

PORTFOLIO TITLE: [Cybersecurity and Information Security Services](#)

LEAD STATE: Idaho

OVERVIEW:

The Master Agreements in this portfolio offer a suite of proactive and reactive Cybersecurity and Information Security Services including Risk Assessment and Mitigation, Incident Response, Breach Coach Services, and Notification and Credit Monitoring Services.

INITIAL TERM: One year

RENEWALS: Up to an additional five years.

TOTAL TERM POSSIBLE: Six years



PRODUCT CATEGORIES:

- **Category 1: Risk Assessment and Mitigation Services** - The Contractor will provide professional services that help organizations identify potential risks, evaluate their likelihood and impact, and then develop strategies to minimize or eliminate those risks, essentially protecting the organization's assets and ensuring business continuity by proactively addressing potential threats; it involves both analyzing potential dangers and taking proactive steps to manage them effectively.
- **Category 2: Incident Response Services** - The Contractor will assist organizations in detecting, containing, and mitigating damage from cybersecurity breaches or attacks, essentially providing a rapid response to security incidents to minimize harm and restore system functionality when a threat occurs; they aim to identify, analyze, and address security issues quickly, while also learning from past incidents to improve future preventative measures.
- **Category 3: Breach Coach Services** - The Contractor will provide guidance and support for businesses experiencing or at risk of a cybersecurity incident, offered to help navigate the incident response process and mitigate potential damages.
- **Category 4: Notification and Credit Monitoring Services** - A la carte services as needed by the Purchasing Entity in the event of a data breach. Based on needs the purchasing entity may choose from any of the following services, or any combination thereof: Notification [of affected individuals], Call Center, Credit Monitoring and Identity Theft Monitoring.



DISCLAIMER: This document is provided by NASPO ValuePoint and is for informational purposes only. While NASPO ValuePoint has worked to ensure the validity of the information provided, the user should not rely solely on the information contained in this document. Official records are maintained by the procurement office of the state that led the solicitation and should be reviewed prior to making any decision.



SUPPLIERS RECOMMENDED FOR AWARD

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		

PRICING:

Pricing shall remain firm through the initial term of the Master Agreement. Customers may negotiate deeper discounts. A Purchasing Entity may customize services ordered from any of the awarded Categories by working with the Contractor to develop a Statement of Work for each order. The Purchasing Entity may elect to use a limited selection of services rather than all services available under any of the awarded Categories.

PROCUREMENT BACKGROUND:

The NASPO ValuePoint Management Board approved conducting a re-solicitation for Cybersecurity and Information Security Services. The lead state, along with a multi-state sourcing team, developed a solicitation, publicly released it, and evaluated the proposal responses. The contract awards allow state and local government end users to access the Cybersecurity and Information Security Services products and services.

STATES ON SOURCING TEAM:

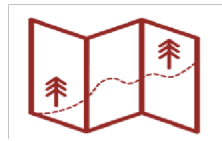
- ★ Idaho – Lead State
- ★ California
- ★ Oregon
- ★ Texas



SOLICITATION INFORMATION:

Type: Request for Proposals (RFP)
 Solicitation Number: RFP928
 Date Released: May 2, 2025
 Date Closed: June 26, 2025
 Amendments: 2
 Pre-Proposal Conference: May 12, 2025 (Supplier Attendance: 136)

DISCLAIMER: This document is provided by NASPO ValuePoint and is for informational purposes only. While NASPO ValuePoint has worked to ensure the validity of the information provided, the user should not rely solely on the information contained in this document. Official records are maintained by the procurement office of the state that led the solicitation and should be reviewed prior to making any decision.



<u>PUBLIC POSTING OF SOLICITATION:</u> Website Posted On: State of Idaho Posting Link: Cybersecurity and Information Security Services Event Days Publicly Posted: 55	<u>PUBLIC OPENING</u> Sealed proposals were opened by the lead state following the closing date. 
<u>VENDOR RESPONSES:</u> 58 proposals were received.	<u>EVALUATIONS:</u> Virtual evaluation meetings were completed on August 7, 2025.
<u>EVALUATION CRITERIA:</u> Proposals meeting or exceeding the Mandatory Requirements were evaluated as follows: 1. Initial Responsiveness Evaluation 2. Technical Criteria Evaluation 3. Cost Evaluation	
<u>DETERMINING NUMBER OF AWARDS:</u> The solicitation allowed for multiple awards to be made by Category. The list of Offerors in each Category met all solicitation Mandatory Requirements, agreed to and signed letters holding their pricing firm through the initial term of the Master Agreement, and met the RFP award criteria of receiving a minimum of 350 points in the Category they were recommended for award in. • Category 1 - Risk Assessment and Mitigation Services – 10 Awards • Category 2 - Incident Response Services – 5 Awards • Category 3 - Breach Coach Services – 4 Awards • Category 4 – Notification and Credit Monitoring Services – 2 Awards	

DISCLAIMER: This document is provided by NASPO ValuePoint and is for informational purposes only. While NASPO ValuePoint has worked to ensure the validity of the information provided, the user should not rely solely on the information contained in this document. Official records are maintained by the procurement office of the state that led the solicitation and should be reviewed prior to making any decision.