENTS AND CERTIFICATIONS

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

A. <u>Debarment.</u> (Check one of the below.)

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

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

B. <u>Non-collusion.</u>

1. This proposal has been developed independently by Offeror and has been submitted without collusion and without any agreement, understanding, or planned common course

of action with any other Offeror or supplier of Deliverables in a manner designed to limit fair and open competition.

2. The contents of this proposal have not been communicated by Offeror or its employees or agents to any person not an employee or agent of Offeror and will not be communicated to any such persons prior to the RFP Close Date.

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

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

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

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

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

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

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

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

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

H. Confidential, Proprietary, or Protected Information. As set forth in Attachment 01, RFP Terms and Conditions, if Offeror is claiming any portion of its proposal as confidential, proprietary, or protected, Offeror must complete the required sections of Attachment 11, Claim of Trade Secrets

and Non-Public Information, and submit with Offeror's proposal a redacted copy of Offeror's proposal, which must be clearly marked as such. Offeror may not mark pricing or Offeror's entire proposal as confidential, proprietary, or protected. Submission of a Claim of Trade Secrets and Non-Public Information does not guarantee that information claimed by Offeror as confidential, proprietary, or protected will not be subject to disclosure in accordance with applicable public information laws, rules, and policies. If Offeror fails to submit a redacted copy of Offeror's proposal, or fails to claim information as confidential, proprietary, or protected in compliance with this RFP, Offeror releases the Lead State, NASPO, NASPO members, and entities represented on the Multistate Sourcing Team from any obligation to keep the information confidential and waives all claims of liability arising from disclosure of the information.

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

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

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

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

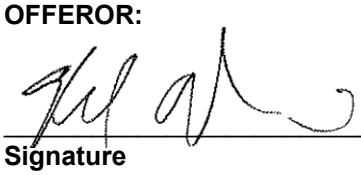
Signature

The undersigned is one of the following:

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

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

OFFEROR:



Signature

June 26, 2025
Date

Paul Denvir
Printed Name

Managing Vice President
Title

paul.denvir@gartner.com
Email Address

+1 908 249 8007
Phone Number