Attachment 07 Amendment 2
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: Infosys Public Services, Inc.
B. Primary Business Address: 700 King Farm Boulevard, Suite 200, Rockville, MD 20850
C. Federal Tax Identification Number: 27-1122707
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.

Infosys Response:

www.infosyspublicservices.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.

Infosys Response:

Infosys Public Services, Inc. (IPS), a wholly owned subsidiary of Infosys Limited, was incorporated on October 9, 2009, in Delaware USA, and is currently headquartered in Rockville, Maryland. The company was created to specifically serve public sector (federal, state and local government organizations) organizations in North America, delivering cutting-edge digital transformation, consulting, and technology services tailored to the unique needs of government agencies. IPS has not been involved in any material acquisitions or mergers.

Infosys Limited, the parent company, was founded in 1981 and is a global leader in next-generation digital services and consulting. Over the past four decades, Infosys has grown from a startup with a capital of $250 to a multinational corporation with over 323,000 employees and FY25 revenues of $19.3 billion.

We also confirm that IPS has not been involved in any material acquisitions or mergers.

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

Infosys Response:

Infosys Public Services has 498 employees.

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

Infosys Response:

Infosys Public Services, Inc. is a wholly owned subsidiary of Infosys Limited.

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.

Infosys Response:

Infosys Public Services has no such litigations.

IV. PROPOSAL CONTACT

(ME) The Contractor must provide a Contract Manager as the single point of contact for management of the NASPO ValuePoint Master Agreement (include: Name, Title, Email, Phone Number), administered by the state of Idaho. **The Contract Manager must have experience of managing contracts for services similar to those required in this RFP. Describe in detail your proposed Contract Manager's experience managing contracts for services like those required in this RFP. Provide a detailed resume for the proposed Contract Manager.** Additionally, provide the name, phone number, email address, and work hours of the person who will act as Contract Manager if you are awarded a Master Agreement. The Proposal Contact must be able to respond timely to communications from the Lead State. Offeror must, within 24 hours, notify the Lead State of any change to Offeror's Proposal Contact.

Infosys Response:

We are pleased to introduce Mr. Vijay Ravichandran, the IPS National Practice Lead for Health and Human Services, as the Contract Manager for this engagement. With over 25 years of industry experience, he has successfully led numerous large-scale projects similar to this one. Mr. Ravichandran will also serve as the single point of contact for the State. His resume is below.

Name:	Vijay Ravichandran	Title:	National practice lead (Health and Human Services)
Email Address:	vijay_ravichandran@infosys.com	**Phone Number:**	(508) 740-3811

Total years of professional experience:	25	**Years of experience as a Contract Manager:**	10
Summary of Relevant Experience:			
Vijay has over 25 years of experience in managing and delivering large IT portfolios. He's the national practice lead for Health and Human Services at Infosys and is responsible for strategic accounts from inception to delivery. He is the Account lead for all Pennsylvania state and local engagements and is currently also managing the Connecticut HHS and South Carolina DHHS account. Prior to being an Account Lead, Vijay was Program Partner/Manager, managing relationships with CXO's, strategic planning, scope control, Risk management, project budgets, and overall delivery.			
Education & Current Professional Licenses:			
Education Master of Science in Industrial Engineering, Oklahoma State			
Evidence of Experience			
Project 1 **Project Title:** South Carolina DHHS **Duration (start date and end date):** July 2021 – Till date **Role:** Account Lead **Responsibilities:** Overall Program Management | Stakeholder management | Schedule and deliverables | Governance | Risk management | Cost tracking control and budgeting **Project 2** **Project Title:** Washington D.C Health Benefit Exchange and Social Programs **Duration (start date and end date):** May 2013 – June 2017 **Role:** Program Manager **Responsibilities:** Overall Program Management | Stakeholder management | Schedule and deliverables | Governance | Risk management | Cost tracking control and budgeting			
Work Hours			
9 a.m. to 5 p.m. Mountain Time			

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.

Infosys Response:

Infosys Public Services brings extensive experience delivering secure, scalable, and compliant cybersecurity solutions to public sector clients across North America. Our technical capabilities span the full lifecycle of information security services, including:

1. **Risk Assessment and Mitigation**
   - Vulnerability assessments and penetration testing

- Privacy impact assessments and internal control evaluations
- Policy and governance reviews aligned with NIST, ISO/IEC 27001, and CIS benchmarks

2. **Event and Incident Management**
   - 24x7 Security Operations Center (SOC) support
   - Incident triage, containment, and root cause analysis
   - Threat intelligence integration and real-time alerting
   - Digital forensics and evidence preservation
3. **Breach Response and Breach Coach Services**
   - Coordination with legal and compliance teams
   - Stakeholder communication planning
   - Regulatory reporting and notification support
   - Post-incident reviews and lessons learned
4. **Security Architecture and Advisory**
   - Zero Trust architecture design and implementation
   - Cloud security posture management (CSPM)
   - Identity and Access Management (IAM) consulting
   - Secure DevOps and application security assessments
5. **Compliance and Governance**
   - Support for FedRAMP, CJIS, HIPAA, and CMMC frameworks
   - Policy development and audit readiness
   - GRC tool integration and automation
6. **Near-Shore Delivery Capabilities**
   - IPS offers secure near-shore delivery centers located in North America, while ensuring:
     - All data remains within U.S. jurisdiction
     - Real-time collaboration in U.S. time zones
     - Compliance with federal and state data residency requirements
     - Scalable, cost-effective support for surge and continuity needs

IPS is committed to delivering high-quality, standards-based cybersecurity services that meet the diverse needs of NASPO ValuePoint Participating Entities. Our technical approach is grounded in industry best practices, continuous innovation, and a deep understanding of public sector security requirements.

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.

Infosys Response:

Infosys is pleased to present its capabilities in delivering enterprise-scale **Risk Assessment and Mitigation Services**, backed by over a decade of experience supporting public sector agencies, Fortune 500 companies, and organizations operating in highly regulated industries such as healthcare, financial services, and energy.

Our approach is grounded in industry-leading frameworks, including **NIST SP 800-30**, **ISO/IEC 27005**, and **COSO ERM**, ensuring alignment with federal and state compliance mandates. These services are executed through our global network of cybersecurity professionals and strategically located **U.S.-based Cyber Defense Centers**, offering both scalability and localized support.

Infosys has a proven track record of delivering services that meet or exceed the scope and complexity outlined in state and federal RFPs. Our core competencies include:

- **Risk Identification and Analysis**
- **Threat Modeling and Vulnerability Assessments**
- **Business Impact Analysis (BIA)**
- **Mitigation Strategy Development**
- **Policy and Control Framework Reviews**
- **Implementation and Monitoring of Risk Controls**

We are confident in our ability to support our clients with tailored, high-impact risk management solutions that enhance resilience and ensure regulatory compliance.

Representative Engagements

Following are some relevant projects we have successfully executed in last five (5) years:

1. **Vendor Risk Assessment for a Major Insurance Company**
   - **Client**: UK-based insurance company
   - **Scope**: Risk assessments for 150+ IT and non-IT suppliers
   - **Services Provided**:
     - Vendor segmentation based on risk score
     - Enhanced security assessments
     - ISO 27001-aligned risk assessments
   - **Outcome**: Improved security posture across HR, finance, and claims departments
2. **Automated Asset-Based Risk Assessment for a Banking Client**
   - **Client**: Global banking and financial services company
   - **Scope**: Automation of IT risk assessments using RSA Archer
   - **Services Provided**:
     - Integration of security tools with RSA Archer
     - Auto-population of control responses
     - Workflow automation and compliance reporting
   - **Outcome**: Reduced assessment cycle from 6 months to 30 days
3. **Cloud Security Risk Assessment for a European Investment Firm:**
   - Client: European Investment Firm
   - Scope: Comprehensive cloud security posture assessment
   - Services Provided
     - Risk identification and mitigation planning
     - Strengthening of cloud-native security controls
   - **Outcome**: Enhanced cloud security and compliance readiness
4. **Electronic Procurement Solution (EPS) – Government of Canada (GC)**
   - **Client**: Public Services and Procurement Canada (PSPC)
   - **Scope**: Government-wide implementation serving all Canadian federal departments and agencies
   - **Services Provided**:
     - Infosys successfully delivered and continues to manage the **EPS (Electronic Procurement Solution)**, a bilingual SaaS platform supporting the full procurement lifecycle.
     - The solution includes **multi-cloud deployments** (SAP, Azure, AWS), an **Identity, Credential, and Access Management (ICAM)** system tailored to federal requirements, and a **Protected B**

compliant facility, which aligns with the security standards of **Controlled Unclassified Information** (CUI) and **Sensitive But Unclassified** (SBU) facilities in the US.
  - A dedicated **24x7x365 Security Operations Center (SOC)** ensures continuous monitoring and incident response.
  - The platform is subject to stringent federal security and privacy requirements, including risk assessments, vulnerability management, and compliance audits.

- **Risk Assessment and Mitigation Experience:**
  - Conducted comprehensive risk assessments across infrastructure, application, and data layers.
  - Implemented mitigation strategies aligned with **Government of Canada IT Security ITSG-33** standards which aligns with the **NIST 800-53** standard.
  - Delivered continuous risk monitoring, threat modeling, and compliance reporting to federal stakeholders.

- **Outcome:**
  - Enabled secure, scalable, and compliant procurement operations across all federal departments.
  - Strengthened Canada's digital procurement infrastructure with proactive risk management and mitigation.

- **(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.

Infosys Response:

Infosys offers a robust team of highly skilled professionals with deep expertise in risk assessment, cybersecurity, regulatory compliance, and business process optimization. Our personnel are carefully selected based on rigorous qualification standards and industry certifications to ensure alignment with the specific needs of public sector engagements.

The structure of our delivery teams is purpose-built to meet—and often exceed—the minimum qualifications and experience requirements outlined in the RFP. This ensures that our clients benefit from both strategic insight and hands-on technical proficiency throughout the engagement lifecycle.

1. Security/Technology Senior Analyst

Minimum Experience: 5+ years in cybersecurity, IT risk management, or technical security roles.

Key Qualifications:

- Proven experience in vulnerability assessments, penetration testing, and internal control evaluations.
- Strong analytical and troubleshooting skills with the ability to design and oversee technical deliverables.
- Experience with mainstream security frameworks (e.g., NIST, ISO 27001, CIS Controls).

Certifications (at least one required):

- Certified Information Systems Security Professional (CISSP)
- GIAC Penetration Tester (GPEN)
- GIAC Enterprise Vulnerability Assessor (GEVA)
- Certified Ethical Hacker (CEH)

2. Business Process / Risk Management Senior Consultant

Minimum Experience: 5+ years in business process analysis, enterprise risk management, or compliance consulting.

Key Qualifications:

- Deep understanding of regulatory environments (e.g., HIPAA, FISMA, GDPR, SOX).
- Ability to assess and redesign business processes in response to risk assessments.
- Skilled in facilitating workshops, stakeholder interviews, and policy reviews.

Certifications (at least one required):

- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified Regulatory and Compliance Professional (CRCP) – FINRA
- Certified in Risk and Information Systems Control (CRISC)

3. Project Manager

Minimum Experience: 5+ years in managing IT or risk-related projects, including scope, budget, and stakeholder communication.

Key Qualifications:

- Demonstrated success in managing multi-disciplinary teams and complex engagements.
- Strong understanding of risk management lifecycle and business continuity planning.
- Excellent communication and reporting skills.

Certifications (at least one required):

- Project Management Professional (PMP)
- Certified ScrumMaster (CSM)
- Agile Certified Practitioner (PMI-ACP)

Additional Areas of Specialization

Infosys also deploys subject matter experts (SMEs) with specialization in:

- Cloud Security and Compliance (e.g., AWS/Azure Security Certified)
- Data Privacy and Protection (e.g., CIPP/US, CIPM)
- Threat Intelligence and Incident Response
- Third-Party Risk Management and Contractual Risk Advisory

Commitment to Continuous Learning

Infosys is deeply committed to fostering a culture of continuous learning and professional development. We maintain a comprehensive internal training and certification program designed to ensure that all personnel remain current with emerging threats, evolving technologies, and dynamic regulatory requirements.

Our employees are actively encouraged and supported in pursuing advanced industry certifications and participating in relevant professional forums, conferences, and knowledge-sharing communities. This commitment ensures that our teams bring the most up-to-date expertise and best practices to every engagement.

- **(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.

Infosys Response:

Infosys is committed to delivering high-quality, secure, and timely Risk Assessment and Mitigation Services that are fully aligned with industry best practices and the specific requirements outlined in Section 2 of the

RFP. Our service delivery is governed by well-defined Service Level Agreements (SLAs) that emphasize responsiveness, accountability, and measurable value for each Participating Entity.

These SLAs are designed not only to ensure compliance and performance transparency but also to foster continuous improvement and stakeholder confidence throughout the engagement lifecycle.

Response Times and Service Commitments

Service Component	Infosys SLA Commitment
Acknowledgment of Service Request	Within 4 business hours
Initial Scoping and Planning Meeting	Within 2 business days
Risk Assessment Engagement Kickoff	Within 5 business days post-approval
Emergency Risk Response (e.g., breach)	Within 24 hours
Final Written Report Delivery	Within 5 business days post-engagement
Ad-hoc Consultations (e.g., third-party terms)	Within 3 business days of request

1. Roles and Responsibilities

Infosys (Contractor):

- Conduct comprehensive risk assessments leveraging industry-standard frameworks such as **NIST**, **ISO/IEC 27001**, and **COBIT**.
- Ensure encryption of all Non-Public Data at rest and in transit in accordance with **FIPS 140-2** or the most current **NIST** standards.
- Deliver actionable mitigation strategies and compliance assessments tailored to the Participating Entity's environment.
- Provide qualified and certified personnel as specified in **Section 2.3**, including but not limited to **CISSP**, **CISA**, **PMP**, and other relevant credentials.
- Maintain all data residency and security controls strictly within the **Continental United States**.
- Submit a comprehensive final report detailing risk statements, impact analysis, and prioritized mitigation recommendations.

Participating Entity:

- Provide timely access to relevant systems, personnel, and documentation necessary for the assessment.
- Clearly identify and classify data as **Public** or **Non-Public**.
- Define the engagement's scope, objectives, and timelines.
- Review deliverables and provide feedback within **three (3) business days** of receipt.

2. Quality Assurance and Monitoring

- **Internal Quality Assurance Reviews:** All deliverables undergo rigorous, multi-tiered quality reviews conducted by senior consultants and subject matter experts.
- **Performance Monitoring:** Infosys continuously tracks SLA compliance through internal dashboards and provides regular status updates to stakeholders.
- **Escalation Protocol:** Any delays or issues are escalated to Infosys engagement leadership within **48 hours** to ensure timely resolution.

3. Continuous Improvement and Flexibility

Infosys employs a **continuous improvement model**, integrating feedback from each engagement to refine methodologies and enhance service delivery. We offer **flexible engagement models** to accommodate the unique operational and strategic needs of each Participating Entity, including:

- Hybrid Delivery Models
- Co-Sourcing Arrangements

- Fully Managed Services

- **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.

Infosys Response:

Infosys offers a comprehensive cybersecurity portfolio that extends well beyond the standard Scope of Work outlined in the RFP. These value-added services are designed to deliver deeper threat insights, accelerated response capabilities, and enhanced cyber resilience for government and public sector entities. These services are available as optional enhancements. Near-shore capabilities from Canada are priced separately in Attachment 09. For other services, Infosys can provide specific pricing during negotiations with NASPO ValuePoint, the lead state, or participating states, based on interest.

1. Cyber Threat Intelligence (CTI) and Threat Hunting

Infosys provides proactive threat intelligence services that include:

- Real-time monitoring of global threat landscapes
- Sector-specific custom threat feeds
- Dark web surveillance for exposed credentials and sensitive data
- Threat hunting engagements to identify advanced persistent threats (APTs)

2. Security Architecture and Zero Trust Consulting

We support agencies in modernizing their security posture through:

- Design and implementation of Zero Trust frameworks
- Cloud-native security architecture assessments
- Identity and Access Management (IAM) evaluations
- Micro-segmentation strategies for enhanced network defense

3. AI-Driven Risk Analytics and Automation

Leveraging the Infosys Topaz AI platform, we offer:

- Predictive analytics to forecast risk exposure
- Automated control testing and compliance validation
- AI-based anomaly detection in user behavior and network traffic
- Executive dashboards and risk heatmaps for decision-making

4. Operational Technology (OT) and IoT Security

For agencies managing critical infrastructure, Infosys delivers:

- ICS/SCADA security assessments
- OT network segmentation and continuous monitoring
- Compliance with NIST SP 800-82 and ISA/IEC 62443
- Threat modeling for IoT ecosystems

5. Cybersecurity Maturity Assessments

We conduct in-depth evaluations using:

- NIST Cybersecurity Framework (CSF)
- Cybersecurity Maturity Model Certification (CMMC)
- ISO/IEC 27001 readiness assessments
- Customized roadmaps for maturity advancement

6. Third-Party and Supply Chain Risk Management

Infosys helps manage external risks through:

- Comprehensive third-party risk assessments and scoring
- Continuous monitoring of vendor security posture
- Contractual risk advisory and SLA enforcement
- Integration with GRC platforms for automated tracking

7. Security Awareness and Behavioral Engineering

To address the human element of cybersecurity, we provide:

- Role-based security awareness training
- Gamified learning modules and phishing simulations
- Behavioral analytics to assess training effectiveness
- Executive-level cyber risk workshops

8. Data Loss Prevention (DLP) and Insider Threat Programs

Our services include:

- DLP strategy development and tool implementation
- Insider threat detection using behavioral analytics
- Endpoint monitoring and data classification
- Policy enforcement and incident response playbooks

9. Cloud Security Posture Management (CSPM)

For hybrid and multi-cloud environments, Infosys offers:

- Cloud configuration audits and remediation
- Identity and entitlement management
- Continuous compliance monitoring (e.g., FedRAMP, CJIS)
- Automation of security controls and reporting

10. Red Team / Blue Team Exercises

We simulate real-world attack scenarios to test and strengthen defenses:

- Red team penetration testing and social engineering
- Blue team defense readiness assessments
- Purple team collaboration for iterative improvement
- Executive tabletop exercises for strategic preparedness

11. Near-Shore Cybersecurity Operations

- Infosys Public Services leverages secure near-shore delivery centers in North America to provide 24x7 cybersecurity monitoring, incident response, and compliance support. These centers operate in U.S. time zones, ensuring rapid response and alignment with public sector requirements. All data processed and stored through these operations will remain within U.S. borders and will be securely maintained in compliance with federal and state data residency requirements.

12. Near-Shore Agile Delivery Teams

- Our near-shore teams support agile project execution, enabling faster turnaround, reduced costs, and seamless collaboration with U.S.-based stakeholders. These teams are trained in public sector compliance and can be scaled on demand.

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.

Infosys Response:

Infosys brings over a decade of demonstrated expertise in delivering comprehensive **Incident Response Services** to global enterprises, government agencies, and organizations operating in highly regulated sectors such as healthcare, finance, and energy. Our Cybersecurity practice is a foundational pillar of the **Infosys Digital Trust** offering, supported by a global team of more than **4,000 cybersecurity professionals** across **50+ countries**.

Relevant Experience

Infosys has been delivering services comparable in scope and complexity to the **Category 2 Incident Response Services** for more than **five (5) years**. Our capabilities span the entire incident response lifecycle, including:

- Threat Detection and Analysis
- Incident Containment and Eradication
- Forensic Investigation and Root Cause Analysis
- Recovery and Restoration
- Post-Incident Reporting and Compliance Support

These services are delivered through our strategically located **Cyber Defense Centers (CDCs)** in the **United States, Europe, and Asia-Pacific**, ensuring **24x7x365 coverage** and rapid response capabilities.

Our approach is grounded in industry best practices and aligned with frameworks such as **NIST SP 800-61**, enabling us to deliver timely, effective, and compliant incident response support tailored to the needs of public sector entities.

Representative Engagements

Following are some relevant projects we have successfully executed in last five (5) years:

1. **U.S.-Based Financial Institution (Fortune 100 Company)**
   - Client: A U.S.-based financial institution
   - **Scope**: End-to-end incident response services including threat hunting, malware analysis, and breach containment.
   - **Size**: Over 50,000 endpoints and 10,000+ servers.
   - **Outcome**: Reduced mean time to detect (MTTD) by 40% and mean time to respond (MTTR) by 60% through automation and playbook-driven response.
2. **Global Pharmaceutical Company**
   - Client: A global pharmaceutical company
   - **Scope**: Managed detection and response (MDR), forensic investigation, and regulatory reporting (HIPAA, GDPR).
   - **Size**: Operations in 30+ countries with sensitive R&D and patient data.
   - **Outcome**: Successfully contained a ransomware attack within 4 hours, preserving critical IP and ensuring compliance with data breach notification laws.
3. **U.S. State Government Agency**
   - Client: A U.S. state government agency
   - **Scope**: Incident response readiness assessment, tabletop exercises, and real-time breach response support.
   - **Size**: Multi-agency environment with over 20,000 users.

- **Outcome**: Enhanced incident response maturity from Level 2 to Level 4 (NIST CSF scale) within 12 months.

4. Government of Canada – Electronic Procurement Solution

- Client: Public Services and Procurement Canada (PSPC)
- **Scope**: Incident response including threat detection, triage, containment, forensics and coordination with GC authorities (e.g., Canadian Centre for Cyber Security, Treasury Board of Canada).
- **Size**: Government wide SaaS platform supporting all federal departments, multi-cloud environment with thousands of users.
- **Outcome**:
  - Established incident detection SLAs and automated alerting integrated with SIEM and SOAR platforms.
  - Successfully mitigated targeted DDoS campaigns, multiple real world incidents with zero operational downtime and full incident documentation and reporting to GC central IT Security Authority.
  - All response procedures aligned with ITSG-33 and the GC's PBMM profile, similar to NIST Risk Management Framework.

Certifications and Framework Alignment

Infosys incident response teams hold industry-recognized certifications, including:

- Certified Information Systems Security Professional (CISSP)
- GIAC Certified Incident Handler (GCIH)
- GIAC Reverse Engineering Malware (GREM)
- Certified Ethical Hacker (CEH)
- Certified Information Security Manager (CISM)

Our methodologies align with leading frameworks such as **NIST SP 800-61**, **MITRE ATT&CK**, and **ISO/IEC 27035**.

- **(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.

Infosys Response:

Infosys ensures that all personnel assigned to deliver Category 2 – Incident Response Services are highly qualified, certified, and possess extensive experience in managing complex cybersecurity incidents across both public sector environments and diverse industry domains.

Our team structure and qualification standards are fully aligned with the minimum requirements specified in Section 3.9 of the Scope of Work. Personnel are selected based on their demonstrated expertise in incident response, forensic analysis, threat containment, and regulatory compliance. Many hold advanced certifications such as CISSP, CISA, GIAC, CEH, and GCFA, ensuring a high level of technical proficiency and adherence to industry best practices.

This commitment to excellence enables Infosys to deliver rapid, effective, and compliant incident response services tailored to the unique needs of each Participating Entity.

1. Forensics Incident Investigator

Minimum Experience: 5+ years in digital forensics, cybercrime investigation, or incident response.

***Key Qualifications**:*

- Expertise in identifying, collecting, preserving, and analyzing digital evidence using industry-standard forensic tools and methodologies.
- Experience with chain-of-custody protocols and legally admissible evidence handling.

Certifications (at least one required):

- GIAC Certified Forensic Analyst (GCFA)
- SANS Certified Incident Handler (GCIH)
- EnCase Certified Examiner (EnCE)
- Certified Computer Examiner (CCE)

Specializations:

- Malware reverse engineering
- Insider threat investigations
- Cloud and mobile forensics

2. Business Process / Risk Management Senior Consultant

***Minimum Experience**:* 5+ years in enterprise risk management, compliance, or cybersecurity governance.

***Key Qualifications**:*

- Deep understanding of regulatory frameworks (e.g., HIPAA, FISMA, GDPR).
- Ability to assess and redesign business processes in response to security incidents.
- Skilled in stakeholder engagement and policy development.

Certifications (at least one required):

- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified Regulatory and Compliance Professional (CRCP – FINRA)
- Certified in Risk and Information Systems Control (CRISC)

3. Project Manager

Minimum Experience: 5+ years in managing cybersecurity or incident response projects.

Key Qualifications:

- Demonstrated experience in managing incident response engagements, including scoping, resource allocation, and budget tracking.
- Strong communication and reporting skills, with the ability to interface with executive leadership and technical teams.

Certifications (at least one required):

- Project Management Professional (PMP)
- Certified ScrumMaster (CSM)
- Agile Certified Practitioner (PMI-ACP)

Additional Areas of Specialization

Infosys also deploys specialized personnel with expertise in:

- Threat Intelligence and Threat Hunting
- Security Operations Center (SOC) Management
- Cloud Incident Response (AWS, Azure, GCP)
- Industrial Control Systems (ICS) and SCADA Security
- MITRE ATT&CK-based detection engineering

Commitment to Excellence

Infosys is committed to maintaining the highest standards of excellence in the delivery of cybersecurity services. We foster a continuous learning culture, requiring all cybersecurity personnel to participate in ongoing training and maintain current certifications to stay ahead of evolving threats, technologies, and regulatory requirements.

Our **Cyber Defense Centers (CDCs)** operate **24x7x365** and are staffed by professionals who are not only technically proficient but also trained in the **legal, regulatory, and communication aspects** of incident response. This multidisciplinary expertise ensures that our teams can respond swiftly, effectively, and in full compliance with applicable laws and standards—while maintaining clear and accurate communication with stakeholders throughout the incident lifecycle.

- **(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.

Infosys Response:

Infosys Public Services (IPS) maintains rigorous standards for the recruitment, training, and performance of Customer Service Representatives (CSRs) to ensure exceptional service delivery aligned with the expectations of NASPO ValuePoint and its Participating Entities.

Minimum Qualifications

All CSRs assigned to the NASPO ValuePoint Master Agreement will meet or exceed the following baseline qualifications:

- High school diploma or equivalent (associate or bachelor's degree preferred)
- Minimum of 1–2 years of experience in a customer-facing or call center environment
- Demonstrated proficiency in verbal and written communication in English
- Strong interpersonal skills and a customer-first mindset
- Familiarity with CRM systems, ticketing tools, and call center technologies
- Ability to handle high call volumes and resolve inquiries efficiently and professionally

Training and Certification

IPS ensures that all CSRs undergo a structured onboarding and continuous training program, which includes:

- **Customer Service Excellence Training**: Focused on empathy, active listening, conflict resolution, and call etiquette
- **Communication Skills Development**: Emphasis on clarity, tone, and professionalism in English
- **System and Process Training**: Hands-on training on client-specific platforms, knowledge bases, and escalation procedures
- **Compliance and Security Awareness**: Training on data privacy, confidentiality, and applicable regulatory standards (e.g., HIPAA, CJIS, as applicable)
- **Quality Assurance and Performance Monitoring**: Ongoing coaching and feedback based on call audits and customer satisfaction metrics

Near-Shore Support (if required)

Where appropriate, IPS can provide near-shore customer service operations from secure U.S.-based or near-shore centers. These centers:

- Operate in U.S. time zones for real-time responsiveness
- Ensure that all customer data remains within U.S. jurisdiction
- Are staffed with English-fluent representatives trained to meet public sector service expectations

IPS is committed to delivering high-quality, responsive, and compliant customer service experience to all NASPO ValuePoint stakeholders.

- **(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.

Infosys Response:

Infosys is committed to delivering **rapid, reliable, and secure Incident Response Services** that align with the **State of Idaho's expectations** and recognized **industry best practices**. Our approach is designed to ensure swift engagement, effective threat containment, and transparent communication throughout the incident lifecycle.

Our **Service Level Agreements (SLAs)** are structured to guarantee:

- **Timely activation** of response teams
- **Efficient containment and eradication** of threats
- **Clear, consistent communication** with stakeholders at every stage

This commitment ensures that the State receives not only technical excellence but also operational transparency and accountability during critical cybersecurity events.

1. Response Times

Service Component	Infosys SLA Commitment
Acknowledgment of Service Request	Within 1 hour of receipt
Incident Manager Response	Within 4 hours (as per RFP Section 3.1.3)
On-Site Presence (if required)	Within 1 business day (Section 3.1.4)
Emergency Containment Initiation	Within 2 hours of confirmed incident
Final Incident Report Delivery	Within 1 week post-engagement (Section 3.7.2.2)

2. Roles and Responsibilities

Contractor Responsibilities (Infosys)

Infosys will fulfill the following responsibilities to ensure effective and compliant delivery of Category 2 – Incident Response Services:

- **Incident Management**: Assign a certified Incident Manager to oversee and coordinate all response activities from initiation through resolution.
- **Containment & Eradication**: Implement both short-term and long-term containment strategies, perform system backups, and execute malware removal procedures.
- **Forensics & Analysis**: Conduct forensic investigations that are legally admissible, including comprehensive root cause analysis to support remediation and compliance efforts.
- **Reporting**: Provide incremental updates and a final incident report, including executive summaries, technical findings, and recommendations.
- **Secure Communication**: Ensure all communications are encrypted and restricted to authorized personnel, in accordance with applicable security protocols.
- **Law Enforcement Coordination**: Support coordination with law enforcement agencies as directed by the Participating Entity, ensuring proper chain-of-custody and documentation.

3. Participating Entity Responsibilities

To facilitate a successful engagement, the Participating Entity will be responsible for:

- **Timely Notification**: Promptly notifying Infosys of any incidents or triggering events upon identification.
- **Access Provisioning**: Providing necessary access to affected systems, logs, and personnel to support investigation and response efforts.
- **Scope Definition**: Collaborating with Infosys to define the scope, objectives, and classification of the incident.
- **Feedback & Review**: Reviewing deliverables and providing feedback within **three (3) business days** to support timely resolution and closure.

4. Quality Assurance and Escalation

Infosys maintains a rigorous quality assurance and escalation framework to ensure service excellence:

- **Quality Assurance Reviews**: All deliverables undergo internal quality reviews conducted by senior cybersecurity professionals and subject matter experts.
- **Escalation Protocol**: Any delays or unresolved issues are escalated to the Infosys Cybersecurity Practice Lead within **24 hours** for expedited resolution.
- **Regulatory Compliance**: All services are delivered in accordance with **NIST SP 800-61**, **ISO/IEC 27035**, and applicable **state and federal regulations**.

5. 24x7 Support

Infosys provides **24x7x365 support** through its **U.S.-based Cyber Defense Center**. A dedicated **toll-free hotline** and **secure email channel** are available for urgent incident reporting, escalation, and real-time coordination.

- **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.

Infosys Response:

In addition to the core services outlined in the Scope of Work (SOW), Infosys Public Services offers a suite of **value-added services** designed to enhance the effectiveness, speed, and resilience of incident response operations. These services are available as optional enhancements. Near-shore capabilities from Canada are priced separately in Attachment 09. For other services, Infosys can provide specific pricing during negotiations with NASPO ValuePoint, the lead state, or participating states, based on interest.

1. Cyber Threat Intelligence (CTI) and Threat Hunting

- Real-time monitoring of global threat landscapes
- Sector-specific threat intelligence feeds
- Dark web surveillance for exposed credentials and sensitive data
- Proactive threat hunting to identify advanced persistent threats (APTs)

2. Red Team / Blue Team / Purple Team Exercises

- Simulated attack scenarios to test organizational defenses
- Blue team readiness assessments and response drills
- Purple team collaboration for continuous improvement
- Executive tabletop exercises for leadership preparedness

3. Forensic Readiness and Legal Advisory

- Pre-incident forensic readiness assessments
- Chain-of-custody documentation and evidence preservation protocols
- Legal advisory support for regulatory and law enforcement coordination

4. AI-Driven Anomaly Detection and Risk Analytics

- Behavioral analytics using Infosys Topaz AI platform
- Predictive modeling to identify high-risk assets and users
- Automated risk scoring and visualization dashboards

5. **Insider Threat Detection and Data Loss Prevention (DLP)**
   - Behavioral monitoring for insider threat indicators
   - DLP strategy development and tool implementation
   - Endpoint monitoring and policy enforcement
6. **Cloud Security Posture Management (CSPM)**
   - Continuous monitoring of cloud environments for misconfigurations
   - Compliance checks against FedRAMP, CJIS, and other frameworks
   - Automated remediation guidance and reporting
7. **Security Awareness and Behavioral Engineering**
   - Role-based training and phishing simulations
   - Gamified learning modules to improve user engagement
   - Behavioral analytics to measure training effectiveness
8. **Third-Party and Supply Chain Risk Management**
   - Vendor risk assessments and scoring
   - Continuous monitoring of third-party security posture
   - Integration with GRC platforms for automated tracking
9. **Near-Shore Delivery Capabilities**
   - Infosys Public Services also offers secure near-shore delivery capabilities to support incident response and cybersecurity operations. These include U.S.-based and near-shore security operations centers that provide 24x7 monitoring, threat detection, and compliance support. All data is securely processed and stored within U.S. borders, ensuring full alignment with federal and state data residency requirements.
   - Near-shore agile teams operate in U.S. time zones, enabling faster response times, reduced costs, and seamless collaboration with public sector stakeholders. These teams are trained in regulatory compliance and can be rapidly scaled to meet surge demands or support continuity during critical incidents.

These services are designed to complement and extend the core incident response capabilities, providing Participating Entities with a more proactive, resilient, and intelligence-driven cybersecurity posture.

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.

Infosys Response:

Infosys brings over a decade of proven experience in delivering comprehensive Breach Coach Services to both global enterprises and public sector organizations. Our services span the entire breach lifecycle—from initial detection and containment to regulatory compliance, stakeholder communication, and post-incident remediation.

We have successfully supported clients across a wide range of industries, including government, healthcare, financial services, and manufacturing, helping them navigate complex breach scenarios with precision, discretion, and full regulatory alignment. Our multidisciplinary approach ensures that legal, technical, and operational considerations are addressed cohesively, enabling clients to respond effectively while minimizing risk and reputational impact.

Experience Overview – Breach Coach Services

Infosys' **Breach Coach Services** are designed to provide both strategic guidance and operational support throughout the lifecycle of a cybersecurity incident. Our multidisciplinary approach ensures that clients receive timely, coordinated, and compliant support during high-pressure breach scenarios.

Our services include:

- **Incident Investigation & Forensics:** Identification of the breach origin, scope, and impact using **legally admissible forensic methodologies**, ensuring evidence and integrity for potential legal or regulatory proceedings.
- **Regulatory Compliance Advisory:** Expert guidance on breach notification obligations under frameworks such as **HIPAA, GDPR, CCPA, and FISMA**, including coordination with internal legal counsel and external regulatory bodies.
- **Consumer & Business Notification Strategy:** Development of tailored communication plans for affected individuals, regulatory agencies, business partners, and media outlets, ensuring transparency and compliance with notification timelines.
- **Crisis Management:** Coordination across internal stakeholders, including **Legal, IT, HR, and Public Relations**—as well as external partners such as **law enforcement and forensic experts**, to ensure a unified and effective response.
- **Post-Breach Remediation:** Delivery of actionable recommendations for **policy updates, control enhancements, and staff training** to strengthen the organization's security posture and reduce the likelihood of recurrence.

Representative Engagements

Following are some relevant projects we have successfully executed in last five (5) years:

1. **Global Beverage Manufacturer – Data Breach Response and Risk Management**
   - **Client:** A global beverage manufacturer
   - **Scope**: Managed security services and breach response for 80,000+ users
   - **Services Provided**:
     - Consolidated fragmented security infrastructure
     - Enabled early detection and automated incident response
     - Supported breach containment and regulatory reporting
   - **Outcome**: Protected sensitive data, reduced breach impact, and improved compliance posture
2. **Strategic Partnership with Sygnia – High-End Breach Advisory Services**
   - **Client:** Sygnia Cybersecurity Services
   - **Scope:** Breach response and advisory services for Fortune 500 clients
   - **Services Provided:**
     - Threat posture assessments and breach response planning
     - Advanced threat hunting and forensic analysis
     - Legal and regulatory advisory during breach events
   - **Outcome**: Accelerated breach containment and improved resilience
3. **Government of Canada – Electronic Procurement Solution (EPS)**

- **Client**: Public Services and Procurement Canada (PSPC)
- **Scope**: Government-wide SaaS platform with Protected B compliance
- **Services Provided**:
  - 24x7x365 Security Operations Center (SOC)
  - Risk assessments and breach readiness aligned with federal standards
  - Incident response planning and secure communication protocols
- **Outcome**: Enabled secure procurement operations across all federal departments with proactive breach readiness and compliance

Breach Lifecycle Expertise

Infosys brings deep, hands-on expertise across the full breach lifecycle, enabling a structured and compliant response to cybersecurity incidents. Our capabilities include:

- **Detection & Investigation:** Deployment of advanced forensic tools and adherence to strict **chain-of-custody protocols** to ensure evidence integrity and support potential legal proceedings.
- **Regulatory Navigation:** In-depth knowledge of **U.S. and international breach notification laws**, including HIPAA, GDPR, CCPA, and FISMA, ensuring timely and accurate compliance with all applicable regulations.
- **Communication Strategy:** Development of clear, audience-specific communication materials, including **regulatory and consumer notifications**, frequently asked questions (FAQs), and **media statements**, to support transparency and trust.
- **Remediation Planning:** Execution of **root cause analysis**, redesign of affected controls, and delivery of targeted **security awareness training** to prevent recurrence and strengthen organizational resilience.

- **(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.

Infosys Response:

Infosys ensures that all Breach Response Specialists assigned to Category 3 – Breach Coach Services are highly qualified professionals with deep expertise in cybersecurity incident response, regulatory compliance, and crisis communication.

Our Breach Coaches are specifically trained to guide Participating Entities through the entire breach lifecycle—from initial detection and containment to regulatory reporting, stakeholder communication, and post-incident remediation. They bring a multidisciplinary perspective that balances technical precision with legal and reputational considerations.

By leveraging proven methodologies and aligning with applicable federal and state regulations, our Breach Coaches help minimize operational disruption and reputational impact while ensuring full compliance throughout the response process.

Minimum Experience and Qualifications (Aligned with RFP Section 4.3.1)

Experience:

- Minimum of **5+ years** of professional experience in breach response, incident management, or cybersecurity consulting.
- Proven track record of assisting organizations in navigating complex data breaches, including multi-jurisdictional regulatory environments.

Core Competencies:

- Expertise in isolating affected data and systems
- Knowledge of breach notification laws (e.g., HIPAA, GDPR, CCPA, FISMA)
- Experience coordinating with legal counsel, regulators, and law enforcement
- Ability to manage crisis communications and stakeholder engagement
- Development of incident response plans and cybersecurity awareness programs

Required Certifications and Specializations

Infosys Breach Coaches typically hold one or more of the following certifications:

- GIAC Certified Incident Handler (GCIH)
- EC-Council Certified Incident Handler (ECIH)
- EnCase Certified Examiner (EnCE)
- Certified Information Privacy Professional (CIPP/US or CIPP/E)
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified in Risk and Information Systems Control (CRISC)

Specializations:

- Regulatory compliance and breach notification strategy
- Legal and ethical advisory during breach events
- Crisis management and public relations coordination
- Forensic readiness and evidence preservation
- Post-breach remediation and policy development

Operational Readiness

Infosys operates a fully staffed, 24x7x365 Cyber Defense Center (CDC), equipped with experienced incident response specialists and certified Breach Coaches who can be rapidly deployed in response to a Triggering Event.

Our Breach Coaches are trained and prepared to:

- **Respond within two (2) business days** of a formal request, in accordance with **RFP Section 4.1.3**
- **Be available for on-site support within one (1) business day**, if required, as specified in **RFP Section 4.1.4**
- **Collaborate seamlessly with internal and external stakeholders,** including legal, IT, communications, and law enforcement, to ensure a coordinated and compliant breach response

This operational readiness ensures that Participating Entities receive immediate, expert support to manage incidents effectively and minimize impact.

- **(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.

Infosys Response:

Infosys is committed to delivering **timely, expert-level Breach Coach Services** that support Participating Entities in effectively managing and mitigating the impact of data breaches. Our approach is grounded in industry best practices and tailored to meet the unique needs of public sector organizations.

Our **Service Level Agreements (SLAs)** are structured to ensure:

- **Rapid response** to triggering events
- **Full compliance** with applicable regulatory requirements

- **Clear and effective communication** throughout the breach lifecycle

This commitment ensures that Participating Entities receive the guidance and support necessary to navigate breach events with confidence, transparency, and operational continuity.

1. **Response Times**

Service Component	Infosys SLA Commitment
Acknowledgment of Service Request	Within 2 business hours
Breach Coach Initial Response	Within 2 business days (per RFP Section 4.1.3)
On-Site Presence (if required)	Within 1 business day (Section 4.1.4)
Notification Strategy Consultation	Within 24 hours of request
Final Breach Report Delivery	Within 5 business days post-engagement or as agreed

2. **Roles and Responsibilities**

Contractor Responsibilities (Infosys)

Infosys will provide comprehensive Breach Coach Services in alignment with the Scope of Work. Our responsibilities include:

- **Assigning a Qualified Breach Coach:** A certified and experienced breach response specialist will be designated as the primary point of contact to lead and coordinate all breach-related activities.
- **Coordinating Incident Response:** Collaborate with the Participating Entity's internal teams and third-party vendors to manage the breach lifecycle, ensuring a unified and efficient response.
- **Regulatory Guidance:** Provide expert advisory on applicable breach notification laws and compliance requirements, including federal and state regulations.
- **Communication Strategy:** Assist in drafting and reviewing communications for affected individuals, regulatory bodies, and media outlets to ensure clarity, accuracy, and compliance.
- **Documentation and Reporting:** Maintain secure, auditable records of all actions taken and deliver comprehensive post-incident reports, including executive summaries and technical findings.
- **Confidentiality and Security:** Ensure all communications and data handling are conducted through secure, encrypted channels, with access limited to authorized personnel.

Participating Entity Responsibilities

To ensure a coordinated and effective breach response, the Participating Entity will:

- **Timely Notification:** Notify Infosys of any Triggering Event as soon as it is identified.
- **Access and Information Sharing:** Provide timely access to relevant systems, personnel, and documentation necessary to support investigation and response efforts.
- **Stakeholder Coordination:** Designate internal points of contact across Legal, IT, HR, and Communications to facilitate cross-functional collaboration.
- **Review and Approval:** Review and approve communication drafts and reports in a timely manner to meet regulatory notification deadlines.

3. **Quality Assurance and Escalation**

Infosys maintains a robust quality assurance and escalation framework to ensure service excellence:

- **Quality Assurance Reviews:** All deliverables are reviewed by senior breach response experts to ensure accuracy, completeness, and alignment with best practices.
- **Escalation Protocol:** Any delays or unresolved issues are escalated to the Infosys Cybersecurity Practice Lead within **24 hours** for prompt resolution.
- **Compliance Alignment:** All services are delivered in accordance with **NIST**, **ISO/IEC 27035**, and applicable **federal and state breach notification laws**.

4. **24x7 Availability**

Infosys operates a **24x7x365 Cyber Defense Center (CDC)** staffed with breach response specialists and incident managers. This ensures continuous availability and immediate support for urgent breach events, enabling rapid mobilization of Breach Coach Services at any time.

- **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.

Infosys Response:

In addition to the core services outlined in the Scope of Work (SOW), Infosys Public Services offers a range of value-added services designed to enhance the effectiveness, speed, and resilience of breach response efforts. These optional enhancements are not currently priced in Attachment 09. However, Infosys can provide pricing for specific services during negotiations with NASPO ValuePoint, the lead state, or participating states, based on interest.

1. **Breach Simulation and Tabletop Exercises**
   - Customized breach scenarios to test organizational readiness
   - Executive-level tabletop exercises to evaluate decision-making and communication protocols
   - Post-exercise reports with actionable recommendations
2. **Forensic Readiness Assessments**
   - Pre-incident evaluations to ensure systems, policies, and teams are prepared to support legally defensible investigations
   - Chain-of-custody planning and evidence handling protocols
3. **Regulatory and Legal Advisory Support**
   - Access to breach response specialists with expertise in HIPAA, GDPR, CCPA, FISMA, and state-specific laws
   - Coordination with legal counsel to ensure compliance and reduce liability
4. **Executive and Board-Level Briefings**
   - Tailored briefings to inform leadership on breach impact, response strategy, and risk mitigation
   - Support for public statements and regulatory disclosures
5. **Post-Breach Risk Assessments and Control Enhancements**
   - Root cause analysis and remediation planning
   - Recommendations for policy updates, control redesign, and staff training
6. **Behavioral Analytics and Insider Threat Detection**
   - Monitoring for anomalous user behavior before and after a breach
   - Integration with existing SIEM and DLP tools for enhanced visibility
7. **Secure Communication and Collaboration Platforms**
   - Deployment of encrypted communication channels for breach response coordination
   - Secure document sharing and audit logging

These value-added services are designed to provide Participating Entities with a more proactive, resilient, and legally sound approach to breach response and recovery.

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

- **(ME) Category 4 – Offeror's Experience. Describe your company's experience** demonstrating that your company has a minimum of five (5) years of experience providing services similar in scope and size to the Category 4 Notification and Credit Monitoring Services required in section Attachment 02, Scope of Work. Provide specific examples that illustrate the specific services furnished and the size, composition, etc. of the entities for whom you have provided services that you are using to demonstrate that your experience meets this minimum requirement.
- **(ME) Category 4 Identity Restoration Personnel – Experience and Qualifications.** All identity restoration personnel must be highly trained, have excellent customer service skills, and be able to communicate clearly in English. **Describe in detail the minimum experience, qualifications and training** you will require for identity restoration representatives servicing the NASPO ValuePoint Master Agreement.
- **(ME) Category 4 Call Center Customer Service Representatives – Qualifications.** All call center customer service representatives must have excellent customer service skills and be able to communicate clearly in English. **Describe in detail the minimum qualifications and training** for call center customer service representatives to be used in servicing the NASPO ValuePoint Master Agreement.
- **(ME) SLA's.** Describe your company's SLA's surrounding Category 4 Services. Include response times, responsibilities of both the Contractor and Participating Entity and any other relevant information surrounding the levels of service.
- **Value-Added Services.** Describe any services related to Category 4, including Identity Theft Insurance, that were not included in the SOW that your company can offer. Prices for any Value-Added Services must be detailed in your response to Attachment 09.

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.

Infosys Response:

Infosys Public Services is committed to delivering the majority of services under the Master Agreement directly through its internal teams. However, to ensure **flexibility, scalability, and access to specialized expertise**, Infosys may engage **pre-approved subcontractors** for specific tasks, subject to **prior written approval** from the Lead State or Participating Entity.

1. Scope and Categories of Subcontractor Use

If subcontractors are utilized, they will be engaged selectively and strategically in the following service categories:

- **Category 1: Risk Assessment and Mitigation Services**
  For specialized compliance audits, penetration testing, or sector-specific risk assessments.
- **Category 2: Incident Response Services**
  For rapid deployment of forensic experts, localized response teams, or surge capacity during high-severity incidents.
- **Category 3: Breach Coach Services**
  For specialized legal, regulatory, and crisis communication support.

2. Qualifications and Experience of Subcontractors

All proposed subcontractors will meet or exceed the minimum qualifications outlined in the RFP and will:

- Possess a minimum of five (5) years of domain-specific experience
- Hold relevant industry certifications such as CISSP, CISA, CEH, GIAC, PMP
- Demonstrate a strong track record of performance in public sector or regulated environments
- Align with Infosys' standards for quality, security, and compliance

Infosys applies a rigorous vetting and onboarding process to ensure subcontractors uphold the same standards of excellence expected from our internal teams.

3. Compliance and Accountability

- All subcontractors will be contractually required to comply with the same **security, confidentiality, and insurance requirements** as Infosys.
- Infosys will retain **full responsibility** for the performance, quality, and compliance of all subcontracted work.
- No subcontractor will be engaged without **prior written approval** from the Lead State or Participating Entity.

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.

Infosys Response:

Infosys has a demonstrated track record of successfully delivering large-scale, multi-agency, and statewide digital transformation and cybersecurity initiatives. We have partnered with federal, state, and provincial governments across North America to modernize mission-critical systems, strengthen cybersecurity postures, and ensure compliance with evolving regulatory requirements.

Experience with Statewide and Consortium Contracts

Infosys has successfully executed contracts that reflect the scope and complexity outlined in Attachment 02 of the RFP, including:

- Risk Assessment and Mitigation Services

- Incident Response and Forensic Investigations
- Breach Coaching and Regulatory Advisory
- Notification and Identity Protection Services

These engagements have required:

- Coordination across multiple departments and agencies
- Integration with both legacy systems and modern cloud-native platforms
- Adherence to stringent federal and state-level data protection laws, including HIPAA, FISMA, and state-specific breach notification statutes

Our experience in managing complex, multi-stakeholder environments ensures that we are well-positioned to support the objectives of this Master Agreement with agility, accountability, and excellence.

Key Large-Scale Contracts

1. **Government of Canada – Electronic Procurement Solution (EPS)**

- **Client**: Public Services and Procurement Canada (PSPC)
- **Scope**: Government-wide SaaS platform for procurement lifecycle management
- **Duration**: 2018 – Present
- **Contract Value**: Approx. [redacted]
- **Highlights**:
  - Multi-cloud deployment (SAP, Azure, AWS)
  - Protected B compliance and 24x7x365 SOC
  - Risk assessments, breach readiness, and compliance with Canadian federal standards

2. **State of Rhode Island – Labor System Modernization**

- **Client**: Department of Labor and Training
- **Scope**: Modernization of unemployment insurance and workforce systems
- **Contract Value**: Approx. [redacted]
- **Highlights**:
  - Cloud-native platform with integrated fraud detection
  - Enhanced data privacy and compliance with federal labor regulations
  - Risk and compliance framework embedded in system design

3. **U.S. Federal Health Agency – Medicaid MMIS Modernization**

- **Scope**: Multi-state Medicaid Management Information System transformation
- **Contract Value**: Approx. [redacted]
- **Highlights**:
  - Modular, cloud-based MMIS platform
  - Real-time risk monitoring and compliance reporting
  - Delivered under CMS guidelines and state-specific mandates

Top 3 Largest Contracts in the Last 5 Years

Client	Contract Value	Program Name
U.S. Federal Health Agency	[redacted]	Medicaid MMIS Modernization
Government of Canada (PSPC)	[redacted]	Electronic Procurement Solution (EPS)
State of Rhode Island	[redacted]	Labor System Modernization

Key Capabilities Demonstrated

- **Multi-jurisdictional coordination** across federal and state agencies
- **Cybersecurity and privacy compliance** with NIST, HIPAA, FISMA, and ISO 27001
- **Scalable service delivery** through Infosys' global delivery model and U.S.-based Cyber Defense Centers

- **24x7x365 support** for incident response, breach management, and stakeholder communication

---

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

Infosys Response:

Infosys Public Services is committed to ensuring the successful adoption and utilization of the Master Agreement by eligible Participating Entities, including U.S. state governments, local agencies, and educational institutions. Our approach is grounded in **strategic engagement, public sector outreach, and thought leadership**, leveraging our existing relationships and experience to drive awareness and participation. Here are the key adoption drivers we plan to use:

1. Strategic Government Engagement

Infosys has long-standing relationships with numerous U.S. state and federal agencies through the successful delivery of large-scale digital transformation and cybersecurity programs. We will leverage these relationships to promote the Master Agreement as a streamlined procurement vehicle for cybersecurity and information security services.

- Direct engagement with state procurement and IT leadership through scheduled briefings, virtual meetings, and participation in state-led forums
- Collaboration with cooperative purchasing organizations such as **NASPO ValuePoint** and state procurement alliances to promote the agreement through established channels

2. Public Sector-Focused Outreach

To raise awareness and encourage participation, Infosys will implement a targeted outreach strategy that includes:

- Participation in public sector conferences and expos (e.g., **NASCIO**, **NIGP**, state-specific IT summits) to showcase the agreement's benefits and use cases
- Hosting webinars and educational sessions for procurement officers, CIOs, and CISOs to explain the scope of services, ordering process, and value proposition
- Launching a dedicated **Master Agreement landing page** on Infosys.com featuring:
  - Overview of available services
  - Case studies and success stories
  - Step-by-step guidance for Participating Entities

3. Thought Leadership and Visibility

Infosys will continue to invest in thought leadership to position the Master Agreement as a trusted resource for cybersecurity services:

- Publishing whitepapers and blogs on breach readiness, regulatory compliance, and digital trust in the public sector
- Issuing press releases and securing media coverage to highlight successful engagements under the Master Agreement
- Running targeted social media campaigns on platforms such as **LinkedIn** and **X (formerly Twitter)** to reach public sector stakeholders

4. Collaboration with State Procurement Networks

Infosys will actively collaborate with key procurement and IT associations to amplify awareness and adoption:

- Partnering with **NASPO ValuePoint** and other cooperative purchasing organizations to promote the agreement through their communication channels
- Engaging with state IT and procurement associations (e.g., **NASCIO**, **NASPO**, **NIGP**) through event sponsorships, conference participation, and content contributions

5. Success Story Amplification

To demonstrate the value and scalability of services offered under the Master Agreement, Infosys will highlight successful implementations such as:

- The Electronic Procurement Solution (EPS) for the Government of Canada
- Labor System Modernization for the State of Rhode Island

These case studies will be featured in outreach materials, presentations, and digital content.

6. Continuous Engagement and Feedback Loop

Infosys will maintain ongoing engagement with Participating Entities to ensure continuous improvement and alignment with evolving needs:

- **Quarterly Stakeholder Updates** to share performance metrics, new service offerings, and best practices
- **Feedback Mechanisms** to gather input from Participating Entities and refine service delivery and outreach strategies

---

- 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.

Infosys Response:

Infosys is committed to supporting the successful implementation and utilization of the Master Agreement through the development and maintenance of a **dedicated, secure, and user-friendly website**. This centralized portal will serve as a digital hub for Participating Entities, enabling them to access information, initiate service requests, and manage engagements efficiently and securely.

Key Features of the Dedicated Website

1. Customized Master Agreement Landing Page

- Overview of the Master Agreement scope, benefits, and service categories
- Eligibility criteria and participation guidelines
- Step-by-step instructions for initiating services

2. Participating Entity-Specific Dashboards

- Secure login for each Participating Entity
- Customized service catalogs and pricing based on the Participating Addendum
- Access to historical service requests, reports, and deliverables

3. Dynamic Price Lists

- Entity-specific pricing aligned with negotiated terms
- Downloadable rate cards and service descriptions
- Real-time updates reflecting amendments, renewals, or pricing adjustments

4. Online Ordering and Service Request Portal

- Digital intake forms for initiating services such as risk assessments, incident response, and breach coaching
- Workflow-enabled request tracking and status updates
- Integration with Infosys' internal service management systems for seamless delivery

5. Staff Contact Directory

- Dedicated points of contact for each service category (e.g., Risk Assessment, Incident Response, Breach Coach)

- Regional engagement managers and escalation contacts
- Live chat and callback request features for real-time support

6. **Resource Center**
   - Case studies, whitepapers, and FAQs
   - Regulatory updates and compliance toolkits
   - Training materials and onboarding guides for new Participating Entities
7. **Security and Accessibility**
   - Hosted in a **FedRAMP-compliant** environment to ensure data security
   - Designed to meet **ADA accessibility standards**
   - Multi-factor authentication and role-based access control for secure user management
8. **Performance and Feedback Tools**
   - Real-time SLA dashboards and service performance metrics
   - Feedback forms and satisfaction surveys
   - Downloadable quarterly performance reports

This portal will be continuously updated and maintained to ensure it remains a reliable, secure, and effective resource for all Participating Entities under the Master Agreement.

- 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.

Infosys Response:

Infosys Public Services is committed to the successful execution and long-term support of the Master Agreement through the deployment of a dedicated, multidisciplinary delivery team and a robust operational framework. Our approach ensures that all personnel are fully trained on the agreement's scope, pricing, and compliance requirements, and that Participating Entities receive consistent, high-quality service throughout the contract lifecycle. Following are the key components of our staffing and training approach:

1. **Dedicated Master Agreement Delivery Team**

Infosys will assign a specialized team responsible for managing and supporting all aspects of the Master Agreement. This team will include:

- **Program Director:** Senior executive accountable for overall contract governance, strategic alignment with the Lead State and Participating Entities, and performance reporting.
- **Contract Manager:** Oversees day-to-day administration of the Master Agreement, including documentation management, pricing compliance, and coordination of Participating Addenda.
- **Service Category Leads:** Subject matter experts for each of the four service categories (Risk Assessment, Incident Response, Breach Coach, Notification Services), responsible for technical delivery, quality assurance, and escalation management.
- **Regional Engagement Managers:** Serve as the primary point of contact for Participating Entities within their assigned regions, facilitating onboarding, service requests, and ongoing relationship management.
- **Security and Compliance Analysts:** Ensure adherence to data protection standards (e.g., FIPS 140-2, NIST 800-53, HIPAA), conduct internal audits, and support incident response readiness in accordance with Section 2.1.1 of the RFP.
- **Technical Support and Operations Staff:** Provide backend support for the dedicated website, service intake, SLA dashboards, and documentation repositories.

2. **Training and Knowledge Enablement**

Infosys will implement a structured training and certification program to ensure all personnel assigned to the Master Agreement are fully equipped to deliver compliant and high-quality services:

- **Master Agreement Orientation Program:** Comprehensive onboarding covering the RFP scope, service categories, pricing models, and compliance requirements, including a review of Attachment 02 and relevant Participating Addenda.
- **Role-Specific Training Modules**
  - *Contract Managers*: Training on pricing compliance, documentation standards, and reporting obligations
  - *Category Leads*: Deep dives into service delivery protocols, quality assurance, and escalation procedures
  - *Engagement Managers*: Training on customer service, onboarding workflows, and communication best practices
- **Compliance and Security Training:** Annual and ad hoc training on data protection, breach notification laws, and secure communication protocols, including simulated breach response exercises.
- **Knowledge Management Tools:** Access to a centralized knowledge base with SOPs, FAQs, pricing matrices, and regulatory updates, supported by internal collaboration platforms for real-time updates and peer support.

3. Resource Scalability and Continuity

Infosys ensures service continuity and responsiveness through a scalable and resilient delivery model:

- **Scalable Delivery Model:** A trained bench of professionals is maintained to support surge capacity and concurrent engagements across multiple Participating Entities.
- **Business Continuity Planning:** Redundant staffing and infrastructure are in place to ensure uninterrupted service delivery in the event of personnel turnover or operational disruptions.
- **Performance Monitoring:** Regular internal reviews, stakeholder feedback loops, and SLA tracking ensure continuous improvement and alignment with Participating Entity expectations.

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

Infosys Response:

Infosys Public Services is committed to driving widespread adoption and sustained utilization of the Master Agreement by Participating and Purchasing Entities. Our strategy is centered on proactive engagement, education, and enablement, ensuring that eligible entities clearly understand the value, accessibility, and flexibility of the agreement. Here are the key drivers of our strategy:

1. Strategic Engagement with State and Local Governments

Infosys will leverage its established relationships with state agencies, municipalities, and public institutions to position the Master Agreement as a streamlined and efficient procurement vehicle. Key activities include:

- Conducting targeted briefings with procurement and IT leadership in each state to outline the benefits and ordering process
- Participating in state-led procurement and IT forums to raise awareness and provide real-time support
- Collaborating with state procurement offices to integrate the Master Agreement into internal procurement portals and guidance materials

2. Enablement Through Education and Demonstration

To ensure Participating Entities are confident and well-equipped to utilize the Master Agreement, Infosys will:

- Host webinars and virtual workshops tailored to procurement officers, CIOs, and CISOs, demonstrating how to initiate services and customize scopes of work
- Provide comprehensive onboarding kits, including:
  - Step-by-step ordering guides
  - FAQs and service category overviews
  - Sample Statements of Work (SOWs)
- Offer live demonstrations of the dedicated Master Agreement website, showcasing how to access pricing, submit service requests, and track engagement progress

3. Dedicated Support and Relationship Management

Infosys will assign Regional Engagement Managers to serve as direct points of contact for Participating Entities. Their responsibilities will include:

- Supporting onboarding and initial service requests
- Advising on service customization to meet specific agency needs
- Ensuring ongoing satisfaction and identifying opportunities for expanded use of the agreement

4. Visibility Through Public Sector Channels

To maximize awareness and visibility, Infosys will promote the Master Agreement through:

- Active participation in national and regional conferences such as **NASCIO**, **NIGP**, and state IT summits
- Publication of thought leadership content on cybersecurity, breach response, and digital trust in government
- Development of case studies and success stories that highlight the value delivered to other agencies through the agreement

5. Continuous Improvement and Feedback Integration

To ensure the Master Agreement remains relevant and responsive to the needs of Participating Entities, Infosys will:

- Conduct **quarterly feedback sessions** with Participating Entities to gather insights and identify areas for improvement
- Use feedback to refine service offerings, enhance user experience, and inform future outreach strategies

---

- 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?)

Infosys Response:

Infosys is committed to a collaborative, flexible, and responsive approach in negotiating Participating Addenda with eligible Participating Entities. We understand that each state or agency may have distinct statutory, regulatory, and operational requirements. Our goal is to accommodate these needs while upholding the integrity and efficiency of the Master Agreement. Following points list down the key components of our approach as well as highlight the available resources to support the same:

1. Flexible and Cooperative Negotiation Process

Infosys will engage with each Participating Entity to ensure their unique requirements are accurately reflected in their Participating Addendum. Our approach includes:

- **Open Dialogue:** We initiate comprehensive discussions to understand each entity's legal, operational, and procurement frameworks.

- **Tailored Language Inclusion:** We support the incorporation of entity-specific provisions, including those related to data privacy, security, indemnification, and governing law.
- **Optional Statutory References:** While statutory citations are welcomed for clarity, they are not mandated for the inclusion of customized terms.

2. Capability for Simultaneous Multi-Entity Negotiations

Infosys possesses the infrastructure and expertise to manage concurrent negotiations with multiple Participating Entities. This capability is supported by:

- **Dedicated Legal and Contracts Team:** Our team brings extensive experience in public sector agreements across diverse jurisdictions.
- **Regional Engagement Leads:** Contract managers coordinate directly with state procurement officials to streamline the negotiation and approval process.
- **Contract Lifecycle Management Tools:** We utilize advanced tools to monitor progress, manage redlines, and ensure timely execution.

3. Commitment to Timeliness and Transparency

Infosys prioritizes efficiency and clarity throughout the negotiation process:

- **Expedited Timelines:** We strive to finalize Participating Addenda within 15–30 business days, depending on the complexity of requested modifications.
- **Prompt Review and Feedback:** All proposed changes are reviewed swiftly, with clear explanations provided for any terms requiring further discussion.
- **Real-Time Communication:** We maintain version-controlled documentation and offer continuous updates to Participating Entities.

4. Post-Execution Support

Following the execution of a Participating Addendum, Infosys ensures a seamless transition into service delivery through:

- **Onboarding Assistance:** We provide guidance to help entities effectively initiate services under the agreement.
- **Customized Documentation:** This includes tailored pricing schedules and ordering guides.
- **Ongoing Relationship Management:** We remain engaged to support future amendments and service expansions.

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

Infosys Response:

Infosys is fully prepared to commence service delivery immediately upon execution of the Master Agreement and any Participating Addendum. Our operational readiness is underpinned by robust infrastructure, a trained and allocated workforce, and streamlined onboarding and activation processes. Below points detail key drivers of our operational readiness, as well as demonstrate it with successful examples:

1. Pre-Established Delivery Infrastructure

Infosys has invested in scalable, secure, and compliant infrastructure to ensure uninterrupted service delivery from day one:

- **24x7x365 Cyber Defense Centers (CDCs):** Our U.S.-based CDCs are fully operational and staffed to deliver services across all categories—Category 1 (Risk Assessment), Category 2 (Incident Response), and Category 3 (Breach Coach)—without delay.
- **Cloud-Ready Platforms:** Services are hosted on secure, compliant platforms (e.g., FedRAMP, SOC 2), enabling immediate provisioning of tools and resources.

- **Dedicated Master Agreement Portal:** A secure, contract-specific portal will be launched within 1–2 weeks of contract execution, providing Participating Entities with access to service catalogs, request submission tools, and engagement initiation workflows.

2. Trained and Allocated Resources

Infosys ensures that qualified personnel are ready to support Participating Entities from the outset:

- **Pre-assigned Delivery Teams:** A core team of program managers, service leads, and technical experts will be trained on the Master Agreement terms and pricing prior to execution.
- **Certified Professional Bench:** We maintain a pool of certified professionals (e.g., CISSP, CISA, GCIH) who are available for immediate deployment.
- **Rapid Onboarding Protocols:** Our internal systems and knowledge repositories are configured to onboard new Participating Entities within 1–2 business days of Addendum execution.

3. Streamlined Service Activation

Infosys has developed standardized tools and workflows to accelerate service initiation:

- **Standardized Intake Forms and SOW Templates:** Ready-to-use templates facilitate rapid initiation of services across all categories.
- **Automated Workflow Tools:** Real-time tracking of service requests, approvals, and delivery milestones ensures transparency and accountability.
- **Pre-configured SLAs:** Service Level Agreements are embedded into our delivery workflows to ensure compliance and performance from day one.

4. Demonstrated Readiness in Practice

Infosys has a proven track record of rapid mobilization and service activation:

- **Government of Canada EPS (Electronic Procurement System) Project:** Services were successfully activated across multiple departments within days of contract execution.
- **State of Rhode Island:** Infosys mobilized resources and commenced system modernization activities within the first week of contract award.

- 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.

Infosys Response:

Infosys is fully committed to maintaining transparency and ensuring strict compliance with NASPO ValuePoint's reporting requirements. We will implement a structured, auditable process to ensure that all sales whether direct or through authorized dealers, partners, or resellers, are reported promptly, accurately, and in full accordance with contractual obligations. Here's our proposed process in detail:

1. Centralized Sales Reporting System

Infosys will leverage its enterprise-grade Contract and Revenue Management System to consolidate and track all transactions under the Master Agreement. This system is designed to:

- **Capture Multi-Channel Sales Data:** Aggregate transactions from direct sales, partners, and resellers.
- **Tag Transactions by Entity and Category:** Ensure traceability by associating each transaction with the relevant Participating Entity and service category.
- **Generate Compliant Reports:** Produce both summary and detailed reports in formats aligned with NASPO ValuePoint's specifications.

2. Partner and Reseller Compliance Framework

To ensure consistent and accurate reporting from all authorized partners, Infosys will implement a robust compliance framework:

- **Mandatory Flow-Down Clauses:** All partner agreements will include contractual obligations to report sales in accordance with NASPO ValuePoint terms.
- **Standardized Reporting Templates:** Pre-defined templates will be provided to ensure uniformity and completeness of submitted data.
- **Monthly Reporting Schedule:** Partners will be required to submit sales data on a monthly basis, aligned with NASPO ValuePoint's reporting calendar.

3. Validation and Quality Assurance

Infosys will employ a multi-tiered validation process to ensure the integrity of reported data:

- **Automated Data Validation:** System-integrated checks will verify completeness, formatting, and duplication.
- **Manual Oversight:** Contract compliance officers will review partner submissions for anomalies or discrepancies.
- **Comprehensive Audit Trail:** All submissions and revisions will be logged and archived to support audit readiness.

4. Reporting to NASPO ValuePoint

Infosys will ensure timely and accurate reporting to NASPO ValuePoint through the following practices:

- **Quarterly Submissions:** Aggregated sales reports will be submitted on a quarterly basis, or as otherwise required.
- **Detailed Breakdown:** Reports will include transaction-level detail by Participating Entity, service category, and transaction type.
- **Zero-Sales Reporting:** Infosys will submit zero-sales reports when applicable to maintain compliance during periods of inactivity.

5. Continuous Monitoring and Improvement

Infosys is committed to continuous improvement in reporting practices through:

- **Partner Training:** Ongoing onboarding and refresher training for partners on reporting obligations and tools.
- **Compliance Dashboards:** Internal dashboards will monitor reporting status, partner compliance, and upcoming deadlines.
- **Corrective Action Protocols:** Any reporting deficiencies will trigger immediate investigation and remediation with the responsible partner.

G. (ME) **Customer Service**

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

Infosys Response:

Infosys is dedicated to delivering responsive, high-quality customer service and account management to all Participating Entities under the Master Agreement. Our support model is designed to ensure timely assistance, including during critical incidents and time-sensitive engagements.

Customer Service Hours of Operation

- **Standard Support Hours:** Monday through Friday, 8:00 AM to 8:00 PM Eastern Time (ET)
  During these hours, Participating Entities have access to:
  - General inquiries and assistance
  - Support with service requests and order initiation
  - Navigation of the dedicated Master Agreement portal

- Documentation access and guidance
- Status updates on ongoing engagements

- **24x7x365 Critical Support:** Infosys provides continuous, around-the-clock support for high-priority services through our U.S.-based Cyber Defense Centers, including:
  - **Category 2:** Incident Response
  - **Category 3:** Breach Coach Services
  - **Security Operations Center (SOC) Escalations**

Key Account Staff Availability

- **Program Manager & Contract Manager:** Available during standard business hours (8:00 AM – 6:00 PM ET) and on-call for escalations. These individuals serve as the primary points of contact for:
  - Contractual matters
  - Performance monitoring and reporting
  - Issue resolution and escalation management
- **Regional Engagement Managers:** Assigned to specific Participating Entities and available during local business hours. Responsibilities include:
  - Onboarding and orientation support
  - Service customization and coordination
  - Liaison between delivery teams and the Participating Entity
- **Service Category Leads:** Available during standard business hours and on-call for urgent matters. These leads oversee:
  - Execution and quality assurance of services within their respective categories
  - Technical guidance and compliance monitoring
- **Technical Support & Operations Staff:** Available during extended support hours (8:00 AM – 8:00 PM ET) to assist with:
  - Portal navigation and technical troubleshooting
  - Order tracking and documentation support
  - General operational inquiries

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

Infosys Response:

Infosys is committed to delivering high-quality services through a responsive, transparent, and structured approach to identifying and resolving problems, service issues, and customer complaints. Our methodology is designed to minimize disruption, maintain service continuity, and ensure high levels of customer satisfaction. Following points explain our approach in detail:

1. Proactive Problem Identification

Infosys employs a combination of technology, communication channels, and stakeholder engagement to detect and address issues before they escalate:

- **Real-Time Monitoring and Alerts:** For cybersecurity and incident response services, Infosys utilizes advanced monitoring tools and dashboards to detect anomalies, SLA breaches, and service degradation in real time. These tools enable early intervention and rapid mitigation.
- **Multi-Channel Issue Reporting:** Participating Entities can report issues through multiple accessible channels, including:
  - The dedicated Master Agreement support portal
  - Regional Engagement Managers
  - A 24x7 support line for urgent matters

- **Scheduled Engagement Reviews:** Regional Engagement Managers conduct regular check-ins with Participating Entities to proactively identify emerging concerns, service delivery gaps, or opportunities for improvement.

2. **Tiered Issue Classification. Below table showcases different severity levels, their description, initial response time, and resolution target.**

All reported issues are categorized based on severity and impact:

Severity Level	Description	Initial Response Time	Resolution Target
Critical (P1)	Service outage, security breach, or data loss	Within 1 hour	4–8 hours
High (P2)	Major service disruption or SLA breach	Within 2 hours	1 business day
Medium (P3)	Functional issues or delays	Within 4 hours	2–3 business days
Low (P4)	Minor issues, documentation requests	Within 1 business day	5 business days

3. **Resolution Workflow**

Infosys follows a standardized, auditable workflow to manage and resolve issues efficiently:

- **Issue Logging:** All reported issues are recorded in Infosys' internal ticketing and contract management system to ensure traceability and accountability.
- **Assignment:** Each issue is assigned to a resolution team based on its nature—technical, contractual, or operational.
- **Root Cause Analysis (RCA):** For recurring or critical issues, a formal RCA is conducted. Findings and corrective actions are shared with the Participating Entity.
- **Resolution and Verification:** Solutions are implemented and verified in collaboration with the customer before the issue is formally closed.
- **Documentation:** All actions, communications, and outcomes are documented and archived to support compliance and future audits.

4. **Customer Complaint Handling**

Infosys ensures that all customer complaints are addressed with urgency, fairness, and transparency:

- **Escalation Pathways:** If a Participating Entity is not satisfied with the initial resolution, the issue is escalated to the Program Manager and, if necessary, to Infosys executive leadership for further review.
- **Customer Advocacy:** Regional Engagement Managers serve as advocates for Participating Entities, ensuring that concerns are addressed promptly and equitably.
- **Feedback Loop:** After resolution, Participating Entities are invited to provide feedback on the handling of the issue. This input is used to refine processes and enhance service quality.

5. **Continuous Improvement**

Infosys integrates issue resolution insights into a broader continuous improvement strategy:

- **Monthly and Quarterly Reviews:** Internal reviews are conducted to analyze issue trends, resolution timelines, and customer satisfaction metrics.
- **Lessons Learned Repository:** Key insights and preventive measures from resolved issues are documented and shared across delivery teams to avoid recurrence.
- **Ongoing Training and Updates:** Staff receive regular training on updated protocols, tools, and customer service best practices to ensure consistent, high-quality support.

- Describe how you will assess customer satisfaction.

Infosys Response:

Infosys is committed to delivering exceptional service and continuously enhancing our performance based on client feedback. To ensure Participating Entities under the Master Agreement are consistently satisfied, Infosys will implement a structured, multi-channel customer satisfaction assessment and improvement program. Following are the key components of the program:

1. Post-Engagement Surveys

Infosys will gather immediate feedback following each engagement or service milestone to assess satisfaction and identify improvement opportunities:

- **Automated Feedback Requests:** Participating Entities will receive brief surveys upon completion of key service milestones.
- **Survey Design:**
  - Quantitative metrics using Likert-scale ratings (e.g., 1–5)
  - Open-ended questions for qualitative insights
- **Delivery Channels:** Surveys will be accessible via the dedicated Master Agreement portal and may be supplemented by follow-up calls from Engagement Managers.

2. Quarterly Satisfaction Reviews

To maintain ongoing alignment with client expectations, Infosys will conduct structured quarterly reviews:

- **Scheduled Review Meetings:** Regular check-ins with Participating Entities to discuss service performance, address concerns, and gather feedback.
- **Performance Dashboards:** Reviews will include analysis of SLA adherence, issue resolution timelines, and satisfaction trends.
- **Action Plans:** Identified issues or areas for improvement will be documented and tracked through formal action plans.

3. Real-Time Feedback Mechanisms

Infosys enables real-time feedback to ensure immediate visibility into client concerns:

- **Live Feedback Widget:** The Master Agreement portal will feature a feedback tool for users to rate their experience or report issues in real time.
- **Direct Escalation:** Participating Entities may escalate concerns directly to their assigned Engagement Manager or Program Lead for prompt resolution.

4. Satisfaction Metrics and Reporting

Infosys will track and report on key satisfaction indicators to monitor service quality and responsiveness:

- Key Metrics:
  - Net Promoter Score (NPS)
  - Customer Satisfaction Score (CSAT)
  - Issue resolution satisfaction
  - Repeat engagement rate
- **Internal Dashboards:** Real-time dashboards will monitor trends and highlight areas for improvement.
- **Reporting to NASPO ValuePoint:** Aggregated satisfaction data may be included in quarterly performance reports to demonstrate service quality and responsiveness.

5. Continuous Improvement Loop

Infosys integrates client feedback into a continuous improvement cycle to enhance service delivery:

- **Root Cause Analysis:** Negative feedback or low satisfaction scores will trigger formal RCA and corrective action.
- **Knowledge Sharing:** Lessons learned are documented and shared across teams to prevent recurrence and promote best practices.

- **Training Enhancements:** Staff training modules are regularly updated based on feedback insights to ensure alignment with evolving client expectations.

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

Infosys Response:

Infosys is committed to upholding the highest standards of information security, privacy, and regulatory compliance. We meet or exceed the mandatory security requirements outlined in the RFP through a combination of industry-recognized certifications, robust internal controls, and strategic partnerships:

1. AICPA SOC 2 Compliance

Infosys maintains **SOC 2 Type II** compliance, covering all five Trust Services Criteria:

- Security
- Availability
- Processing Integrity
- Confidentiality
- Privacy

These audits are conducted annually by an independent third-party auditor. Our most recent SOC 2 Type II report is available upon request and demonstrates our adherence to rigorous internal controls, continuous monitoring, and risk mitigation practices.

2. NIST 800-53 Moderate Controls

Infosys has implemented security controls aligned with **NIST Special Publication 800-53 Revision 5 (Moderate baseline)**. We have undergone third-party assessments within the past two years to validate our compliance, ensuring robust risk management, data protection, and operational resilience.

3. FedRAMP/GovRAMP Authorization

While Infosys is not a FedRAMP-authorized Cloud Service Provider (CSP), we deliver services to U.S. government entities using infrastructure hosted by FedRAMP-authorized providers. This ensures that all cloud-hosted environments used in such engagements meet FedRAMP Moderate or High security requirements, in alignment with federal standards.

4. Comprehensive Security Practices and Documentation

Infosys maintains a well-documented and mature Information Security Management System (ISMS), which includes:

- Information security and data privacy policies
- Incident response and breach notification procedures
- Encryption standards aligned with FIPS 140-2
- Physical and logical access controls
- Secure Software Development Lifecycle (SDLC) practices

These documents are available for review under a Non-Disclosure Agreement (NDA) or upon request by the Lead State or Participating Entities.

5. Ongoing Compliance and Reporting

Infosys is committed to maintaining compliance with all applicable security standards throughout the term of the Master Agreement. We will:

- Provide updated SOC 2 Type II reports or equivalent third-party assessments at least every two years
- Deliver audit documentation within six months of completion, or as otherwise required
- Continuously monitor and enhance our security posture in response to evolving threats and regulatory changes

---

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.

Infosys Response:

Infosys is committed to delivering innovative, secure, and intelligent solutions under the Master Agreement. As part of this commitment, Infosys will leverage its **Applied AI capabilities** through the **Infosys Topaz platform** to enhance cybersecurity, risk assessment, incident response, and data protection services as outlined in the Scope of Work.

1. AI Technologies and Their Purpose

Infosys may deploy the following AI-driven solutions to improve service delivery and operational efficiency:

- **Threat Detection and Risk Analysis:** AI models continuously monitor systems to detect anomalies, identify threats, and assess vulnerabilities in real time.
- **Predictive Analytics:** Machine learning algorithms forecast potential security incidents and prioritize mitigation strategies based on risk severity and impact.
- **Natural Language Processing (NLP):** NLP tools analyze unstructured data—such as incident reports, logs, and communications—to extract actionable insights and accelerate decision-making.
- **Automated Incident Response:** AI-driven automation supports containment, eradication, and recovery workflows, reducing response times and minimizing human error.
- **Forensic Analysis:** AI tools assist in digital forensics by identifying patterns and correlating events across large datasets to support root cause analysis and evidence gathering.

2. Safeguards and Protocols

Infosys ensures the responsible and secure use of AI technologies through a comprehensive set of safeguards:

- **Responsible AI Toolkit:** Infosys has developed and open-sourced a Responsible AI Toolkit to promote transparency, fairness, and accountability in AI systems.
- **Bias Detection and Model Interpretability:** All AI models undergo rigorous testing for bias and are designed to be interpretable, ensuring that decisions can be audited and explained.
- **Continuous Monitoring:** AI systems are continuously monitored for performance, accuracy, and compliance with applicable regulatory standards.
- **Human-in-the-Loop (HITL):** Critical decisions—particularly those involving privacy, legal, or regulatory implications—are subject to human review and approval.
- **Data Privacy and Security:** All AI solutions are deployed in secure environments that comply with SOC 2, NIST 800-53, and FedRAMP standards, ensuring data confidentiality, integrity, and availability.

3. Compliance and Governance

Infosys' AI implementations are aligned with industry best practices and global regulatory frameworks. We actively participate in international AI governance consortiums and adhere to ethical AI principles, ensuring that our solutions are not only effective but also responsible and trustworthy.

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.

L. **IPRO Cost Submission. When submitting your response through IPRO, you must enter**

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

Signature

The undersigned is one of the following:

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

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

OFFEROR:

	June 26, 2025
Signature	**Date**
Bhanu Prasad Narayana	Vice President – Head of US Public Sector
Printed Name	**Title**
Bhanu_PrasadN@infosys.com	+1 301 3541313
Email Address	**Phone Number**