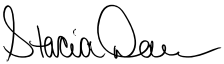




NOTICE OF AWARD

State Of Missouri
Office Of Administration
Division Of Purchasing
PO Box 809
Jefferson City, MO 65102-0809
<http://oa.mo.gov/purchasing>

CONTRACT NUMBER CT260033004	CONTRACT TITLE Statewide – Cybersecurity and Information Security Services (NASPO) CONTRACT PERIOD October 7, 2026 through October 31, 2027.
REQUISITION/REQUEST NUMBER NA	MissouriBUYS SYSTEM ID/MOVERS SUPPLIER ID NUMBER MB00079770/1000939
CONTRACTOR NAME AND ADDRESS Gartner, Inc. 56 Top Gallant Road Stamford, CT 06902-7700	STATE AGENCY'S NAME AND ADDRESS Various State Agencies throughout the State of Missouri
ACCEPTED BY THE STATE OF MISSOURI AS FOLLOWS: In accordance with section 34.046, RSMo, contract CT260033004 between the State of Missouri and Gartner, Inc is hereby awarded by the State of Missouri consisting of the attached documentation as specified in section 4.1 of the attached Cooperative Contract Procurement document.	
BUYER Emily Thompson	BUYER CONTACT INFORMATION Email: Emily.Thompson@oa.mo.gov Phone: (573) 751- 8897 Fax: (573) 526-9816
SIGNATURE OF BUYER 	DATE 10/7/26
DIRECTOR OF PURCHASING  Stacia L. Dawson	



Memorandum

To: File
From: Emily Thompson
Date: 08/31/26
Re: Proprietary Information

Gartner, Inc. requested that a portion of their proposal submitted in response to CPPT30034902600033 be considered proprietary and not be made available for public review. The determination was made that the information is proprietary pursuant to section 610.021, RSMo, and therefore has been sealed and will not be released to the public for review.

State of Missouri
Office of Administration, Division of Purchasing



Cooperative Contract (COOP) for Cybersecurity and Information Security Services

COOP CONTRACT NUMBER NO.:	CT260033004
COOP CONTRACT ISSUED ON BEHALF OF:	Statewide various state agencies
CONTRACTOR NAME AND ADDRESS:	Gartner, Inc. 56 top Gallant Road Stamford, CT 06902-7700
ISSUE DATE:	6/24/26
CONTRACT PERIOD:	Effective Date of Contract through 10/31/2026
REQUISITION NO.:	N/A

REQUESTED RESPONSE DATE: 07/07/26

Response may be submitted by e-mail to the buyer or record or mail, courier, or hand-delivered to the Division of Purchasing at 301 W. High Street, Rm. 630, Jefferson City, MO 65101.

COOP CONTACT INFORMATION:

BUYER: Emily Thompson
PHONE NO.: (573) 751-8897
EMAIL: Emily.Thompson@oa.mo.gov

DELIVER SUPPLIES/SERVICES FREE ON BOARD (FOB) DESTINATION TO THE FOLLOWING ADDRESS:

Various State Agency's throughout Missouri

Vendor's Organization Name:	Gartner, Inc.		
MissouriBUYS Supplier Number:	MB00079770		
Point of Contact:	Will McGuire		
Phone Number:	+1-(571) 683-4482	Email Address:	Will.McGuire@gartner.com
Mailing Address:	56 Top Gallant Road		
City/State/Zip:	Stamford, CT - 06902-7700, United States of America		
Vendor Tax Filing Type with IRS (check one):	☒ Corporation ☐ Individual ☐ State/Local Government ☐ Partnership ☐ Sole Proprietor ☐ IRS Tax-Exempt		
What date did the vendor's organization begin operation?	Date: 06/01/1990		

The Contractor hereby agrees to provide the services and/or supplies described in the attached NASPO ValuePoint Contract #MA2025004 for the State of Missouri subject to the conditions stated on page 2. The Contractor further agrees that when a Notice of Award is signed and issued by an authorized official of the State of Missouri, a binding contract shall exist between the Contractor and the State of Missouri.

Authorized Signature	DocuSigned by: <i>David Vixama</i> CCE13228C8BD44B...	Date	July 22, 2026
Printed Name David Vixama		Title	Assoc. Director

ATTENTION:

1. After reviewing the Cooperative Contract Document (COOP), the contractor must complete and return the **cover page above and all necessary exhibits**.
2. Due to lead times for obtaining the information needed to complete the various **Business Compliance Exhibits** herein as explained in the cooperative contract document's Vendor Response Exhibits, the vendor are encouraged to IMMEDIATELY begin securing these verifications.
3. The vendor must achieve "**Approved**" registration status in MissouriBUYS (WebProcure/Proactis) and "**Spend Authorized**" registration status in MissouriBUYS, powered by MOVERS to be considered for a contract award. Reference Section 5.

Cooperative Contract Organization:

COOP Sections	Section 1	Introduction and Background Information Section
	Section 2	Scope of Work Section
	Section 3	Terms and Conditions Section
	Section 4	General Contractual Requirements Section
	Section 5	Vendor Submission and Award Information Section
COOP Vendor Response Exhibits	Exhibit A	Response Submittal Checklist
	BUSINESS COMPLIANCE EXHIBITS	
	Exhibit B	State of Missouri Tax Compliance
	Exhibit C	Registration of Business Name with the Missouri Secretary of State
	Exhibit D	Business Entity Certification, Enrollment Documentation, and Affidavit of Work Authorization
	Exhibit E	Anti-Discrimination Against Israel Act Certification
	Exhibit F	Services Outside the United States
	Exhibit G	Employee/Conflict of Interest
	Exhibit H	Federal Funding Unique Identity ID
COOP Attachments	Attachments (Separate Documents) (Do not return these documents with response)	
	Attachment 1	Business Associate Provisions
	Attachment 2	Federal Funds Requirements
	Attachment 3	Missouri Statewide Quarterly Admin. Fee Instructions and Report
	Attachment 4	Missouri Statewide Contract Admin. Fee Quarterly Usage Instructions and Report

1. INTRODUCTION AND BACKGROUND INFORMATION SECTION

1.1 Introduction:

- 1.1.1 Purpose: This document constitutes a request from the State of Missouri, Office of Administration, Division of Purchasing, to enter into a cooperative contract for the provision of Cybersecurity and Information Security Services as set forth herein for various State agencies throughout Missouri (hereinafter referred to as “state agency”) in accordance with the requirements, provisions, and pricing specified herein.

1.2 Cooperative Contract Authority:

- 1.2.1 Section 34.046, RSMo, allows the commissioner of administration may also participate in, sponsor, conduct or administer a cooperative purchasing agreement whereby supplies are procured in accordance with a contract established by another governmental entity provided that such contract was established in accordance with the laws and regulations applicable to the establishing governmental entity.

1.3 General Instructions and Requirements:

- 1.3.1 The vendor must complete and sign the first page of this document, thereby agreeing to provide the referenced products and/or services under the requirements, terms and conditions provided herein. Contractor signature is required to confirm the offer to contract for the products and/or services described herein and to confirm agreement that upon receipt of a Notice of Award signed by an authorized official from the State of Missouri, Division of Purchasing, a binding procurement contract shall exist between the vendor and the State of Missouri. Invoices for products and/or services provided for the State of Missouri must be submitted to the address shown on Page 1.

1.4 Glossary of Terms and Acronyms:

- 1.4.1 Whenever the following terms and acronyms appear in the cooperative contract document or any amendment thereto, the definitions or meanings described below shall apply.

1.4.2 General Glossary, Acronyms, and Abbreviations:

- a. **Agency and/or State Agency** means the statutory unit of state government in the State of Missouri for which the equipment, supplies, and/or services are being purchased by the **Division of Purchasing (Purchasing)**. The agency is also responsible for payment, unless otherwise specified herein.
- b. **Amendment** means a written, official modification to a contract.
- c. **Attachment** applies to all documents which are included with cooperative contract document to incorporate any informational data or requirements related to the performance requirements and/or specifications.
- d. **Buyer** means the procurement staff member of Purchasing.
- e. **Code of State Regulation (CSR)** contains the current administrative rules of executive agencies of Missouri government. The regulations are arranged by agency rather than by subject.
- f. **Contract** means a legal and binding agreement between two or more competent parties, for a consideration for the procurement of equipment, supplies, and/or services.
- g. **Contractor** means a supplier, offeror, person, or organization who is a successful vendor as a result of a cooperative contract and who enters into a contract.
- h. **Exhibit** applies to forms which are included with a cooperative contract document for the vendor to complete and submit with their response.
- i. **May** means that a certain feature, component, or action is permissible, but not required.
- j. **Must** means that a certain feature, component, or action is a mandatory condition.
- k. **Party** refers to either the State of Missouri or the contractor as an entity that may enter into a contract pursuant to the terms herein.

- l. **Purchase Order** means the authorized document issued by the state agency to the contractor indicating descriptions, quantities, and agreed prices for products and/or services.
- m. **RSMo (Revised Statutes of Missouri)** refers to the body of laws enacted by the Legislature which govern the operations of all agencies of the State of Missouri. Chapter 34 of the statutes is the primary chapter governing the operations of Purchasing.
- n. **Shall** has the same meaning as the word must.
- o. **Should** means that a certain feature, component and/or action is desirable but not mandatory.
- p. **State** collectively referring to the state government and/or the agencies thereof.
- q. **Supplier** has the same meaning as the word, vendor.
- r. **Vendor** means the supplier, offeror, person, or organization that responds to a cooperative contract by submitting a response to the cooperative contract document.

****END OF INTRODUCTION AND BACKGROUND INFORMATION SECTION****

2. SCOPE OF WORK SECTION

2.1 General Requirement:

- 2.1.1 The contractor shall perform Cybersecurity and Information Security Services specified by the State of Missouri, various state agencies throughout Missouri at the firm, fixed prices specified in the attached documentation. All references to NASPO ValuePoint, Idaho, in the attached documentation shall be deemed to refer to the State of Missouri with the exception of information specific to NASPO ValuePoint, Idaho, such as background information, statistical/factual information, etc.
- 2.1.2 The ordering state agency must obtain quotes from all contractors in the same category, and document the state agency's decision regarding the acquisition decision.

SUPPLIERS AWARDED	RISK ASSESSMENT AND MITIGATION SERVICES	INCIDENT RESPONSE SERVICES	BREACH COACH SERVICES	NOTIFICATION AND CREDIT MONITORING
22nd Century Technologies, Inc.	X	X	X	X
Assurit	X	X	X	
Cogent Infotech Group	X			
Gartner	X			
Global Solutions Group	X	X	X	
Identity Teft Guard – IDX				X
Infosys Public Services	X	X	X	
NTT Data	X			
Online Enterprises	X			
Qlogic	X			
Science Systems	X	X		

2.2 State Data:

- 2.2.1 State Data Location: All data associated with the solution/service shall only be hosted, stored, and accessed within the United States.
- Ownership: The state's electronic data or information submitted by the state or its authorized users with authorized access to the solution/service shall be considered "State Data" for ownership purposes of the contract, as the state serves as either the owner or curator of the data submitted in the solution/service. "State Data" shall include: (a) the state's data collected, used, processed, stored, or generated as the result of the Services; (b) personally identifiable information ("PII") collected, used, processed, stored, or generated as the result of the services, including, without limitation, any information that identifies an individual, such as an individual's social security number or other government-issued identification number, date of birth, address, telephone number, biometric data, mother's maiden name, email address, credit card information, or an individual's name in combination with any other of the elements listed herein; and (c) protected health information ("PHI") as that term is defined under the Privacy Rule, 45 Code of Federal Regulations (CFR) §160.103. State data is and shall remain the sole and exclusive property of the state and all right, title, and interest in the same is reserved by the state.
 - "State Data" stored in the software and services being provided as a result of the contract shall also be known and treated by the contractor as confidential information in accordance with the contract, applicable contractor's documentation, and applicable law.
- 2.2.2 Contractor Use of State Data: The contractor shall: (a) keep and maintain state data in strict confidence, using such degree of care as is appropriate and consistent with its obligations as further described in the contract and applicable law to avoid unauthorized access, use, disclosure, or loss; (b) use and disclose state

data solely and exclusively for the purpose of providing the services, such use and disclosure being in accordance with the contract, any applicable Statement of Work, and applicable law; (c) not use, sell, rent, transfer, distribute, or otherwise disclose or make available state data for contractor's own purposes or for the benefit of anyone other than the state without the state's prior written consent; and, (d) not provide state data to any third party without the express written permission of the state. "...for the purpose of providing the services" as referenced above includes the right of the contractor to use state data to prevent or address service or technical problems, and verify service improvements, in accordance with the contract and the solution's documentation, or in accordance with the state's instructions.

- 2.2.3 End of Contract Extraction of State Data: At the end of the contract, the state shall have the right to extract its data from the solution for an additional sixty (60) calendar days from the date of contract expiration. The end of contract extraction of state data must be at no additional cost, conditions, or contingencies regarding the state's right to extract the data notwithstanding the terms outlined in the contractor's services agreement, and in the format that was mutually agreed to by the parties. If a term greater than 60 calendar days is required by the state to complete the state data extraction, the contractor agrees to work with the state to define the additional term and fees for the additional time.
- 2.2.4 Extraction of State Data Process Validation: The contractor must allow the state to perform routine validation of the extraction of the state's data. The routine validation occurs to ensure the state's data will accurately transfer as prescribed to the state's designated extraction location and accommodates the volume of data transferred. The contractor shall assist the state by providing documentation and tools to allow the state to accurately process the extractions of the state's data for the state's continued use.
- 2.2.5 Backup and Recovery of State Data: Unless otherwise described in the contract, as a part of the services, the contractor shall maintain a backup of state data and perform an orderly and timely recovery of such data in the event that the production services may be interrupted in accordance with the disaster recovery and business continuity plans.
- 2.2.6 Return of State-owned Data: The contractor shall return state-owned data to the State of Missouri in a format mutually agreed to by the state and contractor and with a key or crosswalk to the information, where applicable, at no additional cost to the state. The state shall have the right to test the data extract provided by the contractor at a frequency determined by the state.
- 2.2.7 Software Piracy Prohibition: No state or other public funds payable under the contract shall be used for the acquisition, operation, or maintenance of computer software in violation of United States copyright laws or applicable licensing restrictions. The contractor hereby warrants and certifies that the contractor has in place appropriate systems and controls to prevent such improper use of public funds. Under no circumstances in the course of providing products, services, or any other performance of the contractor's duties/obligations to the state shall the contractor directly or indirectly utilize tools, equipment, and/or software programs that are in violation of third parties' legal copyrights. If the state determines that the contractor is in violation of this paragraph, the state may exercise any remedy available at law including without limitation immediate termination of the contract and any remedy consistent with United States copyright laws.

2.3 Cooperative Procurement Program:

- 2.3.1 The contractor shall participate in the State of Missouri's Cooperative Procurement Program. The contractor shall provide the products and/or services as described herein under the terms and conditions, requirements, and specifications of the contract, including prices, to other government entities in accordance with the Technical Services Act (section 67.360, RSMo, which is available on the internet at: <https://revisor.mo.gov/main/OneSection.aspx?section=67.360&bid=2758&hl>). The contractor shall further understand and agree that participation by other governmental entities is discretionary on the part of that governmental entity and the State of Missouri bears no financial responsibility for any payments due the contractor by such governmental entities. The following website identifies the current members of the

Cooperative Procurement Program: <https://purch.oa.mo.gov/media/pdf/cooperative-procurement-program-members-listing>.

2.4 Missouri Statewide Contract Quarterly Administrative Fee:

- 2.4.1 The contractor shall pay a one percent (1%) administrative fee to the State of Missouri which shall apply to all payments received by the contractor for all services provided under the contract. Payment of the one percent administrative fee shall be non-negotiable.
- 2.4.2 The contractor shall pay the administrative fee at the end of each calendar quarter (i.e. March 31, June 30, September 30, December 31). The total administrative fee for a given quarter must equal one percent (1%) of the total payments (minus returns and credits) received by the contractor during the calendar quarter as reported on the contractor's Missouri Statewide Contract Quarterly Administrative Fee Report specified below. The administrative fee must be received by the Division of Purchasing (Purchasing) no later than the 15th calendar day of the month immediately following the end of the calendar quarter, unless the 15th is not a business day in which case the next business day thereafter shall be considered the administrative fee deadline.
- 2.4.3 Payments shall be made using one of the following acceptable payment methods:
 - a. Check: Personal check, company check, cashier's check, or money order made payable to the "Missouri Revolving Information Technology Trust Fund" and sent to the following mailing address: Division of Purchasing, P.O. Box 809, Jefferson City, MO 65102 – 0809 OR Division of Purchasing, 301 West High Street, Room 630, Jefferson City, MO 65101-1517. The contractor's payment by check shall authorize the State of Missouri to process the check electronically. The contractor understands and agrees that any returned check from the contractor may be presented again electronically and may be subject to additional actions and/or handling fees.
 - b. Electronic Payment: Instructions on how to submit payments electronically by automated clearing house (ACH) will be provided upon request by contacting the Division of Purchasing at (573) 751-2387.
- 2.4.4 All payments of the administrative fee shall include the contract number on any check or transmittal document. However, only one contract number must be entered on a check or transmittal document. If submitting an administrative fee payment for more than one contract, then a separate check or electronic payment and associated transmittal document must be submitted by the contractor for each contract.

2.5 Missouri Statewide Contract Quarterly Administrative Fee Report:

- 2.5.1 The contractor shall submit a Missouri Statewide Contract Quarterly Administrative Fee Report to the Division of Purchasing which shall identify the total payments (minus returns and credits) received by the contractor from state agencies, political subdivisions, and universities that were made pursuant to the contract.
- 2.5.2 The contractor shall prepare and submit the Missouri Statewide Contract Quarterly Administrative Fee Report at the end of each calendar quarter (i.e. March 31, June 30, September 30, December 31) for total payments (minus returns and credits) received by the contractor during the calendar quarter. The Missouri Statewide Contract Quarterly Administrative Fee Report must be received by the Division of Purchasing (Purchasing) no later than the 15th calendar day of the month following the reporting quarter entered on the report, unless the 15th is not a business day in which case the next business day thereafter shall be considered the reporting deadline. Even if there has been no usage of the contract during the reporting quarter, the contractor must still submit a report and indicate no payments were received by marking the appropriate box on the report form.

2.5.3 The Missouri Statewide Contract Quarterly Administrative Fee Report form may be downloaded from the following Purchasing website: <http://oa.mo.gov/purchasing/vendor-information>. The Missouri Statewide Contract Quarterly Administrative Fee Report is also included herein as Attachment 3. The Missouri Statewide Contract Quarterly Administrative Fee Report must be submitted using one of the following methods:

- a. Mail: Division of Purchasing,
P.O. Box 809, Jefferson City MO 65102-0809

OR

Division of Purchasing,
301 West High Street, Room 630, Jefferson City, MO 65101-1517

- b. Fax: (573) 526-9815
c. Email: ereports@oa.mo.gov

2.5.4 The contractor shall agree that the Division of Purchasing reserves the right to modify the requested format and content of the Missouri Statewide Contract Quarterly Administrative Fee Report by providing thirty (30) calendar days written notice to the contractor. The contractor shall also agree the Division of Purchasing may unilaterally amend the contract, with thirty (30) calendar days notice to the contractor to change the method of payment of the administrative fee, the timing for submission of the Missouri Statewide Contract Quarterly Administrative Fee Report, and/or timing for payment of the administrative fee. The contractor shall understand and agree that if such an amendment is issued by the Division of Purchasing, the contractor shall comply with all contractual terms, as amended.

2.6 Missouri Statewide Contract Quarterly Usage Report:

2.6.1 The contractor shall submit a Missouri Statewide Contract Quarterly Usage Report to the Division of Purchasing that provides the Data Element information listed below:

Data Element	Description
Contractor Name	Contractor name as it appears on the contract.
Statewide Contract Number	Statewide contract number as listed on the cover page of your contract with the State of Missouri.
Report Contact Name	Name of the person completing the report on behalf of the contractor.
Contact Phone Number	Phone number for the person completing the report.
Contact Email Address	Email address for the person completing the report.
Date Report Submitted	Date the Missouri Statewide Contract Quarterly Usage Report is submitted to the Division of Purchasing.
Reporting Quarter	Quarter for which the contractor is reporting purchases on the contract.
Entity Type	Indicate the type of entity by entering "S" for Missouri state agency, "P" for Missouri political subdivision, "U" for Missouri university, or "O" for political subdivision or state entity from another state.
Customer Name	Customer's name. If the customer has multiple locations, please only use the main entity name.
Product or Service Description	Description of product or service purchased.
Purchase Authorization Number/Identifier	Purchase Authorization Number/Identifier supplied by customer to contractor. Enter PO or other authorization number/identifier. If procurement card used, enter "P-Card".
Contract Line Item Number	Line item number on the contract.

Data Element	Description
Quantity Delivered	Quantity (i.e. excluding returns) of products delivered. Enter a quantity of "1" for a service/project.
Unit Price Charged	Unit Price Charged (i.e. excluding credits) for the product or service purchased.
Extended Price	Quantity Delivered X Unit Price Charged.

- a. The contractor shall prepare and submit the Missouri Statewide Contract Quarterly Usage Report at the end of each calendar quarter (i.e. March 31, June 30, September 30, December 31) for the purchases made under the contract during the calendar quarter. The Missouri Statewide Contract Quarterly Usage Report must be received by the Division of Purchasing no later than the 15th calendar day of the month following the reporting quarter entered on the Missouri Statewide Contract Quarterly Usage Report, unless the 15th is not a business day in which case the next business day thereafter shall be considered the reporting deadline. Even if there has been no usage of the contract during the reporting quarter, the contractor must still submit a report and indicate no purchases were made.
- b. The contractor must submit a Missouri Statewide Contract Quarterly Usage Report electronically either utilizing the “Missouri Statewide Contract Quarterly Usage Report” worksheet included herein in Attachment 4 which is downloadable from <https://purch.oa.mo.gov/vendor-information> or utilizing another format which is Excel-exportable. The contractor must submit the Missouri Statewide Contract Quarterly Usage Report to the following email address: ereports@oa.mo.gov.
- c. The contractor shall agree that the Division of Purchasing reserves the right to modify the requested format and content of the Missouri Statewide Contract Quarterly Usage Report by providing thirty (30) calendar days’ written notice to the contractor. The contractor shall also agree the Division of Purchasing may unilaterally amend the contract, with thirty (30) calendar days’ notice to the contractor to change the timing for submission of the Missouri Statewide Contract Quarterly Usage Report. The contractor shall understand and agree that if such an amendment is issued by the Division of Purchasing, the contractor shall comply with all contractual terms, as amended.

2.7 Electronic Funds Transfer, Invoicing, and Payment Requirements:

- 2.7.1 Electronic Funds Transfer (EFT): The State of Missouri will submit contract payments to the contractor at the remittance address listed in the contractor’s MissouriBUYS (WebProcure/Proactis) vendor registration. However, the contractor understands and agrees the state reserves the right to make contract payments to the contractor through electronic funds transfer (EFT). Therefore, prior to any payments becoming due under the contract, the contractor must verify and update, if applicable, their vendor registration with their current remittance address and ACH-EFT payment information at <https://MissouriBUYS.mo.gov>.
- 2.7.2 Invoicing: The contractor shall submit invoices in accordance with the provisions of the governmental entity’s contract this cooperative contract is established. The contractor shall perform the services prior to invoicing the state agency, unless the governmental entity’s contract this cooperative contract is established allows for payment in advance.
 - a. The contractor shall invoice the state agency on the contractor’s original descriptive business invoice form and submit the invoice to the address on the listed on the purchase order.
 - b. The contractor shall use uniquely identifiable invoice numbers to distinguish an invoice from a previously submitted invoice and shall include on the invoice the remittance address listed in the contractor’s MissouriBUYS (WebProcure/Proactis) vendor registration.
 - c. Each contractor invoice must be on the contractor’s original descriptive business invoice form and must contain a unique invoice number and the remittance address included in the contractor’s MissouriBUYS (WebProcure/Proactis) vendor registration. The invoice number will be listed on the

state's EFT addendum record to enable the contractor to properly apply state payments to invoices. The contractor must comply with all other invoicing requirements stated in the cooperative contract.

- d. The statewide financial management system has been designed to capture certain receipt and payment information. For each purchase order received, an invoice must be submitted that references the purchase order number and should be itemized in accordance with items listed on the purchase order. Failure to comply with this requirement may delay processing of invoices for payment.
- e. The contractor shall not invoice federal or state taxes unless otherwise required under law or regulation.

2.7.3 Payment:

- a. Payments are due upon receipt of a valid invoice, payable in 30 calendar days. All invoices for equipment, supplies, and/or services purchased by the State of Missouri shall be subject to late payment charges as provided in section 34.055, RSMo.
- b. The State of Missouri does not pay state or federal taxes unless otherwise required under law or regulation.
- c. The State of Missouri assumes no obligation for equipment, supplies, and/or services shipped or provided in excess of the quantity ordered. Any unauthorized quantity is subject to the state's rejection and shall be returned at the contractor's expense.
- d. The contractor may obtain detailed information for payments issued for the past 24 months from the State of Missouri's central accounting system (SAM II) on the Vendor Services Portal at <https://www.vendorservices.mo.gov/vendorservices/Portal/Default.aspx>.

******END OF SCOPE OF WORK SECTION******

3. TERMS AND CONDITIONS SECTION

3.1 Applicable Laws and Regulations:

- 3.1.1 The contract shall be construed according to the laws of the State of Missouri. The contractor and the State of Missouri must follow all applicable federal, state, and local laws and regulations that apply to the performance of the contract. To the extent that a provision of the contract is contrary to the Constitution or laws of the State of Missouri or of the United States, the provisions shall be void and unenforceable. However, the balance of the contract shall remain in force between the parties unless terminated by consent of both the contractor and Purchasing.

3.2 Non-Discrimination and Affirmative Action:

- 3.2.1 The contractor must comply with applicable federal and state laws and regulations addressing discrimination in employment.

3.3 Americans with Disabilities Act:

- 3.3.1 In connection with the furnishing of equipment, supplies, and/or services under the contract, the contractor shall comply with all applicable requirements and provisions of the Americans with Disabilities Act (ADA), ADA is 42 U.S.C. section 1201, et seq.

3.4 Anti-Discrimination Against Israel Act Contractor Requirements:

- 3.4.1 If the contractor meets the definition of a company as defined in section 34.600, RSMo, and has ten or more employees, the contractor shall not engage in a boycott of goods or services from the State of Israel; from companies doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel; or from persons or entities doing business in the State of Israel as defined in section 34.600, RSMo.
- 3.4.2 If during the life of the contract, the contractor's business status changes according to section 34.600, RSMo, then the contractor shall comply with, complete, and submit to the Division of Purchasing an updated **Exhibit E, Anti-Discrimination Against Israel Act Certification**.

3.5 Authorized Personnel/E-Verify:

- 3.5.1 For work performed under the contract, the contractor shall only employ personnel authorized to work in the United States in accordance with applicable federal and state laws, including section 285.530, RSMo and Executive Order 07-13. If the contractor employs personnel not authorized to work in the United States, the state shall have the right to cancel the contract immediately without penalty or recourse, and to pursue any other remedies permitted by the contract or by applicable state or federal law.
- 3.5.2 Prior to the performance of any services, a contractor meeting the definition of a business entity in section 285.525, RSMo, shall maintain enrollment and participation in the E-Verify Federal work authorization program with respect to the employees hired after enrollment in the program for work in connection with the contracted services included herein. If the contractor's business status changes during the life of the contract to become a business entity as defined in section 285.525, RSMo, pertaining to section 285.530, RSMo, then the contractor shall enroll and participate in the E-Verify program.
- 3.5.3 The contractor shall only be required to provide the affidavits required in section 285.530.2, RSMo, to the state on an annual basis. <https://purch.oa.mo.gov/vendor-information/affidavit-work-authorization-annual-renewal>

3.6 Business Associate Provisions:

3.6.1 Some of the state agencies and the contractor are both subject to and must comply with provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH) (PL-111-5) and all regulations promulgated pursuant to authority granted therein. The contractor shall abide by a Business Associate Agreement. The state's current Business Associate provisions are contained in Attachment 1. The final form and content of any required business associate agreement shall be mutually agreed upon by the state and the contractor after award.

3.7 Business Registration:

3.7.1 The contractor must meet the requirements for conducting business in the State of Missouri, prior to performance of services under the contract, and for the duration of the contract. The contractor must be registered and maintain good standing with the Secretary of State of the State of Missouri and other regulatory agencies, as may be required by law or regulations. Such business requirements for formation and operation include, but are not limited to, those in Chapters 347-359, RSMo.

3.8 Data Breach:

3.8.1 If a data breach impacting the State of Missouri's data requires the state to comply with section 407.1500, RSMo, the contractor shall assist the state by providing to the state any requested information held by the contractor concerning the breach and the state's data stored in the software and services being provided as a result of the contract.

3.9 Elected or Appointed Officials and Employees:

3.9.1 Elected or appointed officials or employees of the State of Missouri or any political subdivision thereof, serving in an executive or administrative capacity, must comply with sections 105.452 and 105.454, RSMo, regarding conflict of interest.

3.10 Indemnification:

3.10.1 Unless expressly provided by Missouri law to the contrary, pursuant to the Constitution of the State of Missouri, Article III, section 39, subsections 2 and 5, the state shall not indemnify, hold harmless, or agree in advance to defend, any person or entity.

3.11 Legal Proceedings:

3.11.1 For any legal action or other proceedings, per section 27.050 and section 27.060, RSMo, the Missouri Attorney General is given the authority to represent the State of Missouri's interests. The venue for any legal proceeding relating to or arising out of the cooperative contract shall be in circuit court for Cole County, Missouri or the United States District Court for the Western District of Missouri, Central Division.

3.11.2 The contractor and the state agree that if a dispute concerning the contract arises that the parties shall make an attempt to resolve the dispute through informal methods before initiating litigation.

3.11.3 The State of Missouri does not agree to any arbitration. The State of Missouri does not voluntarily agree to the payment of attorneys' fees. The state may, but is not required to, mediate any dispute arising under the contract, and any vendor provisions requiring mediation or dispute resolution processes shall not be binding upon the state.

3.12 Federal Funds Requirements:

3.12.1 The contractor shall understand and agree that the contract may involve the use of federal funds. The contractor shall comply with applicable Federal Funds Requirements, as amended by the federal

government, which may include some or all of the paragraphs contained in Attachment 2 or other requirements identified by the federal government.

3.13 Invoicing and Payment:

- 3.13.1 Invoicing and payments must follow section 33.120, section 34.055, and section 8.960, RSMo. All payments shall be made in arrears, unless the requirements of 1 CSR 10-3.010 allow for advance payment of goods or services.

3.14 Non-Appropriation of Funds:

- 3.14.1 The contractor understands and agrees that funds required to fund the contract must be appropriated by the General Assembly of the State of Missouri for each fiscal year included within the contract period. The contract shall not be binding upon the state for any period in which funds have not been appropriated, have been withheld, or have been restricted, and the state shall not be liable for any costs associated with termination caused by lack of appropriations or authority to spend. This includes, but is not limited to, the provisions of the Mo. Const. Article IV, sections 23, 27, 28 and in sections 33.030 and 33.065, RSMo and 1 CSR 10-3.010 (1)(B).
- 3.14.2 To the extent that federal funding is used for the contract, the contract shall not be binding upon the state for any period in which such funding is reduced, terminated, withheld, restricted, or is frozen or paused.

3.15 Work Outside the United States:

- 3.15.1 Unless work outside the United States is prohibited by the cooperative contract, any work performed outside of the United States for the contract must comply with Executive Order 04-09.

3.16 Open Records:

- 3.16.1 Pursuant to section 610.021, RSMo, the contract and related documents are available for public review.

3.17 Record Access:

- 3.17.1 The contractor shall grant the State Auditor access to records/items as stated in section 29.235, RSMo.

3.18 Taxes:

- 3.18.1 The contractor must timely file and pay all Missouri sales, withholding, corporate and any other required Missouri tax returns and taxes, including interest and additions to tax. No contract shall be awarded to a vendor that does not meet the conditions of section 34.040.7, -

*****END OF TERMS AND CONDITIONS SECTION*****

4. GENERAL CONTRACTUAL REQUIREMENTS SECTION

4.1 Contract Definition:

- 4.1.1 The cooperative contract awarded by the State of Missouri consisting of the following documents with any conflict among the documents being resolved by giving priority to the documents in the order listed below:
- a. The Division of Purchasing's acceptance of the response by "notice of award";
 - b. The terms and conditions sections included herein the cooperative contract document between the State of Missouri and Gartner, Inc;
 - c. The attached Participating Addendum between the State of Missouri and Gartner, Inc;
 - d. The attached contract #MA2025004 signed by the State of Idaho on behalf of NASPO ValuePoint, as amended by contract amendment(s); and
 - e. The attached solicitation #928 issued by the State of Idaho on behalf of NASPO ValuePoint.
- 4.1.2 The contract expresses the complete agreement of the parties and performance shall be governed solely by the specifications and requirements contained therein.
- 4.1.3 The contractor shall agree to furnish the services specified in the contract, at the prices quoted therein.
- 4.1.4 State agencies may sign or "click-through" and accept agreements if required by the contractor in order to receive services; however, all provisions of such agreements that conflict with the contract shall have no force or effect.

4.2 Contract Amendment:

- 4.2.1 All changes to the cooperative contract must be accomplished by a formal contract amendment executed by both the contractor and the Division of Purchasing prior to the effective date of such change. No other means shall be used or construed as an amendment or modification to the contract.

4.3 Contract Period:

- 4.3.1 The original contract period shall be as specified on the cover page and the subsequent Notice of Award of the cooperative contract. The cooperative contract's contract period shall not exceed the term of the governmental entity's contract the cooperative contract was established.

4.4 Termination for Convenience:

- 4.4.1 The Division of Purchasing reserves the right to terminate the contract at any time, for the convenience of the State of Missouri, without penalty or recourse, by giving written notice to the contractor at least thirty (30) calendar days prior to the effective date of such termination. The contractor shall be entitled to receive compensation for services and supplies delivered to and accepted by the State of Missouri pursuant to the contract prior to the effective date of termination. The state shall determine the value of any work in process, but not completed and accepted by the state, based on the work products created and agreed to by both parties.

4.5 Cancellation for Breach of Contract:

- 4.5.1 In the event of material breach of the contractual obligations by the contractor, the Division of Purchasing may cancel the contract. At its sole discretion, the Division of Purchasing may give the contractor an opportunity to cure the breach or to explain how the breach will be cured. As specified by the Division of Purchasing, the actual cure must be completed within no more than ten (10) state business days from notification, or at a minimum the contractor must provide the Division of Purchasing within ten (10) state business days from notification a written plan detailing how the contractor intends to cure the breach.

4.5.2 If the contractor fails to cure the breach or if circumstances demand immediate action, the Division of Purchasing will issue a notice of cancellation terminating the contract immediately. If it is determined the Division of Purchasing improperly cancelled the contract, such cancellation shall be deemed a termination for convenience in accordance with the contract.

4.5.3 The contractor understands and agrees that funds required to fund the contract must be appropriated by the General Assembly of the State of Missouri for each fiscal year included within the contract period. The contract shall not be binding upon the state for any period in which funds have not been appropriated or where the funds are withheld by the governor, and the state shall not be liable for any costs associated with termination caused by lack of appropriations or due to the governor's withholding.

4.6 **Contractor Liability:**

4.6.1 The contractor shall be responsible for any and all personal injury (including death) or property damage as a result of the contractor's negligence involving any equipment or service provided under the terms and conditions, requirements and specifications of the contract. In addition, the contractor assumes the obligation to save the State of Missouri, including its agencies, employees, and assignees, from every expense, liability, or payment arising out of such negligent act.

- a. The contractor also agrees to hold the State of Missouri, including its agencies, employees, and assignees, harmless for any negligent act or omission committed by a person employed by or under the supervision of the contractor under the terms of the contract.
- b. The contractor shall not be responsible for any injury or damage occurring as a result of any negligent act or omission committed by the State of Missouri, including its agencies, employees, and assignees.
- c. Under no circumstances shall the contractor be liable for any of the following: (1) third party claims against the state for losses or damages (other than those listed above); or (2) economic consequential damages (including lost profits or savings) or incidental damages, even if the contractor is informed of their possibility.

4.7 **Insurance:**

4.7.1 The contractor shall understand and agree that the State of Missouri cannot save and hold harmless and/or indemnify the contractor or employees against any liability incurred or arising as a result of any activity of the contractor or any activity of the contractor's employees related to the contractor's performance under the contract. Therefore, the contractor must acquire and maintain adequate liability insurance in the form(s) and amount(s) sufficient to protect the State of Missouri, its agencies, its employees, its clients, and the general public against any such loss, damage and/or expense related to his/her performance under the contract.

4.7.2 In the event any insurance coverage is cancelled, the state agency must be notified at least thirty (30) calendar days prior to such cancellation.

4.8 **Property:**

4.8.1 Notwithstanding the foregoing, the state acknowledges that the contractor, in the normal conduct of its business, may use ideas, skills, techniques, concepts or modifications of concepts developed while serving other customers. The state acknowledges the benefit which may accrue to it and expressly and irrevocably permits the contractor to continue in perpetuity, and without payment of a royalty, this practice of using these ideas, skills, techniques and concepts developed while serving the state, and modifications of such concepts. Nothing in the contract shall be construed to restrain the contractor or its employees, consultants or subcontractors in the use of the techniques and skills of computer operation and programming which may be acquired in the course of performance of any services rendered pursuant to the contract. Nothing

herein shall give the state any ownership rights in any works or innovations created by the contractor prior to the performance of services by the contractor under the contract.

- a. The state understands and agrees that any ancillary software tools, techniques, methodologies, or pre-printed materials or previously or independently created materials and any modifications or derivatives thereof (e.g., project management software tools or training software tools, etc.) developed or acquired by the contractor (“contractor materials”) that may be necessary to perform a particular service required hereunder but not required as a specific deliverable of the contract, shall remain the property of the contractor; however, the contractor shall ensure such contractor materials are being used in accordance with applicable intellectual property rights and copyrights. The contractor grants to the State of Missouri a non-exclusive, fully-paid up license to use any contractor materials contained in a deliverable in connection with its use thereof upon full payment to the contractor.
- b. The contractor shall further agree that no reports, documentation, or material prepared, which contains the state’s proprietary or confidential information, including the program(s) developed as required by the contract, shall be used or marketed by the contractor or released to the public without the prior written consent of the state.

4.8.2 The state shall be the sole owner of all State Data, as defined in paragraph 2.2 of the RFP, that any state user places in the system to utilize the service. The contractor, its employees, and its subcontractors shall not access such state data except as required to provide the service, as described herein. The contractor, its employees and its subcontractors shall be bound by a non-disclosure agreement protecting the state’s data. The state’s data may not be utilized for any purpose or provided to any third party without the express written permission of the state.

4.8.3 The contractor shall use safeguards designed to prevent the inappropriate use or disclosure of the state’s proprietary or confidential information.

4.8.4 In the event of expiration, termination, or cancellation of the contract, after return of state data and state property to the state, all state information and any other property of the state documents must be held by the contractor for at least sixty (60) calendar days at no additional cost to the state, subject to directions of the state as set out herein. The contractor shall not take any action to intentionally destroy any data or digital content from the solution until the data and digital content has been successfully transferred to the state in a format acceptable to the state and the state informs the contractor in writing of such data or digital content that may be permanently destroyed.

- a. After completing successful transfer of the data and digital content, and upon expiration, termination, or cancellation of the services, the contractor shall destroy the data and digital content in its systems or otherwise in its possession or under its control, unless otherwise required by law. Once any requirement by law to retain the state’s information is fulfilled, the contractor shall destroy all data and digital content in all of its forms. The data and digital content shall be permanently destroyed and shall not be recoverable, according to the National Institute of Standards and Technology or other state approved comparable industry standard methods. The contractor shall provide a confirmation of destruction to the state within seven (7) calendar days after receipt of written request from the state. There shall be no cost to the state for permanent destruction of the state’s data and digital content.

4.9 **Inventions, Patents, and Copyrights:**

4.9.1 If any copyrighted material is developed as a result of the contract, the state agency shall have a royalty-free, nonexclusive and irrevocable right to publish or use, and to authorize others to use, the work for state agency purposes or the purpose of the State of Missouri.

4.10 **Confidentiality and Security Documents:**

- 4.10.1 Neither party shall disclose or use any confidential information of the other party, except as reasonably necessary to perform its obligations or to exercise its rights pursuant to the contract or with the other party's prior written permission.
- 4.10.2 If required by the state, the contractor must sign specific documents regarding confidentiality, security, or other similar documents that align with the confidentiality and security terms in the contract upon request, concerning the services provided for in the contract, and are consistent with the terms of the contract. The contractor shall have the opportunity to review, discuss, and approve the documents the contractor must sign prior to signature. The contractor shall ensure that its personnel adhere to the confidentiality and security required by the contract. Failure of the contractor to sign such documents absent a good faith basis may be considered a breach of contract and subject to the cancellation provisions of this document.
- 4.11 Remedies and Rights:**
- 4.11.1 No provision in the contract shall be construed, expressly or implied, as a waiver by the State of Missouri of any existing or future contractual right and/or contractual remedy available by law in the event of any claim by the State of Missouri of the contractor's default or breach of contract.
- 4.11.2 The contractor understands and agrees that the contract shall constitute an assignment by the contractor to the State of Missouri of all rights, title and interest in and to all causes of action that the contractor may have under the antitrust laws of the United States or the State of Missouri for which causes of action have accrued or will accrue as the result of or in relation to the particular equipment, supplies, and/or services purchased or procured by the contractor in the fulfillment of the contract with the State of Missouri.
- 4.11.3 The contractor understands and agrees that the state reserves the right to consider the contractor's failure to perform requirements and commitments specified in the contract in future procurement evaluations.
- 4.12 Survivability of Terms:**
- 4.12.1 The contractual provisions as to definitions, indemnity, warranties, confidentiality, ownership, data, security, liability, insurance, governing law, venue, and remedy shall survive any payment for goods and services, expiration, termination or cancellation of the contract, and shall continue in full force and effect.

****END OF GENERAL CONTRACTUAL REQUIREMENTS SECTION****

5. VENDOR SUBMISSION AND AWARD INFORMATION SECTION

5.1 Preparation of Response:

- 5.1.1 Business Compliance Pre-Work: **Due to lead times for obtaining the information needed to complete the Business Compliance Exhibits explained herein, vendors are encouraged to IMMEDIATELY begin securing these verifications when preparing a response.**
- 5.1.2 Vendor Response Exhibits: The vendor must submit properly completed cooperative contract document's Vendor Response Exhibits as their response. Each exhibit includes instructions outlining the information to be provided in response to the exhibit.

5.2 Compliance with Requirements, Terms and Conditions:

- 5.2.1 If the vendor's response includes any exceptions to the mandatory provisions of the cooperative contract, the vendor must (1) identify the specific cooperative contract paragraph number to which the exception applies along with a description of why the vendor is taking exception to the provision; and (2) any proposed alternative language the vendor would like the state to consider to replace the provision. However, the vendor must understand and agree:
 - a. Exceptions to mandatory provisions of the cooperative contract make the vendor's response non-responsive and ineligible for award. Any exceptions to mandatory provisions must be addressed in order to be eligible for a contract award.

5.3 Confidentiality and Proprietary Materials:

- 5.3.1 Missouri Sunshine Law: The Division of Purchasing is a governmental body under the Missouri Sunshine Law (chapter 610, RSMo). Section 610.011, RSMo, requires that all provisions be "liberally construed and their exceptions strictly construed" to promote the public policy that records are open unless otherwise provided by law.
- 5.3.2 Response Confidentiality: Regardless of any claim by a vendor as to material being proprietary and not subject to copying or distribution, or how a vendor characterizes any information provided in its response, all material submitted by the vendor in conjunction with the cooperative contract is subject to release after the award of a contract in relation to a request for public records under the Missouri Sunshine Law (see Chapter 610, RSMo). Only information expressly permitted to be closed pursuant to the strictly construed provisions of Missouri's Sunshine Law will be treated as a closed record by the Division of Purchasing and withheld from any public request submitted to the Division of Purchasing after award. The vendor should presume information provided to the Division of Purchasing in a response will be public following the award of the contract and made available upon request in accordance with the provisions of state law. Except for information the Division of Purchasing deems confidential, the vendor is advised not to include any information in the response that the vendor does not want to be viewed by the public, including personal identifying information such as social security numbers. Therefore, the **vendor should NOT include confidential material with their response.**
- 5.3.3 Information Not Considered Confidential: In no event will the following be considered confidential or exempt from the Missouri Sunshine Law; however, this is not meant to be an all-inclusive list:
 - a. Vendor's entire response;
 - b. Vendor's pricing;
 - c. Vendor's product specifications unless specifications disclose scientific and technological innovations in which the owner has a proprietary interest (see subsection 15 of section 610.021, RSMo).

5.4 Foreign Vendor:

- 5.4.1 A foreign vendor who do not have an Employer Identification Number assigned by the United States Internal Revenue Service (IRS) must complete the appropriate IRS W-8 form (found on the www.irs.gov website) and must attach this completed and signed form when registering on the MissouriBUYS (<https://missouribuy.mo.gov>) website.
- When submitting a response, if the vendor does not have an IRS Employer Identification Number they should attach a note to the front page of their response advising the Division of Purchasing if: (1) a completed and signed W-8 form is included with the response or (2) a completed and signed W-8 form is attached to their vendor registration profile on the MissouriBUYS website.
 - A foreign vendor that have an IRS Employer Identification Number may register as a vendor on the MissouriBUYS (<https://missouribuy.mo.gov>) website by using the IRS Employer Identification Number assigned to their company and attaching a completed and signed IRS W-9 form to their vendor registration profile. (Note: Attaching a completed and signed IRS W-8 form is not necessary.)

5.5 Business Compliance Requirements:

- 5.5.1 Due to lead times for obtaining the information needed to complete the Business Compliance Exhibits, the vendor is encouraged to IMMEDIATELY begin securing these verifications when preparing a response. In order to be considered a responsible and reliable vendor and therefore be considered eligible for award of a contract, the vendor must be in compliance with the laws regarding conducting business in the State of Missouri and provide the applicable documentation prior to the award of a contract. In order to verify the vendor's compliance, the state will review the vendor's response to the following Business Compliance Exhibits:
- Business Compliance Exhibit B, State of Missouri Tax Compliance** - In accordance with section 34.040.7 RSMo, the vendor must be in tax compliance with the Missouri Department of Revenue. The Missouri Department of Revenue will issue a "Vendor No Tax Due" certificate if the vendor is properly registered to collect and have properly remitted sales and/or use tax, or if the vendor is not making retail sales in Missouri.
 - Business Compliance Exhibit C, Registration of Business Name with the Missouri Secretary of State** - In accordance with section 351.572, RSMo, the vendor must obtain a certification of authority be properly registered with the Missouri Secretary of State or identify how the vendor's business is exempt from registering with the Missouri Secretary of State.
 - Business Compliance Exhibit D, Business Entity Certification, Enrollment Documentation, and Affidavit of Work Authorization** - Pursuant to section 285.530, RSMo, if the vendor meets the section 285.525, RSMo, definition of a "business entity" (<http://www.moga.mo.gov/mostatutes/stathtml/28500005301.html?&me=285.530>), the vendor must affirm the vendor's enrollment and participation in the E-Verify federal work authorization program with respect to the employees hired after enrollment in the program who are proposed to work in connection with the services requested herein. The vendor should complete applicable portions of **Exhibit D, Business Entity Certification, Enrollment Documentation, and Affidavit of Work Authorization**.
 - Business Compliance Exhibit E, Anti-Discrimination Against Israel Act Certification** - Pursuant to section 34.600, RSMo, if the vendor meets the section 34.600, RSMo, definition of a "company" (<https://revisor.mo.gov/main/OneSection.aspx?section=34.600>) and the vendor has ten or more employees, the vendor must certify in writing that the vendor is not currently engaged in a boycott of goods or services from the State of Israel as defined in section 34.600, RSMo, and shall not engage in a boycott of goods or services from the State of Israel, if awarded a contract, for the duration of the contract.

- e. **Business Compliance Exhibit F, Services Outside the United States** - If any services offered under this cooperative contract are being performed at sites outside the United States, the vendor must disclose such fact and provide details with the response.
- f. **Business Compliance Exhibit G, Employee/Conflict of Interest** – Elected or appointed officials or employees of the State of Missouri or any political subdivision serving in an executive or administrative capacity participating in a response to the RFP must disclose their involvement to identify the conflict of interest.
- g. **Business Compliance Exhibit H, Federal Funding Unique Identity ID** - The vendor must not be presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in the contract by any Federal department or agency pursuant to 2 CFR Part 180, or any other applicable law. The vendor should provide its Unique Identity ID number and on the **Exhibit H, Federal Funding Unique Identity ID**.
- h. **General Business Compliance** - The vendor must be in compliance with the laws regarding conducting business in the State of Missouri. The vendor certifies by signing the signature page of this document that the vendor either is presently in compliance with such laws or shall be in compliance with such laws prior to any resulting contract award. Likewise, the successful vendor shall remain in compliance with such laws for the duration of the resulting contract. The vendor shall provide documentation of compliance upon request by the Division of Purchasing. The compliance to conduct business in the state shall include, but not necessarily be limited to:
 - 1) Taxes (e.g., city/county/state/federal)
 - 2) State and local certifications (e.g., professions/occupations/activities)
 - 3) Licenses and permits (e.g., city/county license, sales permits)
 - 4) Insurance (e.g., worker's compensation/unemployment compensation)
- i. The response will be reviewed for business compliance with the laws regarding conducting business in the state of Missouri.

5.6 Award:

- 5.6.1 The cooperative contract will only be eligible for award if the vendor agrees to comply with the requirements identified herein.
- 5.6.2 Any award of a contract shall be made by notification via email from the Division of Purchasing to the vendor. The final contract award shall be made by the Division of Purchasing.
- 5.6.3 After a contract is executed, the response will be uploaded for public viewing into the Division of Purchasing's imaging system known as the Awarded Bid and Contract Document Search system (<https://purch.oa.mo.gov/bidding-contracts/awarded-bid-contract-document-search>).

****END OF VENDOR SUBMISSION AND AWARD INFORMATION SECTION****

EXHIBIT A, RESPONSE SUBMITTAL CHECKLIST

The following table is provided to assist the vendor in completing their response. It is the vendor's sole responsibility to ensure that all mandatory requirements are met and that their response, including all exhibits, are properly completed and submitted with their response. The vendor may want to check the Task Complete boxes to ensure that each of these items are completed and/or submitted with the vendor's response.

No.	Description	Task Complete
1.	Complete and sign the cover page.	☒
3.	Complete Business Compliance Exhibit B, State of Missouri Tax Compliance and attach "Vendor No Tax Due" certificate.	☒
4.	Complete Business Compliance Exhibit C, Registration of Business Name with the Missouri Secretary of State.	☒
5.	Complete and sign Business Compliance Exhibit D, Business Entity Certification, Enrollment Documentation, and Affidavit of Work Authorization (be sure to complete and return the Affidavit of Work Authorization and the vendor's E-Verify Memorandum of Understanding, if required).	☒
6.	Complete and sign Business Compliance Exhibit E, Anti-Discrimination Against Israel Act Certification.	☒
7.	Complete Business Compliance Exhibit F, Services Outside the United States.	☒
8.	Complete Business Compliance Exhibit G, Employee/Conflict of Interest.	☒
9.	Complete Business Compliance Exhibit H, Federal Funding Unique Identity ID.	☒
10.	If applicable, clearly mark, separate, and seal proprietary or confidential information and describe how the proprietary or confidential information meets Chapter 610, RSMo (ref. Section 5 of the cooperative contract).	☐

BUSINESS COMPLIANCE EXHIBITS

Instructions: In order to be awarded a contract, the vendor must be in compliance with the laws regarding conducting business in the State of Missouri.

The vendor certifies by signing the cover page of this document that the vendor either are presently in compliance with such laws or shall be in compliance with such laws prior to any resulting contract award. The vendor shall provide documentation of compliance with the vendor's response and upon request by the Division of Purchasing.

- Business Compliance Exhibit B, State of Missouri Tax Compliance
- Business Compliance Exhibit C, Registration of Business Name with the Missouri Secretary of State
- Business Compliance Exhibit D, Business Entity Certification, Enrollment Documentation, and Affidavit of Work Authorization
- Business Compliance Exhibit E, Anti-Discrimination Against Israel Act Certification
- Business Compliance Exhibit F, Services Outside the United States
- Business Compliance Exhibit G, Employee/Conflict of Interest
- Business Compliance Exhibit H, Federal Funding Unique Identity ID

**BUSINESS COMPLIANCE EXHIBIT B,
STATE OF MISSOURI TAX COMPLIANCE**

STATE OF MISSOURI TAX COMPLIANCE

In accordance with section 34.040.7, RSMo, Purchasing is precluded from contracting with a vendor or its affiliate who makes sales at retail of tangible personal property or for the purpose of storage, use or consumption in this state but fails to collect and properly pay the tax as provided in chapter 144, RSMo.

In order to verify the vendor's State of Missouri tax compliance with the Missouri Department of Revenue (DOR), the vendor must provide "Vendor No Tax Due" certificate issued by DOR prior to award. By providing the "Vendor No Tax Due" certificate, the vendor is verifying the vendor is either registered to collect sales and/or use tax in Missouri or is not making retail sales of tangible personal property or providing taxable services in Missouri.

The DOR will issue the "Vendor No Tax Due" certificate if the vendor is properly registered to collect and have properly remitted sales and/or use tax, or if the vendor is not making retail sales in Missouri.

How To Obtain A Vendor No Tax Due Certificate

A "Vendor No Tax Due" certificate can be obtained from the Missouri Department of Revenue when a business pays all of its sales/use tax in full, up to date, does not have a sales tax delinquency or does not sell tangible personal property at retail in Missouri.

If taxes are due, depending on the payment history of the business, a cashier's check or money order may be required for payment before a "Vendor No Tax Due" certificate can be issued.

A "Vendor No Tax Due" certificate can be obtained by completing and submitting the Request For Tax Clearance, Form 943, to the Missouri Department of Revenue, Division of Taxation & Collection. This form is available at <http://dor.mo.gov/forms/943.pdf>. Make sure to select the appropriate "Reason for Request" on page 2 of the form.

For assistance, call (573) 751-9268 or e-mail taxclearance@dor.mo.gov. Additional information regarding section 34.040.7, RSMo, is available on the Department of Revenue's website at <http://dor.mo.gov/business/sales>.

NOTE: Make sure to request a "Vendor No Tax Due" certificate as there are other similar tax clearance forms that do not meet this verification requirement. The steps to obtain a "Vendor No Tax Due" certificate is outlined at <https://dor.mo.gov/taxation/business/tax-types/sales-use/hb600.html>.

Instructions: The vendor should complete the information below regarding their "Vendor No Tax Due" status.

Please note: Gartner is not registered to remit sales tax. Gartner files both the Vendor's Use Tax Return as well as the Consumer's use tax return. Our MO tax ID is 14957396.

"Vendor No Tax Due" Certificate is Included with the Response (Yes/No)

Yes ☒ No ☐

If the "Vendor No Tax Due" Certificate is Not Included, Identify Date Vendor Requested Certificate From DOR

Date: __/__/____ (MM/DD/YYYY)

**BUSINESS COMPLIANCE EXHIBIT C,
REGISTRATION OF BUSINESS NAME WITH THE MISSOURI SECRETARY OF STATE**

In accordance with section 351.572, RSMo, the vendor must be properly registered with the Missouri Secretary of State or identify how the vendor's business is exempt from registering with the Missouri Secretary of State.

In order to verify the vendor is properly registered with the Missouri Secretary of State, the vendor must either be 1) properly registered with the Missouri Secretary of State at time of response submission or prior to contract award or 2) must identify how the vendor's business is exempt from registering with the Missouri Secretary of State.

NOTE: For any questions regarding Secretary of State Registration, vendors should go to <https://www.sos.mo.gov/business/startBusiness.asp> or call 866-223-6535, Monday through Friday, 8:00 a.m. to 5:00 p.m., Central Time, excluding state holidays.

Missouri Secretary of State Registration Verification

Registration Verification Instructions: If the vendor's business is already registered, the vendor should complete the table below with the vendor's business name and the charter number assigned to the vendor's business.

Information on registering with Missouri Secretary of State: If the vendor's business is not yet properly registered with the Missouri Secretary of State, the vendor should refer to the Missouri Business Portal at <https://openforbiz.mo.gov/> for additional information.

Business Name	Gartner, Inc.	
Charter Number		
Proof of Good Standing Status Included	Yes ☒ No ☐	
If Proof of Good Standing Not Included, Indicate the Date Vendor Requested Document from Missouri Secretary of State	Date: __/__/____ (MM/DD/YYYY)	

Exemptions

Exemption Instructions: If the vendor is exempt from registering with the Missouri Secretary of State pursuant to section 351.572, RSMo, the vendor should identify the specific section of 351.572 RSMo, which supports the exemption by placing a checkmark in the appropriate box in the "Indicate if Exemption is Applicable" column in the table below. In addition, the vendor should provide documentation supporting an exemption, if applicable.

Section 351.572 RSMo Subsection 2. Exemption Description	Indicate if Exemption is Applicable (Check the appropriate box)
(1) Maintaining, Defending, or Settling any Proceeding	☐
(2) Holding Meetings of the Board of Directors or Shareholders or Carrying on Other Activities Concerning Internal Corporate Affairs	☐
(3) Maintaining Bank Accounts	☐
(4) Maintaining Offices or Agencies for the Transfer, Exchange, and Registration of the Corporation's Own Securities or Maintaining Trustees or Depositories with Respect to those Securities	☐
(5) Creating or Acquiring Indebtedness, Mortgages, and Security Interests in Real or Personal Property	☐
(6) Securing or Collecting Debts or Enforcing Mortgages and Security Interests in Property Securing the Debts	☐
(7) Conducting an Isolated Transaction that is Completed Within Thirty Days and that is Not One in the Course of Repeated Transactions of a Like Nature	☐
(8) Transacting Business in Interstate Commerce	☐
Other – Provide Description of Exemption (List of Exemptions Above is Not Exhaustive)	☐

**BUSINESS COMPLIANCE EXHIBIT D,
BUSINESS ENTITY CERTIFICATION, ENROLLMENT DOCUMENTATION, AND AFFIDAVIT OF
WORK AUTHORIZATION**

BUSINESS ENTITY CERTIFICATION:

The vendor must certify their current business status by completing either Box A or Box B or Box C on this Exhibit.

- | | |
|---------------|---|
| BOX A: | To be completed by a non-business entity as defined below. |
| BOX B: | To be completed by a business entity who has not yet completed and submitted documentation pertaining to the federal work authorization program as described at https://www.e-verify.gov/ . |
| BOX C: | To be completed by a business entity who has current work authorization documentation on file with a Missouri state agency including Division of Purchasing. |

Business entity, as defined in section 285.525, RSMo, pertaining to section 285.530, RSMo, is any person or group of persons performing or engaging in any activity, enterprise, profession, or occupation for gain, benefit, advantage, or livelihood. The term “**business entity**” shall include but not be limited to self-employed individuals, partnerships, corporations, and contractors. The term “**business entity**” shall include any business entity that possesses a business permit, license, or tax certificate issued by the state, any business entity that is exempt by law from obtaining such a business permit, and any business entity that is operating unlawfully without such a business permit. The term “**business entity**” shall not include a self-employed individual with no employees or entities utilizing the services of direct sellers as defined in subdivision (17) of subsection 12 of section 288.034, RSMo.

Note: Regarding governmental entities, business entity includes Missouri schools, Missouri universities, out of state agencies, out of state schools, out of state universities, and political subdivisions. A business entity does not include Missouri state agencies and federal government entities.

(Complete Box A if you are a non-business entity as defined above)

BOX A – CURRENTLY NOT A BUSINESS ENTITY

I certify that _____ (Company/Individual Name) **DOES NOT CURRENTLY MEET** the definition of a business entity, as defined in section 285.525, RSMo pertaining to section 285.530, RSMo as stated above, because: (check the applicable business status that applies below)

- ☐- I am a self-employed individual with no employees; **OR**
☐- The company that I represent employs the services of direct sellers as defined in subdivision (17) of subsection 12 of section 288.034, RSMo.

I certify that I am not an alien unlawfully present in the United States and if _____ (Company/Individual Name) is awarded a contract for the services requested herein under this cooperative contract and if the business status changes during the life of the contract to become a business entity as defined in section 285.525, RSMo pertaining to section 285.530, RSMo then, prior to the performance of any services as a business entity, _____ (Company/Individual Name) agrees to complete Box B, comply with the requirements stated in Box B and provide the Division of Purchasing with all documentation required in Box B of this exhibit.

 Authorized Representative's Name
 (Please Print)

 Authorized Representative's Signature

 Company Name (if applicable)

 Date

**BUSINESS COMPLIANCE EXHIBIT D,
BUSINESS ENTITY CERTIFICATION, ENROLLMENT DOCUMENTATION, AND AFFIDAVIT OF
WORK AUTHORIZATION - CONTINUED**

(Complete Box B if you DO NOT have the E-Verify documentation and a current Affidavit of Work Authorization already on file with the State of Missouri. If completing Box B, do not complete Box C.)

BOX B – CURRENT BUSINESS ENTITY STATUS

I certify that _____ (Business Entity Name) **MEETS** the definition of a business entity as defined in section 285.525, RSMo pertaining to section 285.530.

Authorized Business Entity Representative's
Name (Please Print)

*Authorized Business Entity
Representative's Signature*

Business Entity Name

Date

E-Mail Address

As a business entity, the vendor must perform/provide each of the following. The vendor should check each to verify completion/submission of all of the following:

- ☒ - Enroll and participate in the E-Verify federal work authorization program (Website: <https://www.e-verify.gov/>; Phone: 888-464-4218; Email: e-verify@dhs.gov) with respect to the employees hired after enrollment in the program who are proposed to work in connection with the services required herein;
- AND**
- ☒ - Provide documentation affirming said company's/individual's enrollment and participation in the E-Verify federal work authorization program. Documentation shall include EITHER the **E-Verify Employment Eligibility Verification page listing the vendor's name and company ID OR a page from the E-Verify Memorandum of Understanding (MOU) listing the vendor's name and the MOU signature page completed and signed**, at minimum, by the vendor and the Department of Homeland Security – Verification Division. If the signature page of the MOU lists the vendor's name and company ID, then no additional pages of the MOU must be submitted;
- AND**
- ☒ - Submit a **completed, notarized Affidavit of Work Authorization** provided on the next page of this Exhibit.

**BUSINESS COMPLIANCE EXHIBIT D,
BUSINESS ENTITY CERTIFICATION, ENROLLMENT DOCUMENTATION, AND AFFIDAVIT OF
WORK AUTHORIZATION - CONTINUED**

AFFIDAVIT OF WORK AUTHORIZATION:

The vendor who meets the section 285.525, RSMo, definition of a business entity must complete and return the following Affidavit of Work Authorization.

Comes now _____ (Name of Business Entity Authorized Representative) as _____ (Position/Title) first being duly sworn on my oath, affirm _____ (Business Entity Name) is enrolled and will continue to participate in the E-Verify federal work authorization program with respect to employees hired after enrollment in the program who are proposed to work in connection with the services related to contract(s) with the State of Missouri for the duration of the contract(s), if awarded in accordance with subsection 2 of section 285.530, RSMo. I also affirm that _____ (Business Entity Name) does not and will not knowingly employ a person who is an unauthorized alien in connection with the contracted services provided under the contract(s) for the duration of the contract(s), if awarded.

In Affirmation thereof, the facts stated above are true and correct. (The undersigned understands that false statements made in this filing are subject to the penalties provided under section 575.040, RSMo.)

_____ <i>Authorized Representative's Signature</i>	_____ Printed Name
_____ Title	_____ Date
_____ E-Mail Address	_____ E-Verify Company ID Number

Subscribed and sworn to before me this _____ of _____. I am
(DAY) (MONTH, YEAR)
 commissioned as a notary public within the County of _____, State of _____
(NAME OF COUNTY)
 _____, and my commission expires on _____.
(NAME OF STATE) (DATE)

_____ <i>Signature of Notary</i>	_____ Date
-------------------------------------	---------------

**BUSINESS COMPLIANCE EXHIBIT D,
BUSINESS ENTITY CERTIFICATION, ENROLLMENT DOCUMENTATION, AND AFFIDAVIT OF
WORK AUTHORIZATION - CONTINUED**

(Complete Box C if you have the E-Verify documentation and a current Affidavit of Work Authorization already on file with the State of Missouri. If completing Box C, do not complete Box B.)

BOX C – AFFIDAVIT ON FILE - CURRENT BUSINESS ENTITY STATUS

I certify that Gartner, Inc. (Business Entity Name) **MEETS** the definition of a business entity as defined in section 285.525, RSMo pertaining to section 285.530, RSMo and have enrolled and currently participates in the E-Verify federal work authorization program with respect to the employees hired after enrollment in the program who are proposed to work in connection with the services related to contract(s) with the State of Missouri. We have previously provided documentation to a Missouri state agency that affirms enrollment and participation in the E-Verify federal work authorization program. The documentation that was previously provided included the following.

- ✓ The E-Verify Employment Eligibility Verification page **OR** a page from the E-Verify Memorandum of Understanding (MOU) listing the vendor's name and the MOU signature page completed and signed by the vendor and the Department of Homeland Security – Verification Division
- ✓ A **current, notarized Affidavit of Work Authorization** (must be completed, signed, and notarized within the past twelve months).

Name of **Missouri State Agency** to Which Previous E-Verify Documentation Submitted:
State of Missouri

Date of Previous E-Verify Documentation Submission: See attached.

Previous **Bid/Contract Number** for Which Previous E-Verify Documentation Submitted: 1318287 (if known)

David Vixama

Authorized Business Entity Representative's
Name (Please Print)

Gartner, Inc.

Business Entity Name

E-Mail Address

Authorized Business Entity
Representative's Signature

Date

1318287

E-Verify MOU Company ID Number

DocuSigned by:

David Vixama

CCE13228C8BD44B...

July 22, 2026

FOR STATE OF MISSOURI USE ONLY

Documentation Verification Completed By:

Emily Thompson
Buyer

08/27/26
Date

BUSINESS COMPLIANCE EXHIBIT E, ANTI-DISCRIMINATION AGAINST ISRAEL ACT CERTIFICATION

Statutory Requirement: Section 34.600, RSMo, precludes entering into a contract with a company to acquire products and/or services “unless the contract includes a written certification that the company is not currently engaged in and shall not, for the duration of the contract, engage in a boycott of goods or services from the State of Israel; companies doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel; or persons or entities doing business in the State of Israel.”

Exceptions: The statute provides two exceptions for this certification: 1) “contracts with a total potential value of less than one hundred thousand dollars” or 2) “contractors with fewer than ten employees.” Therefore the following certification is required prior to any contract award.

Section 34.600, RSMo, defines the following terms:

Boycott Israel and Boycott of the State of Israel: engaging in refusals to deal, terminating business activities, or other actions to discriminate against, inflict economic harm, or otherwise limit commercial relations specifically with the State of Israel; companies doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel; or persons or entities doing business in the State of Israel, that are all intended to support a boycott of the State of Israel. A company’s statement that it is participating in boycotts of the State of Israel; companies doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel; or persons or entities doing business in the State of Israel, or that it has taken the boycott action at the request, in compliance with, or in furtherance of calls for a boycott of the State of Israel; companies doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel; or persons or entities doing business in the State of Israel shall be considered to be conclusive evidence that a company is participating in a boycott of the State of Israel; companies doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel; or persons or entities doing business in the State of Israel; provided, however that a company that has made no such statement may still be considered to be participating in a boycott of the State of Israel; companies doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel; or persons or entities doing business in the State of Israel if other factors warrant such a conclusion.

Company: any for-profit or not-for-profit organization, association, corporation, partnership, joint venture, limited partnership, limited liability partnership, limited liability company, or other entity or business association, including all wholly-owned subsidiaries, majority-owned subsidiaries, parent companies, or affiliates of those entities or business associations.

Public Entity: the state of Missouri or any political subdivision thereof, including all boards, commissions, agencies, institutions, authorities, and bodies politic and corporate of the state created by or in accordance with state law or regulations.

Certification - The vendor must therefore certify their current status by completing either Box A, Box B, Box C, or Box D on the next page of this Exhibit.

- | | |
|---------------|--|
| BOX A: | To be completed by any vendor that <u>does not meet the definition of “company”</u> above, hereinafter referred to as “Non-Company.” |
| BOX B: | To be completed by a vendor that meets the definition of “Company” but has <u>less than ten employees</u> . |
| BOX C: | To be completed by a vendor that <u>meets the definition of “Company”</u> and <u>has ten or more employees</u> . |
| BOX D: | To be completed by a vendor that meets the definition of a “ <u>Public Entity</u> ”. |

**BUSINESS COMPLIANCE EXHIBIT E,
ANTI-DISCRIMINATION AGAINST ISRAEL ACT CERTIFICATION - CONTINUED**

BOX A – NON-COMPANY ENTITY

I certify that N/A (Entity Name) currently **DOES NOT MEET** the definition of a company as defined in section 34.600, RSMo, but that if awarded a contract and the entity's business status changes during the life of the contract to become a "company" as defined in section 34.600, RSMo, and the entity has ten or more employees, then, prior to the delivery of any services and/or supplies as a company, the entity agrees to comply with, complete, and return Box C to the Division of Purchasing at that time.

Authorized Representative's Name (Please Print)

Authorized Representative's Signature

Entity Name

Date

BOX B – COMPANY ENTITY WITH LESS THAN TEN EMPLOYEES

I certify that N/A (Company Name) **MEETS** the definition of a company as defined in section 34.600, RSMo, and currently has less than ten employees but that if awarded a contract and if the company increases the number of employees to ten or more during the life of the contract, then said company shall comply with, complete, and return Box C to the Division of Purchasing at that time.

Authorized Representative's Name (Please Print)

Authorized Representative's Signature

Company Name

Date

BOX C – COMPANY ENTITY WITH TEN OR MORE EMPLOYEES

I certify that Gartner, Inc. (Company Name) **MEETS** the definition of a company as defined in section 34.600, RSMo, has ten or more employees, and is not currently engaged in a boycott of goods or services from the State of Israel; companies doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel; or persons or entities doing business in the State of Israel as defined in section 34.600, RSMo. I further certify that if the company is awarded a contract for the services and/or supplies requested herein said company shall not engage in a boycott of goods or services from the State of Israel; companies doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel; or persons or entities doing business in the State of Israel as defined in section 34.600, RSMo, for the duration of the contract.

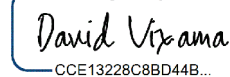
David Vixama

Authorized Representative's Name (Please Print)

Gartner, Inc.

Company Name

DocuSigned by:


CCE13228C8BD44B...

Authorized Representative's Signature

July 22, 2026

Date

**BUSINESS COMPLIANCE EXHIBIT E,
ANTI-DISCRIMINATION AGAINST ISRAEL ACT CERTIFICATION - CONTINUED**

BOX D – PUBLIC ENTITY

I certify that Gartner, Inc. (Entity Name) is a public entity as defined in section 34.600, RSMo, and is not currently engaged in and shall not, for the duration of the contract, engage in a boycott of goods or services from the State of Israel; companies doing business in or with Israel or authorized by, licensed by, or organized under the laws of the State of Israel; or persons or entities doing business in the State of Israel.

Gartner, Inc.

DocuSigned by:

David Vixama
CCE13228C8BD44B...

Authorized Representative's Name (Please Print)

Authorized Representative's Signature

David Vixama

July 22, 2026

Company Name

Date

**BUSINESS COMPLIANCE EXHIBIT F,
SERVICES OUTSIDE THE UNITED STATES**

Pursuant to [Executive Order 04-09](#) subparagraph 4, no state agency shall award a contract to a vendor who contemplates performing work pursuant to the contract at a site outside of the United States, unless one of the exceptions identified below are met. This document must be satisfactorily completed prior to an award of a contract.

Therefore, the vendor must disclose whether services proposed would be performed at a location outside of the United States and provide details in the space below or on an attached page. If vendor does not complete the table below, the vendor is committing to complete all work in the United States for the duration of the contract.

Will any of the services proposed by the vendor be performed at sites outside the United States? If the answer is "yes", then provide the information below. If the answer is "no", then the vendor does not need to complete the rest of this exhibit.	Yes ☐	No ☒
Identify the name of the vendor that would be performing services at a site outside the United States.	N/A	
Describe the services proposed to be performed at sites outside the United States.	N/A	
Identify where the services would be performed at sites outside the United States.	N/A	
Identify when (specific timeframe) in the life of the contract the services would be performed at sites outside the United States.	N/A	
Identify why the services need to be performed at sites outside the United States.	N/A	
Identify whether the proposed services meet at least one of the conditions described in section 4, subparagraphs a, b, c, and d of Executive Order 04-09 and how the exception(s) is met. If the answer is "yes" and exemption applies, then provide the information below.	Yes ☐	No ☐
Mark the appropriate exemption below, and provide the requested details: (a) ☐ Unique good or service that is deemed mandatory pursuant to the requirements herein and has no comparable domestically-provided good or service that can adequately duplicate the unique features provided by the vendor. - EXPLAIN HOW THE GOOD OR SERVICE IS UNIQUE: _____ (b) ☐ Foreign firm hired to market Missouri services/products to a foreign country. - IDENTIFY THE APPLICABLE PARAGRAPHS HEREIN: _____ (c) ☐ A significant or substantial economic cost factor exists that outweighs the economic impact of providing the function or professional services within the United States, and such failure in using the vendor's services would result in economic hardship to the state. - EXPLAIN HOW: _____ (d) ☐ Vendor maintains significant business presence in the United States and only performs trivial portion of contract work outside US. - IDENTIFY MAXIMUM PERCENTAGE of the overall value of the contract, for any contract period, attributed to the value of the services being performed at sites outside the United States identified above: _____ %		

**BUSINESS COMPLIANCE EXHIBIT G,
EMPLOYEE/CONFLICT OF INTEREST**

Vendors who are elected or appointed officials or employees of the State of Missouri or any political subdivision thereof, serving in an executive or administrative capacity, must comply with sections 105.450 to 105.458, RSMo, regarding conflict of interest. If the vendor or any owner of the vendor's organization is currently an elected or appointed official or an employee of the State of Missouri or any political subdivision thereof, please provide the following information. The information must be provided prior to the award of a contract.

Name and title of elected or appointed official or employee of the State of Missouri or any political subdivision thereof:	N/A
If employee of the State of Missouri or political subdivision thereof, provide name of state agency or political subdivision where employed:	N/A
Percentage of ownership interest in vendor's organization held by elected or appointed official or employee of the State of Missouri or political subdivision thereof:	___ N/A _____%

**BUSINESS COMPLIANCE EXHIBIT H,
FEDERAL FUNDING UNIQUE IDENTITY ID**

Federal Debarment: The vendor must not be presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in the contract by any Federal department or agency pursuant to 2 CFR Part 180, or any other applicable law. The vendor should provide its Unique Identity ID number on the table below:

Unique Entity ID: The Unique Entity ID is the official identifier for doing business with the US Government. Vendors should register at <https://sam.gov/content/home> to be assigned a Unique Entity ID. In the table below, identify the Unique Identity ID number and, if applicable, the Parent Organization's Unique Identity ID Number. The Parent Organization's Unique Identity ID number is typically used by large organizations with multiple facilities in several locations. The parent organization's number is the number assigned to the headquarters for the operation.

Vendor Name: Gartner, Inc.	Vendor's Unique Identity ID Number: CFALLJBGZ697
Parent Organization's Name: N/A	Parent Organizations Unique Identity ID Number: N/A

(Health Insurance Portability and Accountability Act of 1996, as amended)

1. Health Insurance Portability and Accountability Act of 1996, as amended - The Department and the contractor are both subject to and must comply with provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH) (PL-111-5) (collectively, and hereinafter, HIPAA) and all regulations promulgated pursuant to authority granted therein. The contractor constitutes a “Business Associate” of the Department. Therefore, the term, “contractor” as used in this section shall mean “Business Associate” and “Department” as used in this section shall mean “covered entity.”
2. The contractor agrees that for purposes of the Business Associate Agreement contained herein, terms used but not otherwise defined shall have the same meaning as those terms defined in 45 CFR Parts 160 and 164 and 42 U.S.C. §§ 17921 *et. seq.* including, but not limited to the following:
 - a. “Access”, “administrative safeguards”, “confidentiality”, “covered entity”, “data aggregation”, “designated record set”, “disclosure”, “hybrid entity”, “information system”, “physical safeguards”, “required by law”, “technical safeguards”, “use” and “workforce” shall have the same meanings as defined in 45 CFR 160.103, 164.103, 164.304, and 164.501 and HIPAA.
 - b. “Breach” shall mean the unauthorized acquisition, access, use, or disclosure of Protected Health Information which compromises the security or privacy of such information, except as provided in 42 U.S.C. § 17921. This definition shall not apply to the term “breach of contract” as used within the contract.
 - c. “Business Associate” shall generally have the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean the contractor.
 - d. “Covered Entity” shall generally have the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this agreement, shall mean the Department.
 - e. “Electronic Protected Health Information” shall mean information that comes within paragraphs (1)(i) or (1)(ii) of the definition of Protected Health Information as specified below.
 - f. “Enforcement Rule” shall mean the HIPAA Administrative Simplification: Enforcement; Final Rule at 45 CFR Parts 160 and 164.
 - g. “Health Care” as defined in 45 CFR §160.103, shall mean care, services, or supplies related to the health of an individual. Health care includes but is not limited to, the following:
 - 1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
 - 2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.
 - h. “HIPAA Rules” shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.
 - i. “Individual” shall have the same meaning as the term “individual” in 45 CFR 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502 (g).
 - j. “Privacy Rule” shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.
 - k. “Protected Health Information” as defined in 45 CFR 160.103, shall mean individually identifiable health information:
 - 1) Except as provided in paragraph (2) of this definition, that is: (i) Transmitted by electronic media; or (ii) Maintained in electronic media; or (iii) Transmitted or maintained in any other form or medium.
 - 2) Protected Health Information excludes individually identifiable health information in (i) Education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g; (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv); and (iii) Employment records held by a covered entity (Department) in its role as employer
 - l. “Security Incident” shall be defined as set forth in the “Obligations of the Contractor” section of the Business Associate Agreement.

- m. "Security Rule" shall mean the Security Standards for the Protection of Electronic Protected Health Information at 45 CFR Part 164, Subpart C.
 - n. "Unsecured Protected Health Information" shall mean Protected Health Information that is not secured through the use of a technology or methodology determined in accordance with 42 U.S.C. § 17932 or as otherwise specified by the secretary of Health and Human Services.
3. The contractor agrees and understands that wherever in this document the term "Protected Health Information" is used, it shall also be deemed to include Electronic Protected Health Information.
4. The contractor must appropriately safeguard Protected Health Information which the contractor receives from or creates or receives on behalf of the Department. To provide reasonable assurance of appropriate safeguards, the contractor shall comply with the business associate provisions stated herein, as well as the provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH) (PL-111-5) and all regulations promulgated pursuant to authority granted therein.
5. The Department and the contractor agree to amend the contract as is necessary for the parties to comply with the requirements of HIPAA and the Privacy Rule, Security Rule, Enforcement Rule, and other rules as later promulgated (hereinafter referenced as the regulations promulgated thereunder). Any ambiguity in the contract shall be interpreted to permit compliance with the HIPAA Rules.
6. **Permitted Uses and Disclosures of Protected Health Information by the Contractor**
- 6.1 The contractor may not use or disclose Protected Health Information in any manner that would violate Subpart E of 45 CFR Part 164 if done by the Department, except for the specific uses and disclosures in the contract.
- 6.2 The contractor may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, the Department as specified in the contract, provided that such use or disclosure would not violate HIPAA and the regulations promulgated thereunder.
- 6.3 The contractor may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1) and shall notify the Department by no later than ten (10) calendar days after the contractor becomes aware of the disclosure of the Protected Health Information.
- 6.4 If required to properly perform the contract and subject to the terms of the contract, the contractor may use or disclose Protected Health Information if necessary for the proper management and administration of the contractor's business.
- 6.5 If the disclosure is required by law, the contractor may disclose Protected Health Information to carry out the legal responsibilities of the contractor.
- 6.6 If applicable, the contractor may use Protected Health Information to provide Data Aggregation services to the Department as permitted by 45 CFR 164.504(e)(2)(i)(B).
- 6.7 The contractor may not use Protected Health Information to de-identify or re-identify the information in accordance with 45 CFR 164.514(a)-(c) without specific written permission from the Department to do so.
- 6.8 The contractor agrees to make uses and disclosures and requests for Protected Health Information consistent with the Department's minimum necessary policies and procedures.
7. **Obligations and Activities of the Contractor**
- 7.1 The contractor shall not use or disclose Protected Health Information other than as permitted or required by the contract or as otherwise required by law, and shall comply with the minimum necessary disclosure requirements set forth in 45 CFR § 164.502(b).
- 7.2 The contractor shall use appropriate administrative, physical and technical safeguards and comply with Subpart C of 45 CFR Part 164 to prevent use or disclosure of the Protected Health Information other than as provided for by the contract. Such safeguards shall include, but not be limited to:
- a. Workforce training on the appropriate uses and disclosures of Protected Health Information pursuant to the terms of the contract;
 - b. Policies and procedures implemented by the contractor to prevent inappropriate uses and disclosures of Protected Health Information by its workforce and subcontractors, if applicable;
 - c. Encryption of any portable device used to access or maintain Protected Health Information or use of equivalent safeguard;

- d. Encryption of any transmission of electronic communication containing Protected Health Information or use of equivalent safeguard; and
 - e. Any other safeguards necessary to prevent the inappropriate use or disclosure of Protected Health Information.
- 7.3 With respect to Electronic Protected Health Information, the contractor shall use appropriate administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Electronic Protected Health Information that contractor creates, receives, maintains or transmits on behalf of the Department and comply with Subpart C of 45 CFR Part 164, to prevent use or disclosure of Protected Health Information other than as provided for by the contract.
- 7.4 In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), the contractor shall require that any agent or subcontractor that creates, receives, maintains, or transmits Protected Health Information on behalf of the contractor agrees to the same restrictions, conditions, and requirements that apply to the contractor with respect to such information.
- 7.5 By no later than ten (10) calendar days after receipt of a written request from the Department, or as otherwise required by state or federal law or regulation, or by another time as may be agreed upon in writing by the Department, the contractor shall make the contractor's internal practices, books, and records, including policies and procedures and Protected Health Information, relating to the use and disclosure of Protected Health Information received from, created by, or received by the contractor on behalf of the Department available to the Department and/or to the Secretary of the Department of Health and Human Services or designee for purposes of determining compliance with the HIPAA Rules and the contract.
- 7.6 The contractor shall document any disclosures and information related to such disclosures of Protected Health Information as would be required for the Department to respond to a request by an individual for an accounting of disclosures of Protected Health Information in accordance with 42 USCA §17932 and 45 CFR 164.528. By no later than five (5) calendar days of receipt of a written request from the Department, or as otherwise required by state or federal law or regulation, or by another time as may be agreed upon in writing by the Department, the contractor shall provide an accounting of disclosures of Protected Health Information regarding an individual to the Department. If requested by the Department or the individual, the contractor shall provide an accounting of disclosures directly to the individual. The contractor shall maintain a record of any accounting made directly to an individual at the individual's request and shall provide such record to the Department upon request.
- 7.7 In order to meet the requirements under 45 CFR 164.524, regarding an individual's right of access, the contractor shall, within five (5) calendar days following a Department request, or as otherwise required by state or federal law or regulation, or by another time as may be agreed upon in writing by the Department, provide the Department access to the Protected Health Information in an individual's designated record set. However, if requested by the Department, the contractor shall provide access to the Protected Health Information in a designated record set directly to the individual for whom such information relates.
- 7.8 At the direction of the Department, the contractor shall promptly make any amendment(s) to Protected Health Information in a Designated Record Set pursuant to 45 CFR 164.526.
- 7.9 The contractor shall report to the Department's Security Officer any security incident immediately upon becoming aware of such incident and shall take immediate action to stop the continuation of any such incident. For purposes of this paragraph, security incident shall mean the attempted or successful unauthorized access, use, modification or destruction of information or interference with systems operations in an information system. This does not include trivial incidents that occur on a daily basis, such as scans, "pings," or unsuccessful attempts that do not penetrate computer networks or servers or result in interference with system operations. By no later than five (5) calendar days after the contractor becomes aware of such incident, the contractor shall provide the Department's Security Officer with a description of any remedial action taken to mitigate any harmful effect of such incident and a proposed written plan of action for approval that describes plans for preventing any such future security incidents.
- 7.10 The contractor shall report to the Department's Privacy Officer any unauthorized use or disclosure of Protected Health Information not permitted or required as stated herein immediately upon becoming aware of such use or disclosure and shall take immediate action to stop the unauthorized use or disclosure. By no later than five (5) calendar days after the contractor becomes aware of any such use or disclosure, the contractor shall provide the Department's Privacy Officer with a written description of any remedial action taken to mitigate any harmful effect of such disclosure and a proposed written plan of action for approval that describes plans for preventing any such future unauthorized uses or disclosures.

- 7.11 The contractor shall report to the Department's Security Officer any breach immediately upon becoming aware of such incident and shall take immediate action to stop the continuation of any such incident. By no later than five (5) calendar days after the contractor becomes aware of such incident, the contractor shall provide the Department's Security Officer with a description of the breach, the information compromised by the breach, and any remedial action taken to mitigate any harmful effect of such incident and a proposed written plan for approval that describes plans for preventing any such future incidents.
- 7.12 The contractor's reports required in the preceding paragraphs shall include the following information regarding the security incident, improper disclosure/use, or breach, (hereinafter "incident"):
- a. The name, address, and telephone number of each individual whose information was involved if such information is maintained by the contractor;
 - b. The electronic address of any individual who has specified a preference of contact by electronic mail;
 - c. A brief description of what happened, including the date(s) of the incident and the date(s) of the discovery of the incident;
 - d. A description of the types of Protected Health Information involved in the incident (such as full name, Social Security Number, date of birth, home address, account number, or disability code) and whether the incident involved Unsecured Protected Health Information; and
 - e. The recommended steps individuals should take to protect themselves from potential harm resulting from the incident.
- 7.13 Notwithstanding any provisions of the Terms and Conditions attached hereto, in order to meet the requirements under HIPAA and the regulations promulgated thereunder, the contractor shall keep and retain adequate, accurate, and complete records of the documentation required under this agreement for a minimum of six (6) years as specified in 45 CFR Part 164.
- 7.14 The contractor shall not directly or indirectly receive remuneration in exchange for any Protected Health Information without a valid authorization.
- 7.15 If the contractor becomes aware of a pattern of activity or practice of the Department that constitutes a material breach of contract regarding the Department's obligations under the Business Associate Agreement of the contract, the contractor shall notify the Department's Security Officer of the activity or practice and work with the Department to correct the breach of contract.
- 7.16 The contractor shall indemnify the Department from any liability resulting from any violation of the Privacy Rule or Security Rule or Breach arising from the conduct or omission of the contractor or its employee(s), agent(s) or subcontractor(s). The contractor shall reimburse the Department for any and all actual and direct costs and/or losses, including those incurred under the civil penalties implemented by legal requirements, including but not limited to HIPAA as amended by the Health Information Technology for Economic and Clinical Health Act, and including reasonable attorney's fees, which may be imposed upon the Department under legal requirements, including but not limited to HIPAA's Administrative Simplification Rules, arising from or in connection with the contractor's negligent or wrongful actions or inactions or violations of this agreement.
8. **Obligations of the Department**
- 8.1 The Department shall notify the contractor of limitation(s) that may affect the contractor's use or disclosure of Protected Health Information, by providing the contractor with the Department's notice of privacy practices in accordance with 45 CFR 164.520.
- 8.2 The Department shall notify the contractor of any changes in, or revocation of, authorization by an Individual to use or disclose Protected Health Information.
- 8.3 The Department shall notify the contractor of any restriction to the use or disclosure of Protected Health Information that the Department has agreed to in accordance with 45 CFR 164.522.
- 8.4 The Department shall not request the contractor to use or disclose Protected Health Information in any manner that would not be permissible under HIPAA and the regulations promulgated thereunder.
9. **Expiration/Termination/Cancellation:** Except as provided in the subparagraph below, upon the expiration, termination, or cancellation of the contract for any reason, the contractor shall, at the discretion of the Department, either return to the Department or destroy all Protected Health Information received by the contractor from the Department, or created or received by the contractor on behalf of the Department, and shall not retain any copies of such Protected Health Information. This provision shall also apply to Protected Health Information that is in the possession of subcontractor or agents of the contractor.
- a. In the event the Department determines that returning or destroying the Protected Health Information is not feasible, the contractor shall extend the protections of the contract to the Protected Health Information for as long as the contractor

maintains the Protected Health Information and shall limit the use and disclosure of the Protected Health Information to those purposes that made return or destruction of the information infeasible. If at any time it becomes feasible to return or destroy any such Protected Health Information maintained pursuant to this paragraph, the contractor must notify the Department and obtain instructions from the Department for either the return or destruction of the Protected Health Information.

10. **Breach of Contract:** In the event the contractor is in breach of contract with regard to the business associate provisions included herein, the contractor agrees that in addition to the requirements of the contract related to cancellation of contract, if the Department determines that cancellation of the contract is not feasible, the State of Missouri may elect not to cancel the contract, but the Department shall report the breach of contract to the Secretary of the Department of Health and Human Services.

ATTACHMENT 2: FEDERAL FUNDS REQUIREMENTS

1.1 Federal Fund Requirements:

The contractor shall understand and agree that the contract involves the use of federal funds. Upon award of the contract, the state agency will provide the contractor the federal fund information. In the event the federal fund information changes, the contractor will be notified in writing by the state agency.

- 1.1.1 Federal Debarment and Suspension (Executive Orders 12549 and 12689) - The contractor certifies by signing the front page of this document that neither it nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in the contract by any Federal department or agency pursuant to 2 CFR Part 180, or any other applicable law.
- 1.1.2 Applicable Laws and Regulations and Public Policy Requirements - In performing its responsibilities under the contract, the contractor shall fully comply with the Office of Management and Budget (OMB) Uniform Administrative Requirements, Cost Principles, and Audit Requirements for Federal Awards (2 CFR, Chapter 1, Chapter, II, Part 200, et al.), as applicable, including any subsequent amendments.
 - a. The contractor shall comply with all applicable implementing regulations, and all other laws, regulations and policies authorizing or governing the use of any federal funds paid to the contractor through the contract. The contractor shall ensure compliance with U.S. statutory and public policy requirements, including but not limited to, those protecting public welfare, the environment, and prohibiting discrimination.
- 1.1.3 Stevens Amendment - The contractor shall not issue any statements, press releases, requests for proposals, bid solicitations, and other documents describing projects or programs funded in whole or in part with Federal funds without the prior approval of the state agency, and the contractor shall clearly state the following:
 - a. The percentage of the total costs of the program or project that will be financed with federal money;
 - b. The dollar amount of federal funds for the project or program; and
 - c. The percentage and dollar amount of the total costs of the project or program that will be financed by nongovernmental sources.
- 1.1.4 Publicity - Any publicity releases and publications mentioning contract activities shall reference the contract number and the state agency. The contractor shall obtain approval from the state agency prior to the release of such publicity release or publications.
- 1.1.5 Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts, and Cooperative Agreements - The contractor shall comply with 37 CFR part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts, and Cooperative Agreements" and any implementing regulations, as applicable.
- 1.1.6 Byrd Anti-Lobbying Amendment (31 U.S.C. 1352), Certification Regarding Lobbying - The contractor shall comply with all requirements of 31 U.S.C. 1352 that is incorporated herein as if fully set forth.
 - a. The contractor certifies by signing the first page of the document that no federal appropriated funds have been paid or will be paid, by or on behalf of the contractor, to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, or the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.
 - b. The contractor certifies that no funds under the contract shall be used to pay for any activity to support or defeat the enactment of legislation before the Congress, or any State or local legislature or legislative body. The contractor shall not use any funds under the contract to pay for any activity to support or defeat any proposed or pending regulation, administrative action, or order issued by the executive branch of any State or local government.
 - c. The contractor certifies that no funds under the contract shall be used to pay the salary or expenses of the contractor, or an agent acting for the contractor who engages in any activity designed to influence the

enactment of legislation or appropriations proposed, or pending before the Congress, or any State, local legislature or legislative body, or any regulation, administrative action, or Executive Order issued by the executive branch of any State or local government.

- d. The above prohibitions include any activity to advocate or promote any proposed, pending, or future Federal, State or local tax increase, or any proposed, pending, or future requirement or restriction on any legal consumer product, including its sale or marketing, including but not limited to the advocacy or promotion of gun control.
- e. If any funds other than federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a member of Congress, an officer or employee of Congress, or an employee of a member of Congress in connection with any Federal contract, grant, loan, or cooperative agreement, the contractor shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying" in accordance with its instructions.
 - 1) The contractor shall require that the language of this section be included in the award documents for all subawards at all levels (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly.
 - Each tier must also disclose any lobbying with non-federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-federal award.
 - 2) This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by 31 U.S.C. § 1352. Any person who fails to file the required certification shall be subject to a civil penalty of not less than \$10,000.00 and not more than \$100,000.00 for each such failure.

1.1.7 Drug Free Workplace Act - The contractor shall provide a drug free workplace in accordance with the Drug Free Workplace Act of 1988, 41 U.S.C. Chapter 81, and all applicable regulations. The contractor shall report any conviction of the contractor's personnel under a criminal drug statute for violations occurring on the contractor's premises or off the contractor's premises while conducting official business. A report of a conviction shall be made to the state agency within five (5) working days after the conviction.

1.1.8 Pro-Children Act - The contractor shall comply with the Pro-Children Act of 1994 (20 U.S.C. 6081).

- a. The Pro-Children Act of 1994, (Public Law 103-227, 20 U.S.C. §§ 6081-6084), requires that smoking not be permitted in any portion of any indoor facility owned or leased or contracted for by an entity and used routinely or regularly for the provision of health, day care, early childhood development services, education, or library services to children under the age of 18, if the services are funded by Federal programs either directly or through State or local governments, by general grant, contract, loan, or loan guarantee. The Pro-Children Act also applies to children's services that are provided in indoor facilities that are constructed, operated, or maintained with such federal funds.
 - 1) The Pro-Children Act does not apply to children's services provided in private residences; portions of facilities used for inpatient drug or alcohol treatment; service providers whose sole source of applicable federal funds is Medicare or Medicaid; or facilities where WIC coupons are redeemed.
- b. The contractor certifies that it will comply with the requirements of the Pro-Children Act and will not allow smoking within any portion of any indoor facility used for the provision of services for children as defined by the Pro-Children Act.
- c. The contractor shall require the language of this certification be included in any subcontract or subaward that contains provisions for children's services and that all subrecipients shall certify accordingly.
- d. Failure to comply with the provisions of the Pro-Children Act may result in the imposition of a civil monetary penalty of up to \$1,000.00 for each violation and/or the imposition of an administrative compliance order on the responsible entity.

1.1.9 Contractor Whistleblower Protections:

- a. The contractor shall comply with the provisions of 41 U.S.C. 4712 that states an employee of a contractor, subcontractor, grantee, or subgrantee may not be discharged, demoted, or otherwise discriminated against as a reprisal for “whistleblowing”. In addition, whistleblower protections cannot be waived by any agreement, policy, form, or condition of employment.
- b. The contractor’s employees are encouraged to report fraud, waste, and abuse. The contractor shall inform their employees in writing they are subject to federal whistleblower rights and remedies. This notification must be in the predominant native language of the workforce.
- c. The contractor shall include this requirement in any agreement made with a subcontractor or subgrantee.

1.1.10 Human Rights and Affirmative Action:

- a. The contractor shall comply with all federal and state statutes, regulations, and executive orders relating to nondiscrimination and equal employment opportunity to the extent applicable to the contract. These include but are not limited to the following:
 - 1) Title VI of the Civil Rights Act of 1964 (P.L. 88-352) that prohibits discrimination on the basis of race, color, or national origin (this includes individuals with limited English proficiency) in programs and activities receiving federal financial assistance and Title VII of the Act that prohibits discrimination on the basis of race, color, national origin, sex, or religion in all employment activities;
 - 2) Equal Pay Act of 1963 (P.L. 88-38, as amended, 29 U.S.C. Section 206(d));
 - 3) Title IX of the Education Amendments of 1972, as amended (20 U.S.C 1681-1683 and 1685-1686) that prohibits discrimination on the basis of sex;
 - 4) Section 504 of the Rehabilitation Act of 1973, as amended (29 U.S.C. 794), the Americans with Disabilities Act of 1990 (42 U.S.C. 12101 et seq.), and Americans with Disabilities Act Amendments Act of 2008 (Public Law 110-325, “ADAAA”) which prohibit discrimination on the basis of disabilities;
 - 5) The Age Discrimination Act of 1975, as amended (42 U.S.C. 6101-6107) that prohibits discrimination on the basis of age;
 - 6) Equal Employment Opportunity – E.O. 11246, “Equal Employment Opportunity”, as amended by E.O. 11375, “Amending Executive Order 11246 Relating to Equal Employment Opportunity”;
 - 7) Genetic Information Non-Discrimination Act (GINA)
 - 8) Missouri State Regulation, 19 CSR 10-2.010, Civil Rights Compliance Requirements;
 - 9) Missouri Governor’s E.O. #94-03 (excluding article II due to its repeal);
 - 10) Missouri Governor’s E.O. #10-24; and
 - 11) The requirements of any other nondiscrimination federal and state statutes, regulations, and executive orders that may apply to the services provided via the contract.
- b. In connection with the furnishing of equipment, supplies, and/or services under the contract, the contractor and all subcontractors shall agree not to discriminate against recipients of services or employees or applicants for employment on the basis of race, color, religion, national origin, sex, age, disability, or veteran status unless otherwise provided by law. If the contractor or subcontractor employs at least 50 persons, the contractor shall have and maintain an affirmative action program that shall include:
 - 1) A written policy statement committing the organization to affirmative action and assigning management responsibilities and procedures for evaluation and dissemination;
 - 2) The identification of a person designated to handle affirmative action;
 - 3) The establishment of non-discriminatory selection standards, objective measures to analyze recruitment, an upward mobility system, a wage and salary structure, and standards applicable to layoff, recall, discharge, demotion, and discipline;
 - 4) The exclusion of discrimination from all collective bargaining agreements; and
 - 5) Performance of an internal audit of the reporting system to monitor execution and to provide for future planning.

- c. If discrimination by a contractor is found to exist, the Division of Purchasing shall take appropriate enforcement action which may include, but not necessarily be limited to, cancellation of the contract, suspension, or debarment by the Division of Purchasing until corrective action by the contractor is made and ensured, and referral to the Attorney General's Office, whichever enforcement action may be deemed most appropriate.

1.1.11 Clean Air Act and Federal Water Pollution Control Act - The contractor shall comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act (42 U.S.C. 7401 *et seq.*) and the Federal Water Pollution Control Act, as amended (33 U.S.C. 1251 *et seq.*).

Missouri Statewide Contract Quarterly Usage Report Instructions

The contractor shall prepare and submit a Missouri Statewide Contract Quarterly Usage Report to the Division of Purchasing which shall provide the Data Element information listed below.

The Missouri Statewide Contract Quarterly Usage Report must be received by the Division of Purchasing (Purchasing) no later than the 15th calendar day of the month following the reporting quarter entered on the Missouri Statewide Contract Quarterly Usage Report, unless the 15th is not a business day in which case the next business day thereafter shall be considered the reporting deadline. Even if there has been no usage of the contract during the reporting quarter, the contractor must still submit a report and indicate no purchases were made by marking the appropriate box on the report form.

The contractor must submit a Missouri Statewide Contract Quarterly Usage Report electronically either utilizing the "Missouri Statewide Contract Quarterly Usage Report" worksheet included in this spreadsheet which is downloadable from the following Purchasing website address:

<http://oa.mo.gov/purchasing/vendor-information> or utilizing another format which is Excel-exportable.

The contractor must submit the Missouri Statewide Contract Quarterly Usage Report to the following email address: ereports@oa.mo.gov.

Data Element	Description
Contractor Name	Contractor name as it appears on the contract.
Statewide Contract Number	Statewide contract number as listed on the cover page of your contract with the State of Missouri.
Report Contact Name	Name of the person completing the report on behalf of the contractor.
Contact Phone Number	Phone number for the person completing the report.
Contact Email Address	Email address for the person completing the report.
Date Report Submitted	Date the Missouri Statewide Contract Quarterly Usage Report is submitted to Purchasing.
Reporting Quarter	Quarter for which the contractor is reporting purchases on the contract.
Entity Type	Indicate the type of entity by entering "S" for Missouri state agency, "P" for Missouri political subdivision, "U" for Missouri university, or "O" for political subdivision or state entity from another state.
Customer Name	Customer's name. If the customer has multiple locations, please only use the main entity name.
Product or Service Description	Description of product or service purchased.
Purchase Authorization Number/Identifier	Purchase Authorization Number/Identifier supplied by customer to contractor. Enter PO or other authorization number/identifier. If procurement card used, enter "P-Card".
Contract Line Item Number	Line item number on the contract.
Quantity Delivered	Quantity (i.e. excluding returns) of products delivered. Enter a quantity of "1" for a service/project.
Unit Price Charged	Unit Price Charged (i.e. excluding credits) for the product or service purchased.
Extended Price	Quantity Delivered X Unit Price Charged.

Attachment 3 Missouri Statewide Contract Quarterly Usage Report

Contractor Name:		Report Contact Name:		Contact Email Address:			
Statewide Contract Number:		Contact Phone Number:		Date Report Submitted:			
If no purchases were made during the reporting quarter, check the box below:		Reporting Quarter: (check one)		[] January 1 - March 31		[] April 1 - June 30	
				[] July 1 - September 30		[] October 1 - December 31	
[] No purchases were made during this quarter on the contract identified above.							
Entity Type*	Customer Name	Product or Service Description	Purchase Authorization Number/Identifier	Contract Line Item Number	Quantity Delivered	Unit Price Charged	Extended Price
							\$0.00
							\$0.00
							\$0.00
							\$0.00
							\$0.00
							\$0.00
							\$0.00
							\$0.00
							\$0.00
							\$0.00
							\$0.00
							\$0.00
							\$0.00
							\$0.00
							\$0.00
							\$0.00
Overall Total of Purchases							\$0.00

* Entity Type: "S" = Missouri state agency; "P" = Missouri political subdivision; "U" = Missouri university; "O" = political subdivision or state entity from other state

Quarterly Administrative Fee Report

The contractor shall submit a "Quarterly Administrative Fee Report" to the Division of Purchasing (Purchasing) for all purchases made under the contract for which payment has been received by the contractor during the reporting quarter. The contractor must submit the "Quarterly Administrative Fee Report" to Purchasing no later than the 15th calendar day of the month following the "Reporting Quarter". The contractor shall complete the "Quarterly Administrative Fee Report" in accordance with the definitions and requirements stated below. Completed electronic forms will feed into a central database for aggregate usage. Please contact Purchasing (573) 751-2387 if you have specific questions about your contract area, the submission of this report, or payment of the administrative fee.

Header Definitions.

Contractor Name	Contractor name as it appears on the contract.
Statewide Contract Number	Statewide contract number as listed on the first page of your contract with the State of Missouri.
Date Report Submitted	Date Administrative Fee Report is submitted.
Report Contact Name	Name of the person completing the report on behalf of the contractor.
Contact Phone Number	Phone number for person completing the report.
Contact Email Address	Email address for the person completing the report.

Administrative Fee Payment Calculation - The total amount in payments received (minus returns & credits) from state agency(ies), political subdivision(s), universities, and governmental entities in other states, the Overall Total Payments Received, and the Total Administrative Fee Payment (calculated as 1% of the Overall Total Payments Received) for the Reporting Quarter.

If no payments were received during the Reporting Quarter, check the box below: Complete section if applicable.

Reporting Quarter	Quarter for which the contractor is reporting purchases for which payment has been received. This must be in format QX, where X is the Quarter number as follows: Q1: January 1 - March 31 Q3: July 1 - September 30 Q2: April 1 - June 30 Q4: October 1 - December 31
--------------------------	--

Signature of Responsible Party for Report Content: The signature and title of the person completing the report on behalf of the contractor and the date the report was completed.

Attachment - Missouri Statewide Contract Quarterly Administrative Fee Report

Contractor Name:		Report Contact Name:	
Statewide Contract Number:		Contact Phone Number:	
Date Report Submitted:		Contact Email Address:	
Administrative Fee Payment Calculation: <i>(If no payments received during Reporting Quarter, skip to next section)</i>		Reporting FY Quarter (check one):	
Total Payments Received (minus returns & credits) from Missouri <u>State Agencies</u> during the Reporting Quarter :		☐ July 1 - September 30 Quarter 1	☐ October 1 - December 31 Quarter 2
Total Payments Received (minus returns & credits) from Missouri <u>Political Subdivisions</u> (cities, counties, etc.) during the Reporting Quarter:		☐ January 1 - March 31 Quarter 3	☐ April 1 - June 30 Quarter 4
Total Payments Received (minus returns & credits) from Missouri <u>Universities</u> during the Reporting Quarter:		Submit this report to the Division of Purchasing (Purchasing) using one of the methods below:	
Total Payments Received (minus returns & credits) from <u>Governmental Entities in Other States</u> during the Reporting Quarter:		1) Mail: Division of Purchasing, P.O. Box 809, Jefferson City MO 65102 - 0809 OR 301 West High Street, Room 630, Jefferson City MO 65101 - 1517 2) Fax: (573) 526-9815 3) Email: ereports@oa.mo.gov	
Overall Total Payments Received (minus returns & credits) during the Reporting Quarter :	\$0.00	Indicate below the method of payment used for submitting the Total Administrative Fee Payment for the Reporting Quarter and date of payment submission:	
1% Administrative Fee (Multiply Overall Total Payments by 1% to determine Total Administrative Fee Payment)	1.00%	Method of Payment Used: ☐ Personal check ☐ Money Order ☐ Company check ☐ ACH (Electronic Payment) ☐ Cashier's check	
Total Administrative Fee Payment for the Reporting Quarter:	\$0.00	Date of Payment Submission: ____/____/20____ (mm/dd/yyyy)	
If no payments were received during the Reporting Quarter, check the box below:		Signature of Responsible Party for Report Content:	
☐ No payments were received this calendar quarter for any purchases on the contract identified above.		Signature: _____ Title: _____ Date: _____	

Participating Addendum Number MA2025004
for
Cybersecurity and Information Security Services
between
State of Missouri
and
Gartner, Inc.

This Participating Addendum is entered into by the **State of Missouri** ("Participating Entity") and the following Contractor (each a "Party" and collectively the "Parties") for the purpose of participating in NASPO ValuePoint Master Agreement Number MA2025004, executed by Contractor and the State of Idaho ("Lead State") for **Cybersecurity and Information Security Services** ("Master Agreement"):

Gartner, Inc. ("Contractor")
56 Top Gallant Road
Stamford, CT 06902-7700

I. PARTICIPATING ADDENDUM CONTACTS.

Contractor's contact for this Participating Addendum is:

Will McGuire
Contract Manager
Will.McGuire@Gartner.com
+1 (571) 683-4482

Participating Entity's contact for this Participating Addendum is:

Emily Thompson
Procurement Analyst
Emily.Thompson@oa.mo.gov
573-751-8897

- II. TERM.** This Participating Addendum is effective as of the date of the last signature below, and will terminate upon termination of the Master Agreement, as amended, unless the Participating Addendum is terminated sooner in accordance with the terms set forth herein.
- III. PARTICIPATION AND USAGE.** This Participating Addendum may be used by all state agencies, institutions of higher education, cities, counties, districts, and other political subdivisions of the state, and nonprofit organizations within the state if authorized herein and by law. Participating Entity has sole authority to determine which entities are eligible to use this Participating Addendum. If Contractor becomes aware that an entity's use of this Participating Addendum is not authorized, Contractor will notify NASPO ValuePoint to initiate outreach to the appropriate parties.
- IV. GOVERNING LAW.** The construction and effect of this Participating Addendum and any Orders placed hereunder will be governed by, and construed in accordance with, Participating Entity's laws.
- V. SCOPE.** Except as otherwise stated herein, this Participating Addendum incorporates the scope, pricing, terms, and conditions of the Master Agreement and the rights and obligations set forth therein as applied to Contractor and Participating Entity and Purchasing Entities.
- a. Services.** All services available through the Master Agreement may be offered and sold by Contractor to Purchasing Entities.
- i. Category 1 – Risk Assessment and Mitigation Services**
- b. Contractor Partners.** All subcontractors, dealers, distributors, resellers, and other partners identified on Contractor's NASPO ValuePoint webpage as authorized to provide Products and Services to

**Participating Addendum Number MA2025004 for
Cybersecurity and Information Security Services**

Between **State of Missouri** and
Gartner, Inc.

Participating Entity may provide Products and Services to users of this Participating Addendum. Contractor will ensure that the participation of Contractor's subcontractors, dealers, distributors, resellers, and other partners is in accordance with the terms and conditions set forth in the Master Agreement and in this Participating Addendum.

Any amendment to the Master Agreement shall be deemed incorporated into this Participating Addendum unless the amendment is rejected by Participating Entity in writing to Contractor within ten (10) calendar days of the amendment's effective date and is documented thereafter via written amendment hereto.

Any conflict between this Participating Addendum and the Master Agreement will be resolved in favor of the Participating Addendum. The terms of this Participating Addendum, including those modifying or adding to the terms of the Master Agreement, apply only to the Parties and shall have no effect on Contractor's participating addenda with other participating entities or Contractor's Master Agreement with the Lead State.

- VI. ORDERS.** Purchasing Entities may place orders under this Participating Addendum by referencing the Participating Addendum Number on an Order. Each Order placed under this Participating Addendum is subject to the pricing and terms set forth herein and in the Master Agreement, including applicable discounts, reporting requirements, and payment of administrative fees to NASPO ValuePoint and Participating Entity, if applicable.
- VII. PARTICIPATING ENTITY REPORTING REQUIREMENTS AND ADMINISTRATIVE FEE.** The contractor shall pay a one percent (1%) administrative fee to the State of Missouri which shall apply to all payments received by the contractor for all services provided under the contract. Payment of the one percent administrative fee shall be non-negotiable.
- a. The contractor shall pay the administrative fee at the end of each calendar quarter (i.e. March 31, June 30, September 30, December 31). The total administrative fee for a given quarter must equal one percent (1%) of the total payments (minus returns and credits) received by the contractor during the calendar quarter as reported on the contractor's Missouri Statewide Contract Quarterly Administrative Fee Report specified below. The administrative fee must be received by the Division of Purchasing (Purchasing) no later than the 15th calendar day of the month immediately following the end of the calendar quarter, unless the 15th is not a business day in which case the next business day thereafter shall be considered the administrative fee deadline.

Payments shall be made using one of the following acceptable payment methods:

- b. Check: Personal check, company check, cashier's check, or money order made payable to the "Missouri Revolving Information Technology Trust Fund" and sent to the following mailing address: Division of Purchasing, P.O. Box 809, Jefferson City, MO 65102 – 0809 OR Division of Purchasing, 301 West High Street, Room 630, Jefferson City, MO 65101-1517. The contractor's payment by check shall authorize the State of Missouri to process the check electronically. The contractor understands and agrees that any returned check from the contractor may be presented again electronically and may be subject to additional actions and/or handling fees.

Electronic Payment: Instructions on how to submit payments electronically by automated clearing house (ACH) will be provided upon request by contacting the Division of Purchasing at (573) 751-2387.

- c. All payments of the administrative fee shall include the contract number on any check or transmittal document. However, only one contract number must be entered on a check or transmittal document.

If submitting an administrative fee payment for more than one contract, then a separate check or electronic payment and associated transmittal document must be submitted by the contractor for each contract.

- VIII. MISSOURI STATEWIDE CONTRACT QUARTERLY ADMINISTRATIVE FEE REPORT.** The contractor shall submit a Missouri Statewide Contract Quarterly Administrative Fee Report to the Division of Purchasing which shall identify the total payments (minus returns and credits) received by the contractor from state Division of Purchasing.
- a. The contractor shall prepare and submit the Missouri Statewide Contract Quarterly Administrative Fee Report at the end of each calendar quarter (i.e. March 31, June 30, September 30, December 31) for total payments (minus returns and credits) received by the contractor during the calendar quarter. The Missouri Statewide Contract Quarterly Administrative Fee Report must be received by the Division of Purchasing (Purchasing) no later than the 15th calendar day of the month following the reporting quarter entered on the report, unless the 15th is not a business day in which case the next business day thereafter shall be considered the reporting deadline. Even if there has been no usage of the contract during the reporting quarter, the contractor must still submit a report and indicate no payments were received by marking the appropriate box on the report form.
 - b. The Missouri Statewide Contract Quarterly Administrative Fee Report form may be downloaded from the following Purchasing website: <http://oa.mo.gov/purchasing/vendor-information>. The Missouri Statewide Contract Quarterly Administrative Fee Report is also included herein as Attachment 3. The Missouri Statewide Contract Quarterly Administrative Fee Report must be submitted using one of the following methods:

Mail: Division of Purchasing,
P.O. Box 809, Jefferson City MO 65102-0809

OR

Division of Purchasing,

301 West High Street, Room 630, Jefferson City, MO 65101-1517

Fax: (573) 526-9815
Email: ereports@oa.mo.gov
 - c. The contractor shall agree that the Division of Purchasing reserves the right to modify the requested format and content of the Missouri Statewide Contract Quarterly Administrative Fee Report by providing thirty (30) calendar days written notice to the contractor. The contractor shall also agree the Division of Purchasing may unilaterally amend the contract, with thirty (30) calendar days notice to the contractor to change the method of payment of the administrative fee, the timing for submission of the Missouri Statewide Contract Quarterly Administrative Fee Report, and/or timing for payment of the administrative fee. The contractor shall understand and agree that if such an amendment is issued by the Division of Purchasing, the contractor shall comply with all contractual terms, as amended.

- IX. **MISSOURI STATEWIDE CONTRACT QUARTERLY USAGE REPORT.** The contractor shall submit a Missouri Statewide Contract Quarterly Usage Report to the Division of Purchasing that provides the Data Element information listed below:

Data Element	Description
Contractor Name	Contractor name as it appears on the contract.
Statewide Contract Number	Statewide contract number as listed on the cover page of your contract with the State of Missouri.
Report Contact Name	Name of the person completing the report on behalf of the contractor.
Contact Phone Number	Phone number for the person completing the report.
Contact Email Address	Email address for the person completing the report.
Date Report Submitted	Date the Missouri Statewide Contract Quarterly Usage Report is submitted to the Division of Purchasing.
Reporting Quarter	Quarter for which the contractor is reporting purchases on the contract.
Entity Type	Indicate the type of entity by entering "S" for Missouri state agency, "P" for Missouri political subdivision, "U" for Missouri university, or "O" for political subdivision or state entity from another state.
Customer Name	Customer's name. If the customer has multiple locations, please only use the main entity name.
Product or Service Description	Description of product or service purchased.
Purchase Authorization Number/Identifier	Purchase Authorization Number/Identifier supplied by customer to contractor. Enter PO or other authorization number/identifier. If procurement card used, enter "P-Card".
Contract Line Item Number	Line item number on the contract.
Quantity Delivered	Quantity (i.e. excluding returns) of products delivered. Enter a quantity of "1" for a service/project.
Unit Price Charged	Unit Price Charged (i.e. excluding credits) for the product or service purchased.
Extended Price	Quantity Delivered X Unit Price Charged.

- a. The contractor shall prepare and submit the Missouri Statewide Contract Quarterly Usage Report at the end of each calendar quarter (i.e. March 31, June 30, September 30, December 31) for the purchases made under the contract during the calendar quarter. The Missouri Statewide Contract Quarterly Usage Report must be received by the Division of Purchasing no later than the 15th calendar day of the month following the reporting quarter entered on the Missouri Statewide Contract Quarterly Usage Report, unless the 15th is not a business day in which case the next business day thereafter shall be considered the reporting deadline. Even if there has been no usage of the contract during the reporting quarter, the contractor must still submit a report and indicate no purchases were made.
- b. The contractor must submit a Missouri Statewide Contract Quarterly Usage Report electronically either utilizing the "Missouri Statewide Contract Quarterly Usage Report" worksheet included herein in Attachment 4 which is downloadable from <https://purch.oa.mo.gov/vendor-information> or

**Participating Addendum Number MA2025004 for
Cybersecurity and Information Security Services**

Between **State of Missouri** and
Gartner, Inc.

utilizing another format which is Excel-exportable. The contractor must submit the Missouri Statewide Contract Quarterly Usage Report to the following email address: ereports@oa.mo.gov.

- c. The contractor shall agree that the Division of Purchasing reserves the right to modify the requested format and content of the Missouri Statewide Contract Quarterly Usage Report by providing thirty (30) calendar days' written notice to the contractor. The contractor shall also agree the Division of Purchasing may unilaterally amend the contract, with thirty (30) calendar days' notice to the contractor to change the timing for submission of the Missouri Statewide Contract Quarterly Usage Report. The contractor shall understand and agree that if such an amendment is issued by the Division of Purchasing, the contractor shall comply with all contractual terms, as amended.

X. FEDERAL FUNDING REQUIREMENTS. Orders funded with federal funds may have additional contractual requirements or certifications that must be satisfied at the time the Order is placed or upon delivery. When applicable, a Purchasing Entity will identify in the Order any alternative or additional requirements related to the use of federal funds. By accepting the Order, Contractor agrees to comply with the requirements set forth therein.

XI. ATTACHMENTS. This Participating Addendum includes the following attachments:

- a. **Attachment 1: Business Associates Provisions**
- b. **Attachment 2: federal Funds Requirement**
- c. **Attachment 3: Missouri Statewide Quarterly Admin. Fee Instructions and Report**
- d. **Attachment 4: Missouri Statewide Contract Admin. Fee Quarterly Usage Instructions and Report**

XII. NOTICE. Any notice required herein shall be sent to the following:

For Contractor:

Will McGuire
Contract Manager
Will.McGuire@Gartner.com
+1 (571) 683-4482

For Participating Entity:

Emily Thompson
Procurement Analyst
Emily.Thompson@oa.mo.gov
573-751-8897

XIII. SUBMISSION OF PARTICIPATING ADDENDUM TO NASPO VALUEPOINT. Upon execution, Contractor shall promptly email a copy of this Participating Addendum and any amendments hereto to NASPO ValuePoint at pa@naspovaluepoint.org. The Parties acknowledge and agree that the Participating Addendum, as amended, may be published on the NASPO ValuePoint website.

SIGNATURE

The undersigned for each Party represents and warrants that this Participating Addendum is a valid and legal agreement binding on the Party and enforceable in accordance with the Participating Addendum's terms and that the undersigned is duly authorized and has legal capacity to execute and deliver this Participating Addendum and bind the Party hereto.

Participating Addendum Number MA2025004 for
Cybersecurity and Information Security Services

Between **State of Missouri** and
Gartner, Inc.

IN WITNESS WHEREOF, the Parties have executed this Participating Addendum.

CONTRACTOR:

DocuSigned by:

David Vixama
CCE13228C8BD44B...

Signature

David Vixama

Printed Name

Assoc. Director

Title

July 22, 2026

Date

PARTICIPATING ENTITY:

Stacia Dawson

Signature

Stacia Dawson

Printed Name

Director

Title

7/28/26

Date

ATTACHMENT 1

MISSOURI ECONOMIC IMPACT

The utilization of Missouri businesses and Missouri employees and other positive economic impact in the provision of the products and/or services under the agreement between the State of Missouri and the vendor is highly desirable for the State of Missouri. Therefore, please provide responses to the following to describe your Missouri economic impact.

1. Provide a description of the company's economic presence within the State of Missouri, including Missouri employees statistics, Missouri business facilities (size, type of facility, location), Missouri subcontractors, etc.

Gartner does not provide itemized breakdowns of our economic contributions by State, however we can confirm that Gartner does employ associates that reside in Missouri. Gartner also maintains a robust subcontractor network, including Missouri subcontractors. Gartner does not have any physical office locations in Missouri.

2. Provide a description of the proposed services that will be performed and/or the proposed products that will be provided by the Missourians and/or Missouri products under Missouri Contract Number CPPT30034902600033.

Services provided under this contract will be in accordance with the scope defined by the contract. Individual projects will be contracted via detailed Statements of Work developed in collaboration with State customers. Gartner Consulting's Cybersecurity and Resilience practice drives stronger outcomes by staying ahead of evolving threats and technologies using data-driven consulting, enriched by Gartner insights. We support organizations across industries with research, analytics, and deep expertise to strengthen security posture, increase resilience, and confidently navigate change. Today's cybersecurity and technology leaders are accelerating transformation by:

- Enhancing mission-critical services through secure digital transformation and responsible AI integration
- Modernizing service delivery with resilient and adaptive technologies
- Boosting operational efficiency while ensuring transparency and accountability
- Protecting critical infrastructure and sensitive data against emerging threats
- Upgrading legacy systems to reduce risk and improve responsiveness
- Accelerating agility to meet evolving business, regulatory, and stakeholder demands

3. Provide a description of the economic impact returned to the State of Missouri through tax revenue obligations.

Gartner's services drive significant indirect economic returns to the State of Missouri by stabilizing the macro-fiscal environment and optimizing the use of taxpayer dollars. By utilizing Gartner's IT Budget Benchmark and Cost Optimization research, the State has identified mechanisms to reduce "run" expenditures and reallocate those funds toward "transformational" projects that stimulate economic activity. This strategic realignment is critical as the State navigates a projected \$2.2 billion revenue gap in FY26. By mitigating technical debt and preventing costly cybersecurity breaches through Gartner-guided infrastructure hardening, the State protects its core general revenue and ensures that tax obligations are met with maximum efficiency and minimal waste.

4. List all Missouri certified Minority Business Enterprises (MBE)/Women Business Enterprises (WBE) as defined at Website: <http://oeo.mo.gov> you will use in the provision of products and services under the contract:

Gartner does not anticipate the need for subcontractors to perform the scope of work contemplated in this Proposal. Gartner has substantial experience, knowledge, skills and resources specific to the services requested, as well as the resources and capacity to perform the services under the contract.

Should the need for additional skills, knowledge or local resources arise, we will discuss such matters with the client and seek approval prior to engaging any subcontractors. Gartner is committed to conducting business in an ethical and honest manner and in compliance with all applicable laws and regulations.

5. List all Missouri Organizations for the Blind or any Missouri Sheltered Workshops as listed at Websites <http://dese.mo.gov/special-education/sheltered-workshops/directories>, <http://www.lhbindustries.com> and <http://www.alphapointe.org> you will use in the provision of products and services under the contract:

Gartner does not anticipate the need for subcontractors to perform the scope of work contemplated in this Proposal. Gartner has substantial experience, knowledge, skills and resources specific to the services requested, as well as the resources and capacity to perform the services under the contract. Should the need for additional skills, knowledge or local resources arise, we will discuss such matters with the client and seek approval prior to engaging any subcontractors. Gartner is committed to conducting business in an ethical and honest manner and in compliance with all applicable laws and regulations.

6. List all Missouri Service-Disabled Veteran Business Enterprises (SDVE's) as listed at Website <https://purch.oa.mo.gov/vendor-information/missouri-service-disabled-veteran-business-enterprise-sdve-information> you will use in the provision of products and services under the contract:

Gartner does not anticipate the need for subcontractors to perform the scope of work contemplated in this Proposal. Gartner has substantial experience, knowledge, skills and resources specific to the services requested, as well as the resources and capacity to perform the services under the contract. Should the need for additional skills, knowledge or local resources arise, we will discuss such matters with the client and seek approval prior to engaging any subcontractors. Gartner is committed to conducting business in an ethical and honest manner and in compliance with all applicable laws and regulations.



State of Idaho Contract Number MA2025004 Amendment Number 1

Parties

Agency	Contractor
Department of Administration 650 W. State St. Boise, ID 83702	Gartner, Inc. 56 top Gallant Road Stamford, CT 06902-7700

Contract Summary

Contract Name: Cybersecurity and Information Security Services Contract Description: Cybersecurity and Information Security Services Original Effective Date: 12/08/2025 Current Expiration Date: 10/31/2027	Contract Usage Type: NASPO
---	-----------------------------------

Agency Contacts

Contact Name	Contact Type	Contact Email
DOP Contract Administration	Contract Administrator	contractadmin@adm.idaho.gov

Contractor Contacts

Contact Name	Contact Phone	Contact Email
Will McGuire	(571) 683-4482	will.mcguire@gartner.com

Recitals

- The Parties entered into a Contract (MA2025004) for Cybersecurity and Information Security Services for NASPO ValuePoint, effective December 8, 2025.
- With this Amendment No. 1, the Parties desire to Renew the contract for one year and incorporate certifications required by Idaho Code, as further detailed below.

Agreement

Based on the above recitals, and good and valuable consideration, the receipt of which is hereby acknowledged, the Contract is amended as follows:

- The Contract is renewed from November 1, 2026, to October 31, 2027
- The following certifications are added to the Contract:
 - ADA accessibility language The Contractor shall use best efforts ensure all digital products, services, and content provided under this Agreement comply with the Americans with Disabilities Act (ADA), Section 508 (as applicable), and WCAG 2.1 Level AA. This requirement applies to all websites, applications, software, documents, multimedia, and any digital tools or services provided or procured for the State of Idaho. Failure to

meet WCAG 2.1 Level AA may result in any remedies available under Idaho procurement law, including but not limited to: Requiring the Contractor to cure deficiencies, State performed testing or remediation at no cost to the State, Withholding payment, Termination of the Contract. In the event of an alleged failure, the State will first provide the Contractor with written notice and a reasonable opportunity to cure any deficiencies before considering any other remedies.

3. Except as expressly modified in this Amendment, all other terms and conditions of the Contract remain in full force and effect.
4. This Amendment is effective upon the date of the last signature below. In no event will this Amendment be effective until executed by the Department of Administration.

Department of Administration

Signature: Connor Long

Name: Connor Long

Contract Administration

Title: _____

08/06/2026

Date: _____

Gartner, Inc.

Signed by:
David Vixama
E0DD967FBB7047F...

Signature: _____

Name: David Vixama

Title: Assoc. Director

Date: August 6, 2026

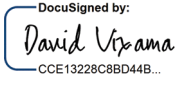
Certificate Of Completion

Envelope Id: 1D2DCD18-3ACE-877E-80BD-E669E7AEE546	Status: Completed
Subject: Complete with Docusign: NASPO Cyber - Missouri.pdf	
Source Envelope:	
Document Pages: 55	Signatures: 5
Certificate Pages: 1	Initials: 50
AutoNav: Disabled	Envelope Originator:
Envelopeld Stamping: Disabled	David Vixama
Time Zone: (UTC-08:00) Pacific Time (US & Canada)	56 Top Gallant Road
	Stamford, CT 06904
	david.vixama@gartner.com
	IP Address: 136.226.59.116

Record Tracking

Status: Original	Holder: David Vixama	Location: DocuSign
7/22/2026 2:41:00 PM	david.vixama@gartner.com	

Signer Events

Signer Events	Signature	Timestamp
David Vixama	DocuSigned by:  CCE13228C8BD44B...	Sent: 7/22/2026 2:41:49 PM
david.vixama@gartner.com		Viewed: 7/22/2026 2:41:56 PM
Assoc. Director		Signed: 7/22/2026 2:51:56 PM
Gartner, Inc.		Freeform Signing
Security Level: Email, Account Authentication (None)	Signature Adoption: Pre-selected Style Using IP Address: 136.226.59.116	

Electronic Record and Signature Disclosure:
Not Offered via Docusign

In Person Signer Events	Signature	Timestamp
Editor Delivery Events	Status	Timestamp
Agent Delivery Events	Status	Timestamp
Intermediary Delivery Events	Status	Timestamp
Certified Delivery Events	Status	Timestamp
Carbon Copy Events	Status	Timestamp
Witness Events	Signature	Timestamp
Notary Events	Signature	Timestamp
Envelope Summary Events	Status	Timestamps
Envelope Sent	Hashed/Encrypted	7/22/2026 2:41:49 PM
Certified Delivered	Security Checked	7/22/2026 2:41:56 PM
Signing Complete	Security Checked	7/22/2026 2:51:56 PM
Completed	Security Checked	7/22/2026 2:51:56 PM
Payment Events	Status	Timestamps



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.

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



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

**Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES**

Issued by the **State of Idaho**
Solicitation Number RFP#928



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

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



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		Scope
- 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		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		Key Deliverables
- 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		- 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

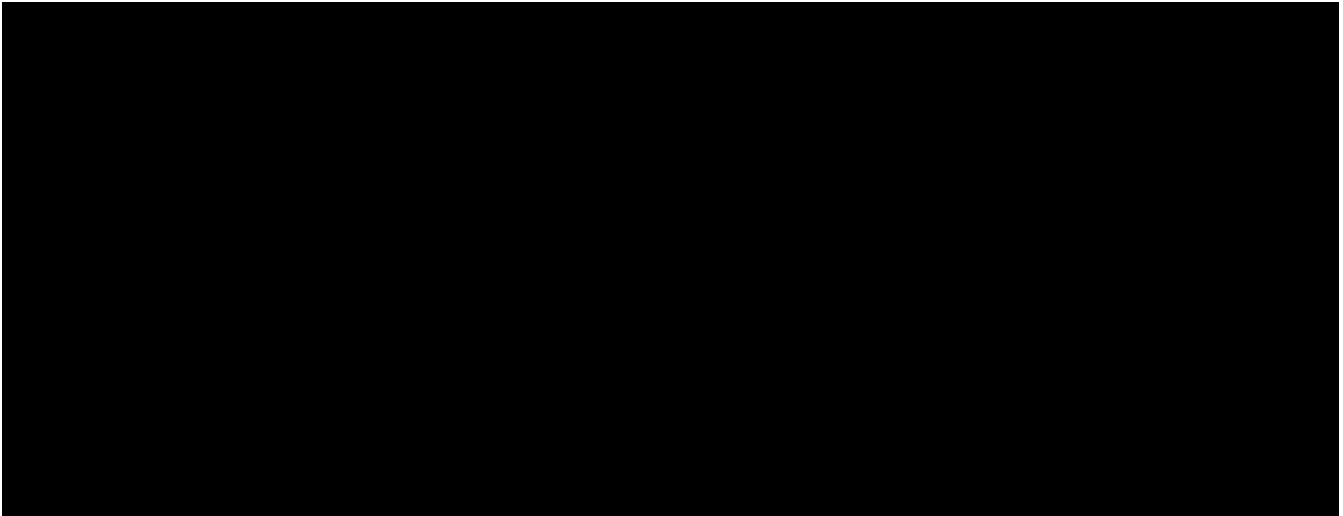


integrators — to help our clients achieve their most critical objectives. Gartner maximizes access to Subject Matter Experts (SMEs) by blending Research Analysts and Consultants to provide thought leadership and support innovation.

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.

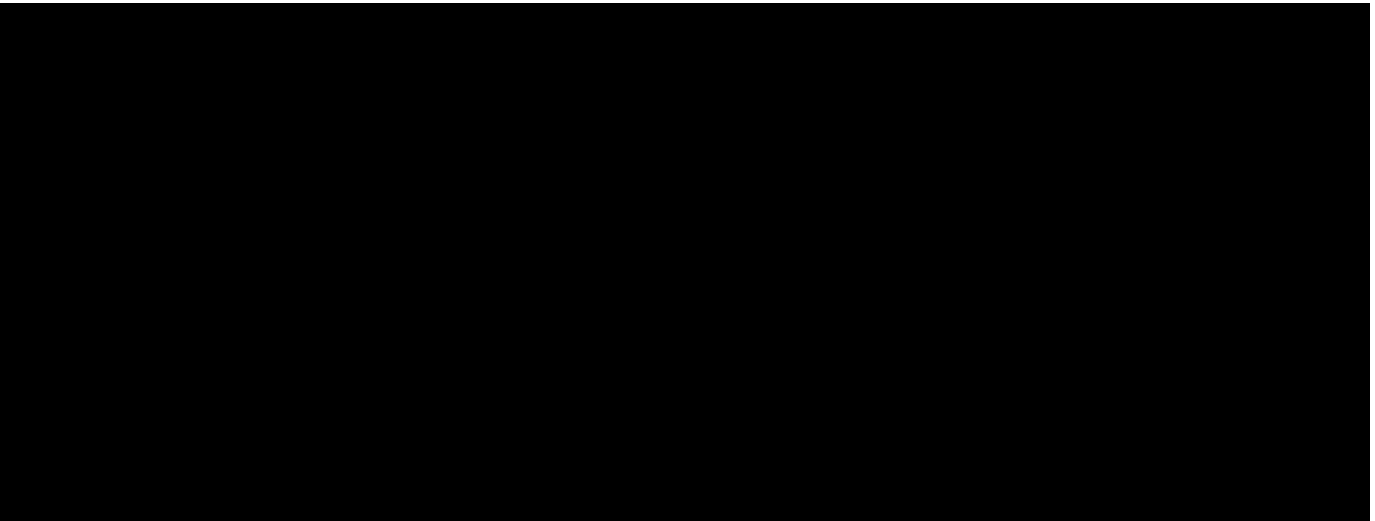
Assessing Maturity to inform Risk Mitigation: As security maturity increases, reducing additional risk requires exponential increases in cost and effort. Therefore, organizations in any industry must identify their ideal return on investment

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 identify areas of risk consistently. Illustrative examples include:

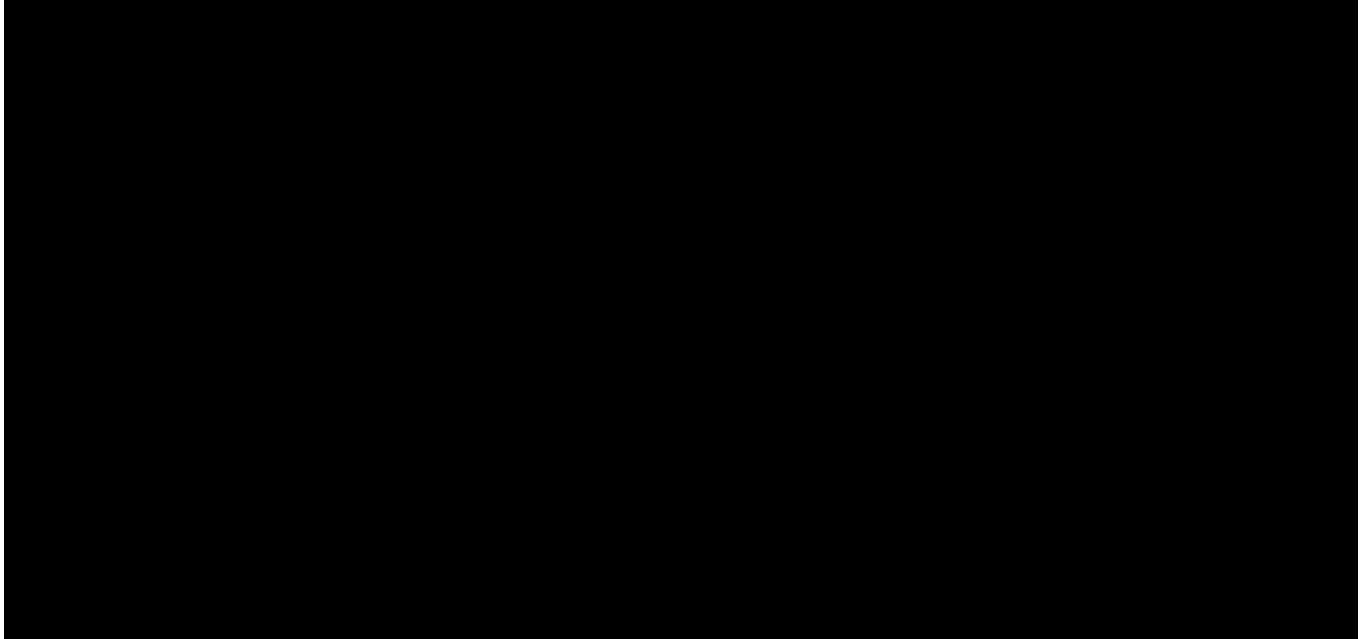
Figure 2. Sample Entity Assessment Deliverables





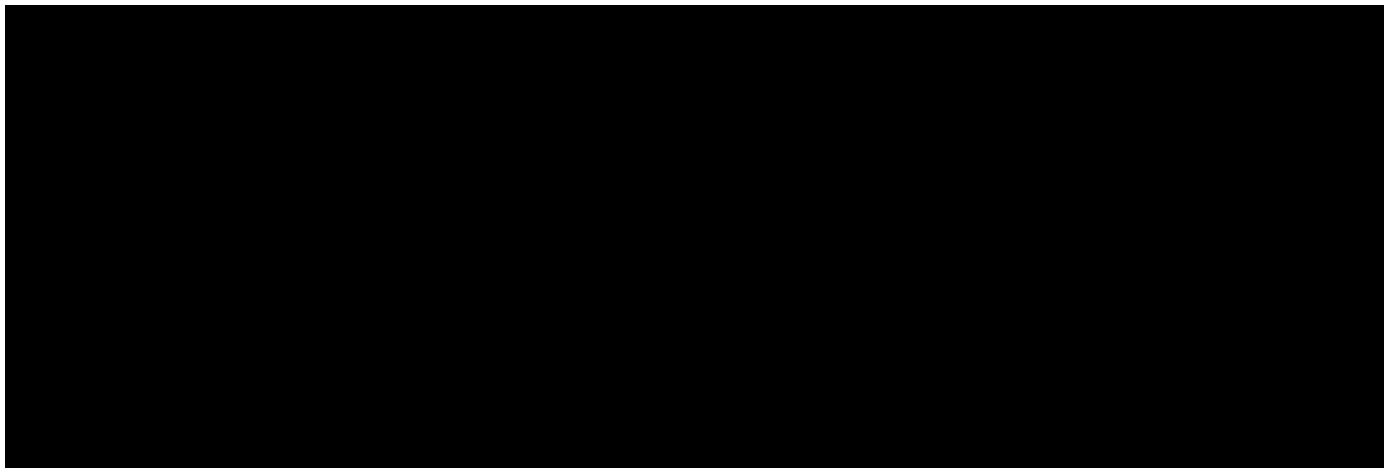
Benchmarking Against Peers: An entity's maturity is benchmarked against peer organizations, including spending and staffing models. Enabling strategic planning to consider performance against peer organizations while considering differences in staffing and spending levels.

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:

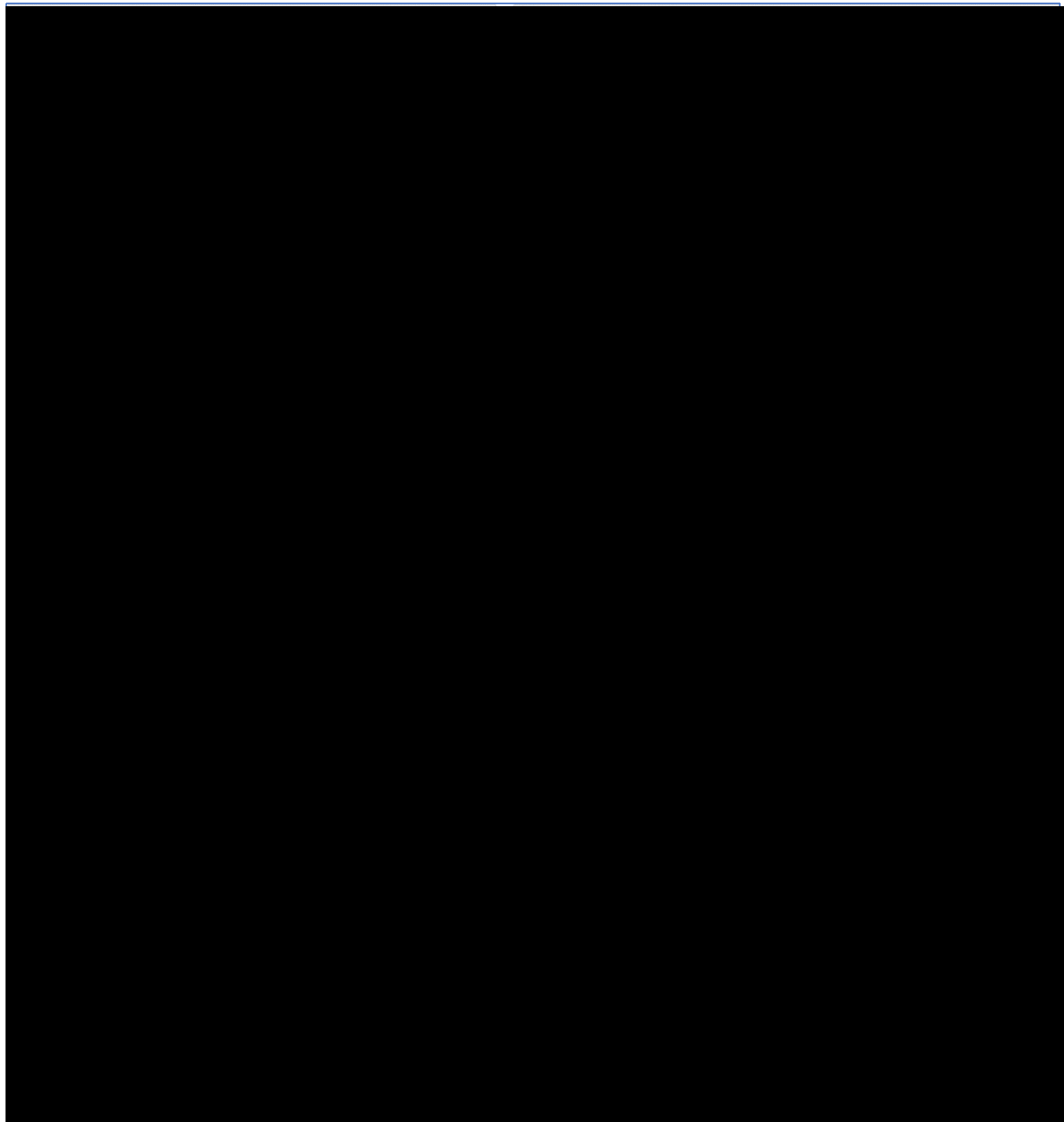
Figure 4. Sample Vulnerability Gap Assessment Report Excerpt





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

Gartner achieves results through a coordinated engagement

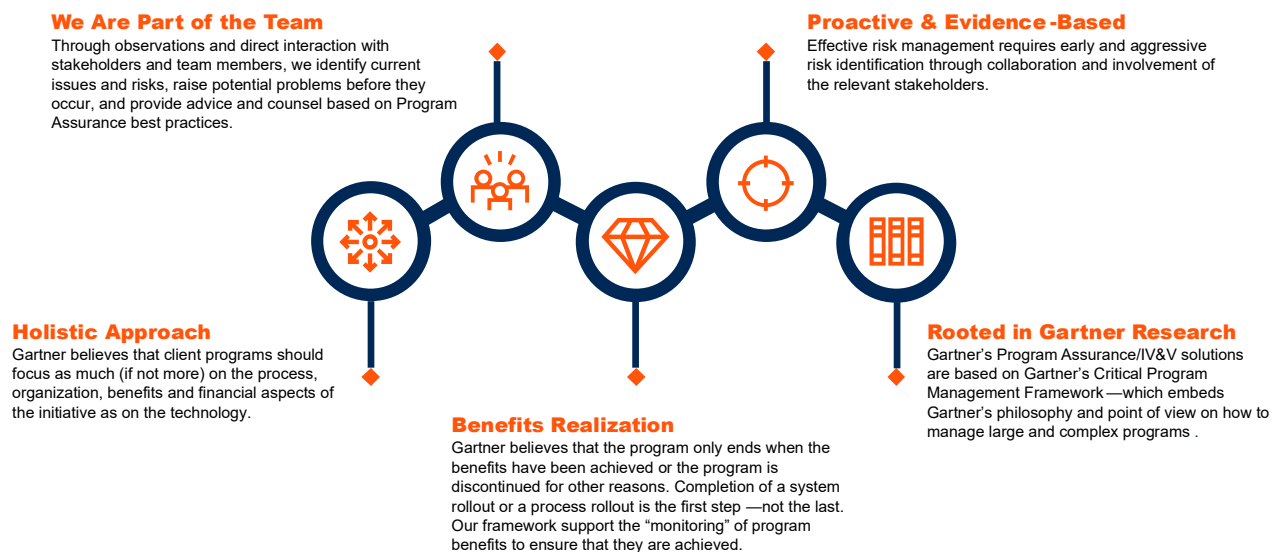


Figure 7. Program Assurance Approach

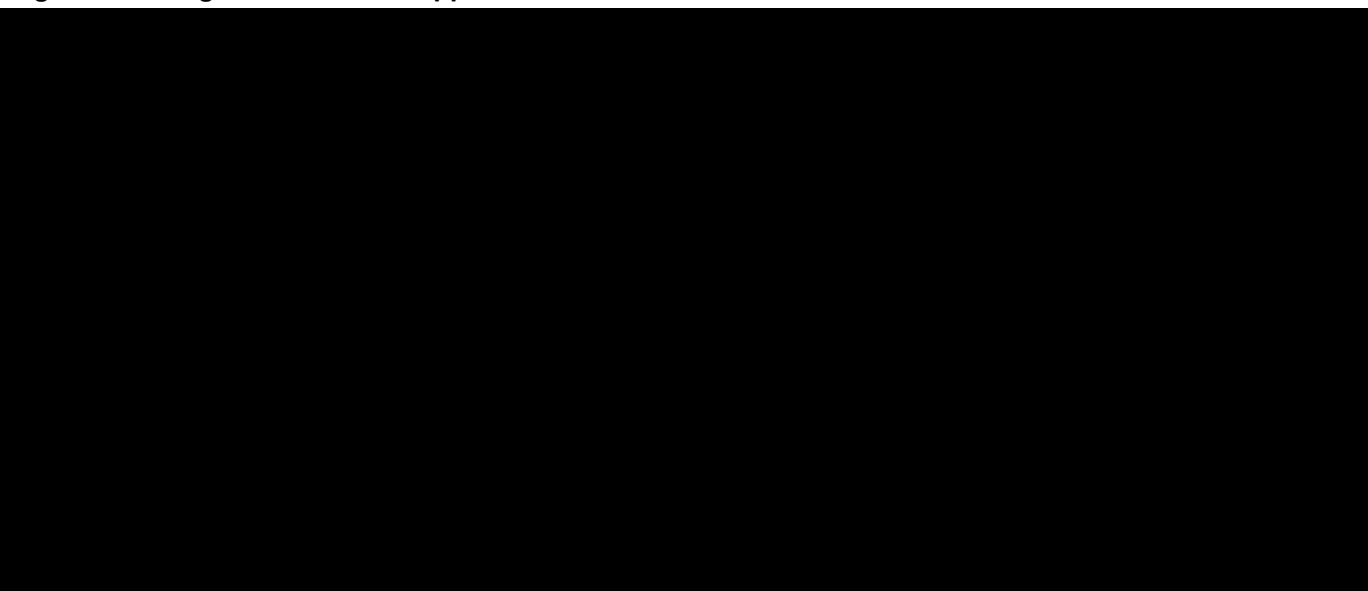
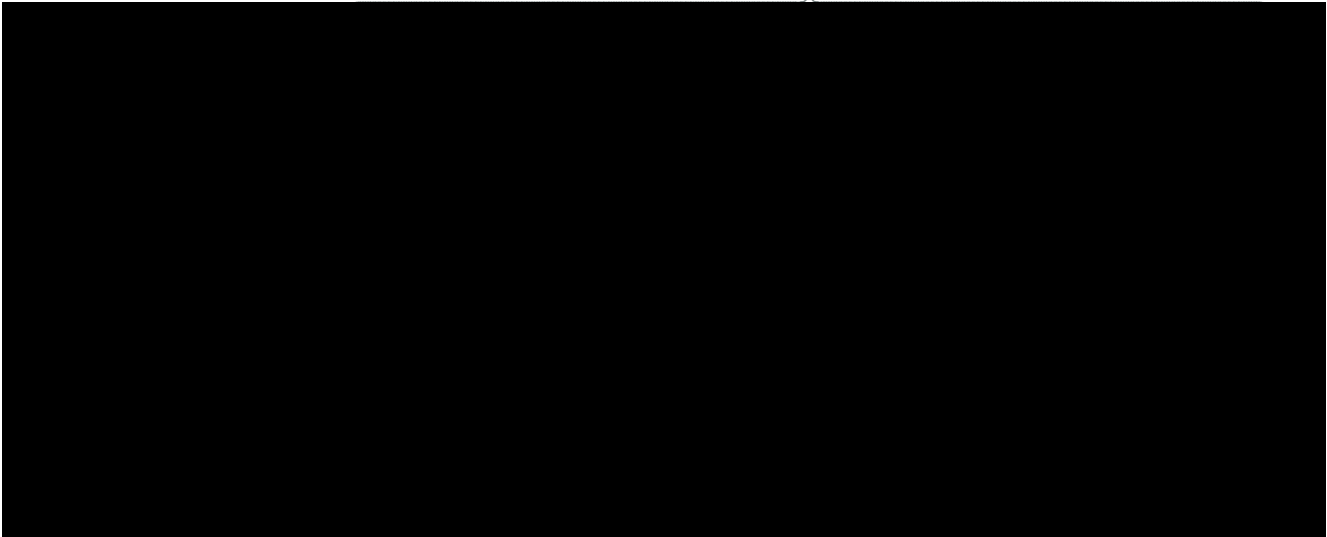


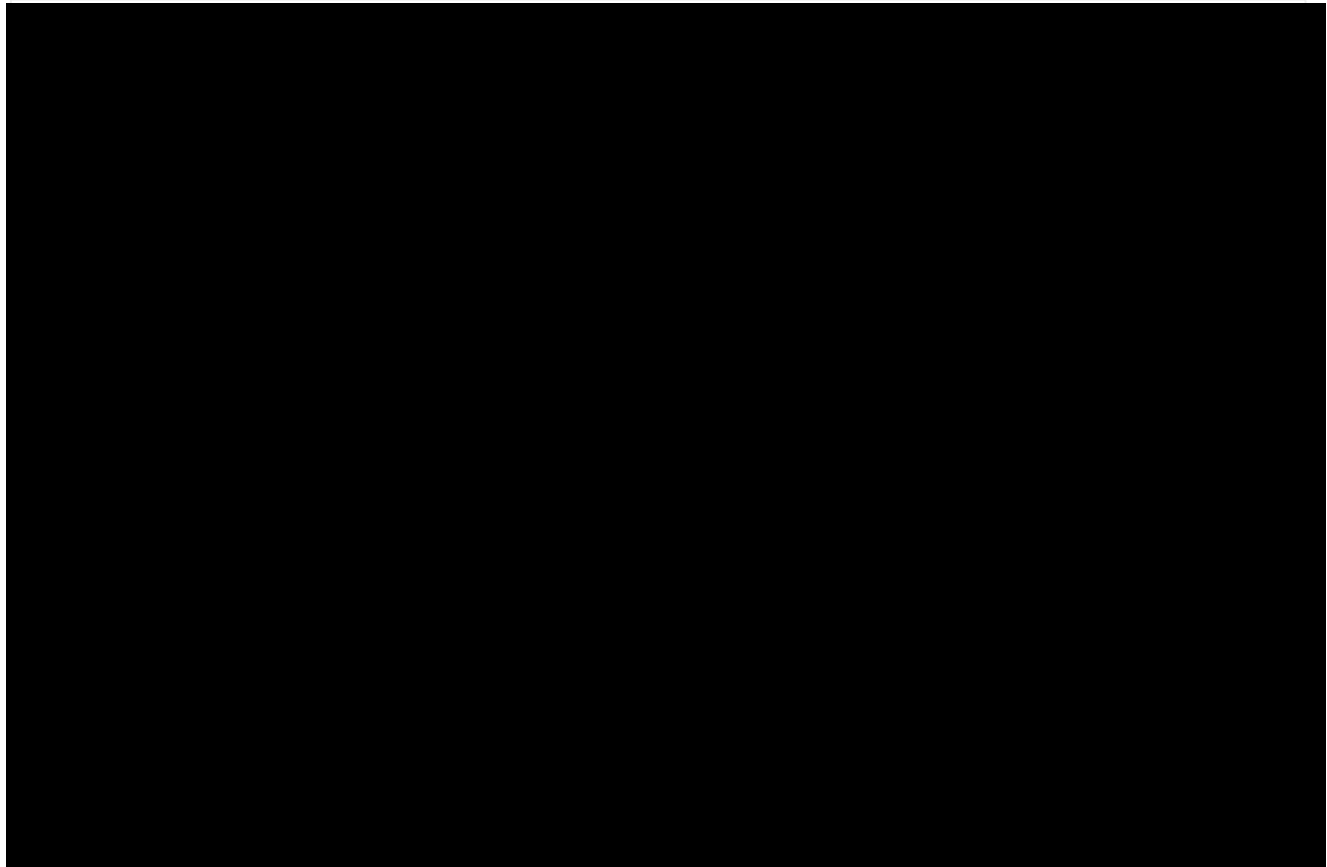


Figure 8. Program Assurance Risk/Readiness Methodology



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.

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



- 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.

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



- 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.

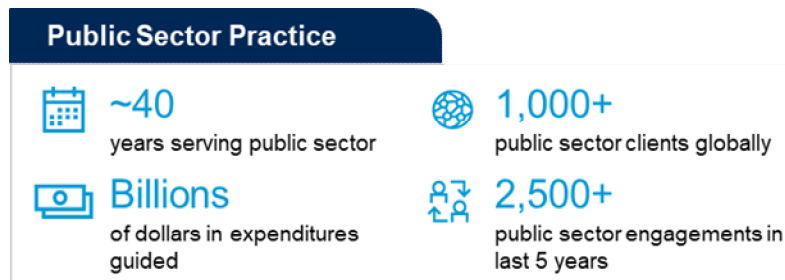
Gartner extensively covers the cybersecurity market with +100 dedicated industry experts, routinely advising and gathering insights from clients, vendors and customers in 600+ calls and interactions each year.

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



Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



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

Client Organization	Risk Assessment & Mitigation Activities				
	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

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



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.

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



Client Name	Project Title	Project Duration	Key Activities	Outcomes
[REDACTED]	▪ Cybersecurity Risk and Maturity Assessment	12/2021-04/2022	▪ 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.
		05/2022-10/2022		
		01/2025-03/2025		
[REDACTED]	▪ Cybersecurity Risk and Maturity Assessment	Phase 1: 10/2020-02/2021	▪ 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.
	▪ Cybersecurity Mitigation Recommendations & Roadmap	Phase 2: 06/2022-10/2022		
	▪ Election Security Assessment & Penetration Testing	Phase 3: 07/2023-12/2023		
		Phase 4: 09/2024-12/2024		
[REDACTED]	▪ Security Risk Assessment & Strategy	Phase 1: 01/2018-04/2018	▪ 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.
		Phase 2: 01/2021-04/2021		

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



Client Name	Project Title	Project Duration	Key Activities	Outcomes
[REDACTED]	Cybersecurity Risk and Maturity Assessment	07/2015-09/2015	Conducted tri-annual Risk Assessments with process rigor, intensity, and breadth of coverage for the overall organization in a consistent and standardized manner.	- 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.
		08/2019-11/2019		
		09/2022-12/2022	- 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.	
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.

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



Client Name	Project Title	Project Duration	Key Activities	Outcomes
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	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.	
			- 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.

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



- **(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.

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



	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.

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



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

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



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:

Gartner's Cybersecurity & Resilience Practice Provides a Comprehensive Suite of Solutions and Capabilities

Cross Industry Expertise and Scalable Delivery Models					
Cybersecurity Resilience	Cybersecurity Operations	Cybersecurity Architecture and Design	Cybersecurity and Risk Management	Identity and Access Management	Framework Alignments
Exercises and Tabletops	Threat Modeling	Cloud Security	Cybersecurity Metrics/ Executive Dashboards	IAM Architecture Modernization	ISO27000 Certification Prep
Business Continuity	SOC Security Services	Network Security	Third Party Risk Management	IAM Maturity and Tool Optimization	Utilities (NERC/FERC) Protection
Resilience	Pen Testing	Application Security	Maturity Assessment	IGA Implementation Readiness	
Disaster Recovery	Incident Response	Operational Technology (OT)	Security Operating Model Modernization	PAM Implementation Readiness	
		AI Risk and Security	Security Policy & Standards Development		
		Cybersecurity Sourcing and Vendor Management			
		Zero Trust Enablement			
		Data Security and Privacy			

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.

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



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.

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



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 your 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 identify opportunities to realized talent and location strategy.

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



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.

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



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.

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



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.

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



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.

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



3. [REDACTED]

Sales under contract in last 5 years: \$ [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 tradeshow 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 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 NASPO 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.

**Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES**

Issued by the **State of Idaho**
Solicitation Number RFP#928



- 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.

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



- 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 tradeshow or expos as well as emailed to existing and prospective customers who are candidates for using this contract.

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



- **Webinars:** Gartner produces and presents regular webinars available to NASPO Participating Entities/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 NASPO 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

**Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES**

Issued by the **State of Idaho**
Solicitation Number RFP#928



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 it 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. **Debarment.** (Check one of the below.)

- ☒ Neither Offeror nor its principals are presently debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participation in public procurement or contracting by any governmental department or agency.
- ☐ Offeror cannot certify the statement above, and Offeror will affix a written explanation to this attachment for review by the Lead State. If after reviewing Offeror's written explanation the Lead State determines it is not in the best interest of the Lead State, Participating Entities, or Purchasing Entities to award Offeror a Master Agreement, the Lead State may reject Offeror's proposal.

B. **Non-collusion.**

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



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

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

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

- ☒ Offeror is not an entity subject to laws, rules, or policies potentially requiring disclosure of, or provision of access to, customer data to foreign governments or entities controlled by foreign governments, and Offeror's offerings do not contain, include, or utilize components or services supplied by any entity subject to the same. Offeror's offerings also do not contain, include, or utilize covered technology prohibited under Section 889 of the National Defense Authorization Act, as amended.
- ☐ Offeror cannot certify all statements above, and Offeror will affix a written explanation to this attachment for review by the Lead State. If after reviewing Offeror's written explanation the Lead State determines it is not in the best interest of the Lead State, Participating Entities, or Purchasing Entities to award Offeror a Master Agreement, the Lead State may reject Offeror's proposal.

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

- ☒ Offeror represents that none of its officers or employees are officers or employees of the Lead State and that none of its officers or employees have a conflict of interest as defined by the laws, rules, or policies of the Lead State.
- ☐ Offeror cannot certify the statement above, and Offeror will affix a written explanation to this attachment for review by the Lead State. If after reviewing Offeror's written explanation the Lead State determines it is not in the best interest of the Lead State, Participating Entities, or Purchasing Entities to award Offeror a Master Agreement, the Lead State may reject Offeror's proposal.

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

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

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

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



- and Non-Public Information, and submit with Offeror's proposal a redacted copy of Offeror's proposal, which must be clearly marked as such. Offeror may not mark pricing or Offeror's entire proposal as confidential, proprietary, or protected. Submission of a Claim of Trade Secrets and Non-Public Information does not guarantee that information claimed by Offeror as confidential, proprietary, or protected will not be subject to disclosure in accordance with applicable public information laws, rules, and policies. If Offeror fails to submit a redacted copy of Offeror's proposal, or fails to claim information as confidential, proprietary, or protected in compliance with this RFP, Offeror releases the Lead State, NASPO, NASPO members, and entities represented on the Multistate Sourcing Team from any obligation to keep the information confidential and waives all claims of liability arising from disclosure of the information.
- I. **Cancellation and Transfer.** Offeror understands and agrees that the Lead State may, as set forth in Attachment 01, RFP Terms and Conditions, cancel this RFP or transfer this RFP to a new Lead State if the Lead State determines that such transfer is in the best interest of the Lead State and potential Participating Entities and Purchasing Entities.
- J. **Conditional Awards.** Offeror understands that awards and execution of a Master Agreement are conditional as set forth in Attachment 01, RFP Terms and Conditions, and Offeror agrees to hold the Lead State and NASPO harmless and release the Lead State and NASPO from any liability for damages arising from non-award or non-execution of a contract.
- K. **Understanding of the RFP.** Offeror has read the RFP in its entirety and understands and agrees to comply with all requirements set forth therein. Any conflicts in the materials composing the RFP and any issues relating to the content of the RFP, including instructions, requirements, or specifications Offeror believes to be ambiguous, unduly restrictive, erroneous, anticompetitive, or unlawful, have been brought to the attention of the Lead State using the process described in the RFP for asking questions or, if applicable, by filing a protest. In accordance with Attachment 01, RFP Terms and Conditions, Offeror acknowledges and understands that any protest, claim, dispute, or action based upon a conflict or issue described herein must be filed no later than the RFP Close Date, and Offeror waives the right to file any protest, claim, dispute, or action based upon a conflict or issue described herein if not filed by the RFP Close Date.

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

Request for Proposals for
CYBERSECURITY AND INFORMATION SECURITY SERVICES

Issued by the **State of Idaho**
Solicitation Number RFP#928



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:

A handwritten signature in black ink, appearing to read "Paul Denvir", written over a horizontal line.

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