Amendment 2
Attachment 07
OFFEROR RESPONSE WORKSHEET, ACKNOWLEDGEMENTS, AND CERTIFICATIONS

Offeror must provide complete responses to each item below. **Insert your responses into this worksheet directly below each question or prompt.**

I. Indicate the Service Category(ies) Offeror is responding to:

- ☒ **Category 1: Risk Assessment and Mitigation Services**
- ☐ **Category 2: Incident Response Services**
- ☐ **Category 3: Breach Coach Services**
- ☐ **Category 4: Notification and Credit Monitoring Services**

II. OFFEROR INFORMATION

A. Company's Full Legal Name: NTT DATA State Health Consulting, LLC.
B. Primary Business Address: 7950 Legacy Drive, Suite 1100 Plano, TX 75024
C. Federal Tax Identification Number: 37-1802584
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

OFFEROR'S RESPONSE:

NTT DATA uses proprietary, securely hosted, generative AI capabilities to identify relevant source proposal materials, approaches and experience from our large body of current and historical projects.

III. BUSINESS DETAILS

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

OFFEROR'S RESPONSE: https://www.nttdata.com/global/en

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.

OFFEROR'S RESPONSE:

NTT DATA State Health Consulting, LLC, (NTT DATA) brings more than 35 years of experience providing advisory services to state agencies. The business now known as NTT DATA State Health

Consulting was founded in 1987 as Fox Systems and gradually established a national reputation as a leading consultancy. The consulting company was acquired by Cognosante Holdings, LLC, in 2010. Several years later, this consulting business became known as Cognosante Consulting, LLC, a new entity launched in 2016.

In 2019, Cognosante Consulting, LLC, was acquired by the NTT DATA Group and renamed NTT DATA State Health Consulting, LLC (NTT DATA). Over the years, NTT DATA has served as a trusted partner for state agencies across 49 states, the District of Columbia, and Puerto Rico, providing tailored solutions that address the unique challenges faced by these entities. Our expert consultants, who have dedicated their careers to working with state agencies, utilize proven methodologies to deliver high-quality services in cybersecurity, project management, modular procurement, quality assurance, and independent verification and validation (IV&V).

With strong roots as a leading consultancy and backed by extensive corporate resources, NTT DATA has the expertise to help government organizations serve the public more intelligently and effectively.

Cybersecurity and Related Experience. In cybersecurity, we audit, assess, and advise on various security frameworks and technologies to safeguard data and infrastructure. Our project management services ensure timely and budget-conscious project delivery, while our modular procurement solutions streamline the acquisition of necessary components and services. Our quality assurance processes guarantee that deliverables meet the highest standards, and our IV&V services offer objective assessments to enhance project outcomes.

Assessing and mitigating risks is a cornerstone of NTT DATA's approach in all our projects. Our commitment to identifying potential threats and implementing effective mitigation strategies ensures the protection of our clients' assets and the continuity of their operations. Through rigorous risk management processes, we provide solutions that address both current and emerging risks, thereby enhancing the resilience and security of the organizations we serve. This long-standing focus on risk management underscores our dedication to delivering excellence and reliability in every project we undertake.

NTT DATA's comprehensive services empower state governments to optimize operations, improve service delivery, and better serve their constituents, making us the partner of choice for public sector clients nationwide.

NTT DATA Americas and the NTT DATA Group. NTT DATA State Health Consulting is a wholly owned subsidiary of NTT DATA Americas, Inc. NTT DATA Americas has provided IT services in the United States for close to 60 years. Incorporated on March 6, 1967, this company is headquartered in Plano, Texas.

NTT DATA Americas, in turn, is a U.S. subsidiary of the NTT DATA Group, a global top 10 IT services provider with 193,500 employees, including more than 10,000 in the United States. The NTT DATA Group is a full-stack IT services provider—one of the few companies able to build, operate, maintain, and transform applications and full IT systems in-house through with capabilities that range from advisory services to application services, infrastructure services, digital transformation services, and more.

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

OFFEROR'S RESPONSE:

NTT DATA State Health Consulting, LLC is a subsidiary of the NTT DATA Group Corporation, a top 10 global IT services provider with operations in more than 50 countries. The NTT DATA Group has 193,500 employees worldwide, including more than 10,000 in the United States, 500 of which are part of the NTT DATA State Health Consulting, LLC, team.

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

OFFEROR'S RESPONSE:

NTT DATA State Health Consulting, LLC, is a wholly owned subsidiary of NTT DATA Americas, Inc. NTT DATA Americas, Inc., in turn, is a U.S. subsidiary of the NTT DATA Group, a top 10 (based on sales) global IT services provider.

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.

OFFEROR'S RESPONSE:

Neither NTT DATA State Health Consulting, LLC, nor any of its principals have had any claims against them for non-performance or breach from customers in excess of $5,000 nor any related civil, criminal, or appellate litigation matters or criminal convictions in the past 5 years.

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.

OFFEROR'S CONTRACT MANAGER:
NTT DATA designates Patti Garofalo as the Contract Manager and single point of contact for management of the NASPO ValuePoint Master Agreement. Please see her resume below along with her title, phone number, email address, and work hours.

PATTI GAROFALO, Senior Director of Statewide Consulting

Patti Garofalo leads NTT DATA projects for Social Services programs including Child Support, Child Welfare, Integrated Eligibility, Medicaid, and other related public sector programs. She is a proven SME with over 30 years of demonstrated experience in public and private sector organizations planning, developing and leading business and IT transformation initiatives. Additionally, Patti brings over 20 years of experience holding leadership and Contract Manager roles for state and local government systems modernization projects, including four years serving the State of Idaho as a Project Director and as the Consultant Services Manager providing both business and technical resources to Idaho Projects. She has also spent over 18 years serving in Project Director and Account Executive roles for modernization initiatives, including multiple strategic planning, project management office (PMO), quality assurance (QA), IV&V, DDI and security assessment engagements. Patti resides in Meridian, Idaho.

Contact Information
Phone Number: [redacted]
Email Address: Patti.Garofalo@nttdata.com

Work Hours: 8:00 a.m. – 5:00 p.m. MT

Education

- Bachelor of Science, IT, American Intercontinental University

Certifications and Training

- Certified PMP
- Certified Lean Six Sigma Master Blackbelt
- NTT DATA Bronze Level Diversity, Equity, and Inclusion Awareness

Employment Experience

Senior Director, NTT DATA **04/21 – Present**

As the leader of NTT DATA's State Health Consulting practice, Patti:

- Provides engagement, contract management and leadership guidance on projects across the United States for complex business and technology projects and strategic initiatives to maximize client goals and objectives.
- Leads business optimization, organizational realignment, and service delivery model transformations.
- Serves as the Contract Manager for the Idaho MMIS System Integration Strategy Services Project
- Serves on the NCSEA Emerging Issues and Social Media subcommittees.
- Served on the CMS sponsored MITA Governance Outcomes Based SS-A Working Group.

Senior Manager, Ernst & Young, LLP **08/18 – 04/21**

- Provided engagement management and leadership to HHS project teams on a national level across multiple service offerings.
- Led business development activities across multiple HHS programs, including Medicaid, Eligibility, MITA, Child Support, and Child Welfare.

Vice President, Practice Director, CSG Government Solutions **04/10 – 07/18**

- Led the Program Modernization Practice and Services for Medicaid, MITA, Child Support, Unemployment Insurance, Motor Vehicle, and related national client engagements.
- Provided executive leadership, contract management and subject matter expertise on 45+ engagements, assuring project management, QA, and IV&V methodologies were executed consistently across the organization.
- Co-authored the federal CMS MITA Framework 3.0.
- Served as a Technical Advisor on the American Association of Motor Vehicle Administrators System Modernization Workgroup.
- Served as the National Medicaid EDI Healthcare MITA Workgroup Co-Chair.

System Modernization Director, CNSI **07/08 – 04/10**

- Provided oversight and managerial direction to facilitate full and complete integration of the new MMIS for the State of South Dakota.
- Overall responsibility for project quality, delivery, and contract management for 100+ personnel (functional and technical managers, team leads, and development staff), and client relationship management.

MMIS Project Director, State of Idaho **10/04 – 06/08**

- Oversaw the procurement and implementation of MMIS comprised of five separate vendor contracts (Base MMIS, Electronic Document Management System, Pharmacy Benefits System, Decision Support System/Data Warehouse, and Independent QA).
- Directed and managed five MMIS vendor contracts and staff, and the state project team consisting of 25+ staff.
- Directed 70+ IT consultants and sub-contractors for statewide software releases.

V. TECHNICAL RESPONSE. This section contains technical requirements pertaining to Information Security Services. Other sections of this RFP contain additional requirements that must be met to be considered responsive. **Mandatory Evaluated (ME)**: (ME) requires a response which is evaluated by the evaluation team. Offerors who do not provide a response to a (ME) section may be found non responsive.

VI. For Sections A-D, Offerors must respond to the section(s) for the Service Category(ies) Offeror is responding to. For Section E-I, Offerors must respond to these sections.

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

- **(ME) Offeror's Experience. Describe your company's experience,** demonstrating that your company has a minimum of five (5) years of experience providing services similar in scope and size to the Category 1 Risk Assessment and Mitigation Services required in Attachment 02 Scope of Work. Provide specific examples that illustrate the specific services furnished and the size, composition, etc. of the entities for whom you have provided services that you are using to demonstrate that your experience meets this minimum requirement.
- **(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.
- **(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.
- **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.

OFFEROR'S EXECUTIVE SUMMARY:

NTT DATA is pleased to present our detailed approach to providing Risk Assessment and Mitigation Services for safeguarding organizational assets and ensuring business continuity. Throughout our response you will see a tack icon followed by narrative with blue background. This represents solicitation language and is present to assist with traceability between the RFP and SOW requirements and our response within this worksheet.

NTT DATA excels in delivering comprehensive cybersecurity solutions across the public sector, offering a wide range of security and privacy consulting services. Our portfolio includes dedicated Security Advisors, framework gap analysis, risk assessment, and evaluation of security and privacy controls. With a commitment to customization, we tailor our solutions to align with each Purchasing Entity's unique needs, particularly when securing state data amidst evolving threats and diverse regulatory landscapes.

Our assessments are grounded in the NIST Risk Management Framework (RMF), Special Publication (SP) 800-37 and align with multiple security and risk frameworks. Our team, certified by ISC2, ISACA, CompTIA, GIAC, CSA, Azure, AWS, and EC-COUNCIL, employs advanced automated tools and techniques to identify security weaknesses and test system defenses. Our proven track record of delivering projects on time and within budget, combined with our comprehensive methodologies, ensures exceptional results.

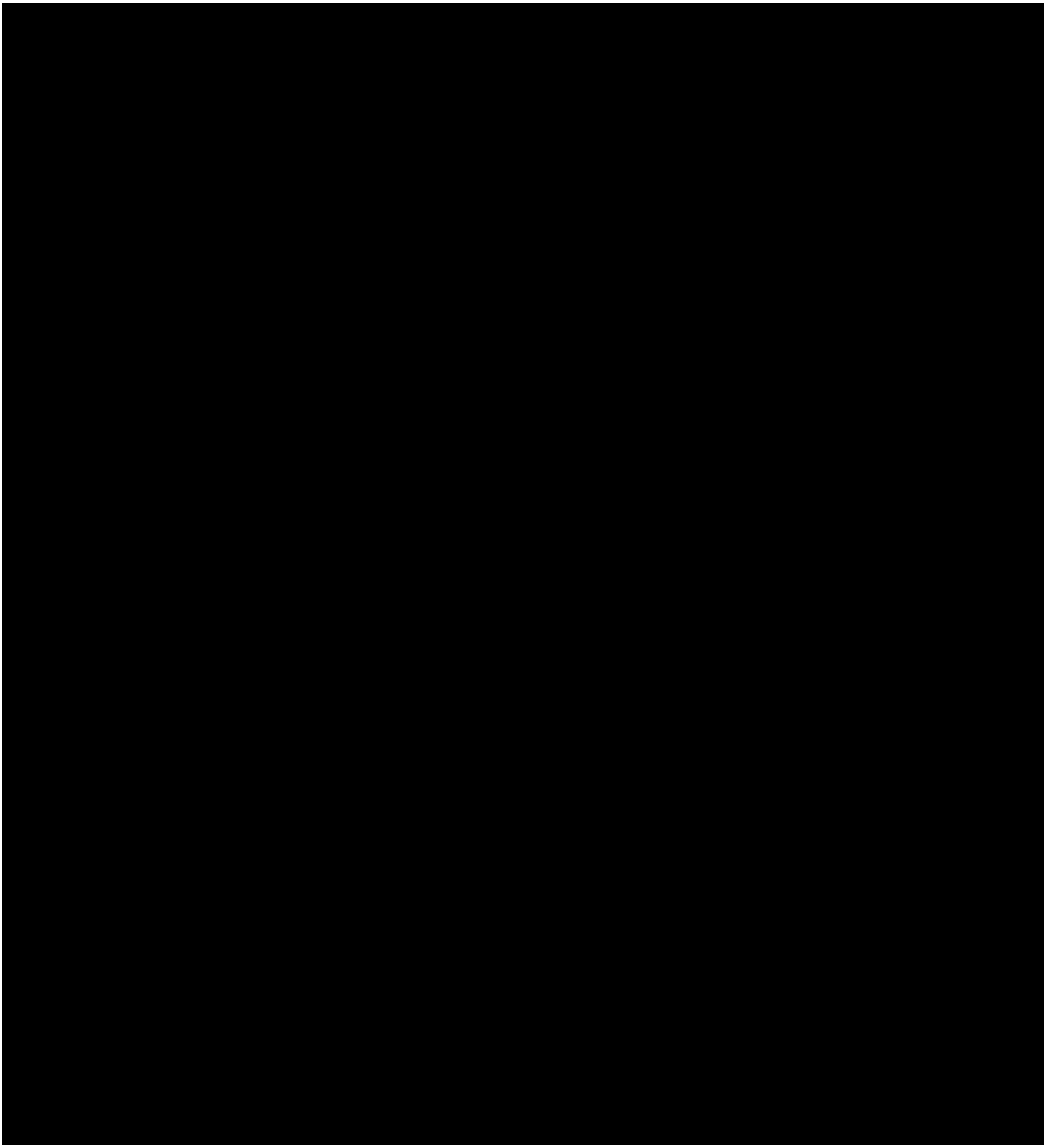
We provide clear, actionable recommendations that enhance our Risk Assessment and Mitigation Services, foster trust and ensure project success. Our holistic approach is tailored to benefit all state departments, institutions, agencies, political subdivisions, and other eligible public and nonprofit entities across the United States and its territories. Our extensive expertise and commitment to excellence make us an ideal partner for clients seeking to enhance their IT security capabilities and achieve strategic objectives.

NTT DATA – A Trusted Partner in Idaho

NTT DATA has recent experience supporting the following Idaho Department of Health and Welfare (IDHW) projects:

- **March 2024 – Present:** NTT DATA is engaged with the IDHW to develop the integration strategy for the MMIS replacement. Our team develops standards and processes for module vendors to comply with and institutes an Architecture Review Board and a Data Governance Board. Once the procurements are complete, our team provides technical oversight over all module vendors. Our team is also the liaison for Data Governance for the Self Reliance system which manages the SNAP, Temporary Assistance for Needy Families (TANF), Medicaid Eligibility, and Child Care Systems.
- **November 2024 - January 2025:** The IDHW requested a review of their Medicaid eligibility system, processes, and policy documents. NTT DATA conducted a review to identify gaps and make improvements in policy, processes, and system application services to ensure eligibility determinations are accurate. IDHW contracted with NTT DATA to provide consulting services to the Division of Self Reliance to complete a limited review of their eligibility system, process, and policy to develop a report that addresses the requirements of the IDHW Director's Bulletin 2024-11: Strengthening Medicaid Eligibility Integrity. NTT DATA conducted a system and business assessment in concert with a gap analysis of the current Idaho Benefit Eligibility System (IBES) to identify improvements based on best practices and policy requirements. NTT DATA also evaluated the functionality and compliance of IBES by executing test and process scenarios.

Furthermore, we have multiple employees that live in Idaho and others who worked with or for the Idaho Department of Health and Welfare, such as Patti Garofalo – your contract manager, Lisa Alger, Monty Fleenor, Monica Coon, Janice Gillett, Randy Browning, Colleen May, Paul Combs, and Stan Panfilov. This enhances our knowledge and strengthens our commitment to Idaho's modernization success.



Category 1 – Risk Assessment and Mitigation Services – Experience and Qualifications
(1st bullet) (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.*

OFFEROR'S COMPANY EXPERIENCE:

An evolving threat landscape requires organizations to continuously review and analyze new risks, threats, and vulnerabilities that can negatively affect businesses. NTT DATA surpasses the minimum of five years' experience by possessing over 35 years of extensive experience in delivering risk assessments and mitigation services, underscoring our deep expertise and commitment to excellence in this critical area. Throughout these decades, we have partnered with a diverse range of clients across multiple industries, providing tailored solutions that address unique risk profiles and operational challenges. Our seasoned professionals employ a comprehensive approach to risk management, integrating industry-leading methodologies and tools to identify potential threats, evaluate their impact, and develop effective mitigation strategies. This long-standing experience not only highlights our ability to protect our clients' assets and ensure operational continuity but also demonstrates our capacity to adapt to evolving threats and regulatory landscapes. Our track record of successful project execution and client satisfaction is a testament to our dedication to delivering superior risk management services that meet and exceed client expectations, as highlighted in **Figure 3**.

[1]Gartner® Market Share Analysis: Security Services, Worldwide, 2023, published July 2024
[2]IDC MarketScape: Worldwide Systems Integrators/Consultancies for Cybersecurity Consulting Services 2024 Vendor Assessment, published January 2024

Figure 3: Industry Recognition

At NTT DATA, we are acutely aware of the complex landscape of risks that can impact privacy concerns and inform policy decisions. In today's interconnected digital environment, safeguarding personal and sensitive data is paramount, and understanding the nuances of these risks is crucial to maintaining trust and compliance. We recognize that the state of Idaho, along with Participating Entity states, has a fundamental obligation to protect its citizens' Personally Identifiable Information (PII), Protected Health Information (PHI), and Federal Tax Information (FTI). This responsibility requires comprehensive internal controls and strategic frameworks that are both proactive and responsive to potential threats.

Our commitment to information security is grounded in three core principles: confidentiality, integrity, and availability. These principles are the foundation of our security strategy and drive our approach to data protection.

We are currently engaged with 10 states to support their cybersecurity needs and manage numerous task orders which support multiple contracts in Arkansas, Florida, Hawaii, Idaho, Illinois, Maryland, Mississippi, Oregon, Tennessee, and Wyoming. Given our extensive experience in highly regulated industries, including financial services, insurance, technology, and healthcare, we are positioned to provide insight into specific issues relevant to Idaho. Idaho benefits from this expertise through our unique perspectives, industry knowledge, and the recommendations we include in deliverables that assist Idaho in safeguarding its IT enterprise infrastructure and sensitive data.

We drive client satisfaction by continually evaluating and evolving our services to align with the changing cybersecurity landscape. Based on these ongoing evaluations and our experience, we excel in delivering risk assessments for our clients. **Figure 4, Figure 5, Figure 6, Figure 7, Figure 8, Figure 9 and Figure 10** summarize our recent assessment experience for agencies across multiple states, which exceeds the minimum of five years of experience.

Figure 4. Risk Assessment Experience - Arkansas

State and Project Name	Contract Term
Arkansas Enterprise Project Management Office (EPMO)	2016 – Ongoing
Project Description, Size, and Composition	
NTT DATA manages the Enterprise Project Management Office (EPMO) for the Arkansas Department of Human Services (DHS), overseeing more than 45 projects that range from process improvements to complex IT implementations, such as Medicaid Management Information Systems (MMIS), Medicaid/SNAP Eligibility and Enrollment Frameworks, and Child Welfare Information Systems. The EPMO organizes governance meetings, manages the project portfolio, and ensures alignment with state and federal requirements. A key function of the EPMO is conducting comprehensive risk assessments for each project. This process includes identifying risks related to system integration, compliance, and timelines. The EPMO then develops and implements risk mitigation strategies to address these challenges, helping projects stay on schedule and within budget. By proactively managing risks, the EPMO enhances project success rates, supports strategic planning, and improves service delivery and operational efficiency for Arkansas DHS.	
NTT DATA's Risk Assessment Experience During this Engagement	
Throughout the contract, NTT DATA has executed a wide range of security and risk-related functions. • As an advisor to the Information Security Officer for the Arkansas Medicaid Eligibility System, we demonstrated our commitment to excellence by consulting and reporting to the Centers for Medicare and Medicaid Services (CMS). In collaboration with the Department of Human Services System Integrator, we facilitated the implementation of appropriate security controls as systems transitioned to the cloud environment. • Our expertise includes conducting comprehensive assessments based on the NIST Cybersecurity Framework (CSF) and Risk Management Framework (RMF), as well as executing various risk, privacy, and business impact assessments. • We conduct risk gap analyses to ensure compliance with the Social Security Administration, the Internal Revenue Service regarding Federal Tax Information, the FBI's Criminal Justice Information Services Division, and the Family Educational Rights and Privacy Act (FERPA). • Additionally, NTT DATA consistently performs HIPAA security risk assessments, demonstrating our ongoing commitment to safeguarding sensitive information and maintaining regulatory compliance.	

Figure 5: Risk Assessment Experience - Delaware

State and Project Name	Contract Term
Delaware Health and Social Services, Delaware Medicaid Enterprise System (DMES) Quality Assurance Engagement	2014 – 2018
Project Description, Size, and Composition	
NTT DATA provided quality assurance and business analysis services for the Delaware Medicaid Enterprise System (DMES) project, which aimed to modernize Delaware's Medicaid Management Information System. Starting in 2014, NTT DATA ensured compliance with quality standards and regulations, supported planning and procurement, and contributed to the system's successful CMS certification in March 2018. A key part of our support included conducting a comprehensive risk assessment. This assessment identified potential challenges such as issues with system integration, vendor coordination, and regulatory compliance. By evaluating these risks early, NTT DATA developed and implemented mitigation strategies to minimize disruptions and ensure project continuity. These risk management efforts enabled a smooth transition to the new modular, multi-vendor solution, enhancing the reliability and effectiveness of the system for the Delaware Department of Health and Social Services.	
NTT DATA's Risk Assessment Experience During this Engagement	
NTT DATA provided technical risk management within quality assurance (QA) oversight for all Medicaid Management Information Systems (MMIS) functional areas, including security access control, testing, and operations. • This involved proactively identifying, assessing, and mitigating potential technical issues that could negatively impact project quality and success. • We offered feedback on security assessments and operational performance, authored a De-Identification White Paper, and advised the state on role-based security and testing in the MMIS. • Additionally, we co-authored monthly and quarterly project assessment reports.	

Figure 6: Risk Assessment Experience - Hawaii

State and Project Name	Contract Term
Hawaii Med-QUEST Division (MQD) Health Analytics	2022 – Ongoing
Project Description, Size, and Composition	
NTT DATA is providing project management services for the Hawaii Med-QUEST Division (MQD) Health Analytics project, building on its previous experience with MQD during the 2019 Medicaid Information Technology Architecture state self-assessment (MITA SS-A). The project aims to develop an integrated data and analytics platform for the Department of Human Services (DHS), enabling better analysis and comparison of data related to social determinants of health, quality measures, and program integrity. A key part of NTT DATA's role is conducting ongoing risk assessments throughout the project lifecycle. These assessments focus on identifying and mitigating risks associated with data integration, system interoperability, and compliance with health data regulations. NTT DATA creates and applies mitigation strategies to ensure the project meets its goals without compromising data integrity or security. NTT DATA supports procurement, development, and implementation activities, manages multiple contracts, and works closely with MQD leaders to ensure alignment with the division's vision. Their tailored project management approach streamlines complex activities and enhances data availability, governance, and quality across all program areas. The proactive risk assessment process is integral to identifying and addressing potential challenges, contributing to the project's overall success.	
NTT DATA's Risk Assessment Experience During this Engagement	
NTT DATA provides annual security services for the Hawaii Department of Human Services (DHS) KOLEA system, aligning with the Centers for Medicare and Medicaid Services (CMS) requirements. • This includes delivering a Security and Privacy Assessment Report (SAR) for systems connected to the Federal Data Services Hub. • KOLEA is a crucial data source for the Med-QUEST Division's (MQD) Integrated Data Analytics Platform (IDAP). Therefore, ensuring the privacy and security of data within the KOLEA system is imperative.	

Figure 7: Risk Assessment Experience - Idaho

State and Project Name	Contract Term
Idaho System Integration Technical Advisor (SITA)	2024 – Ongoing
Project Description, Size, and Composition	
NTT DATA acts as the System Integration Technical Advisor for the Idaho Department of Health and Welfare (IDHW) during the modernization of its Medicaid Management Information System (MMIS). Our responsibilities include guiding change management processes, reviewing and approving project deliverables, managing user security access across 15 systems, and supporting communications and outreach for healthcare providers. NTT DATA also leads process mapping and analysis to document and improve current Medicaid processes and assists in developing the MMIS procurement Advance Planning Document to align with IDHW's strategic and compliance goals. A critical aspect of NTT DATA's engagement is the comprehensive risk assessment conducted throughout the project lifecycle. These assessments identify potential risks and challenges during procurement and the design, development, and implementation (DDI) phases. NTT DATA develops mitigation strategies to proactively address these risks, supporting smooth project progress. The risk assessment process includes creating audit plans, leading audit teams for site visits, and reporting findings with recommendations to state leadership, ensuring effective risk management and project alignment with objectives. This proactive approach helps ensure the project's overall success and alignment with IDHW's strategic objectives.	
NTT DATA's Risk Assessment Experience During this Engagement	
NTT DATA provides security architect consultation to the Idaho Department of Health and Wellness. The team's responsibilities include: • Providing information technology consulting services for the Idaho Medicaid Modernization Project and offering direction on risk, security, compliance, and privacy program activities. • Verifying that third-party engagements conform to applicable federal frameworks, such as NIST, CMS MARS-E, HIPAA, CJIS, FERPA, FTI, SSA, PCI, and state law.	

- Creating, updating, and reviewing team deliverables, including policies, standards, guidelines, system security plans, policy manuals, incident response plans, and business continuity plans.

Figure 8: Risk Assessment Experience - Illinois

State and Project Name	Contract Term
Illinois Medicaid Management Information Systems Independent Verification and Validation	2008 – Ongoing

Project Description, Size, and Composition

NTT DATA provides Independent Verification and Validation (IV&V) services for the Illinois Medicaid Management Information Systems (MMIS) project, overseeing and validating that the system meets federal and state standards throughout its development and implementation. Their responsibilities include comprehensive oversight of project requirements, design, implementation, and vendor deliverables for the MMIS, Provider Enrollment, Enterprise Data Warehouse (EDW) and Third-Party Liability (TPL) modules.

A key component of our role is performing risk assessment and mitigation. NTT DATA proactively identifies and addresses risks and issues that could affect project success through continuous monitoring and reporting. We keep state and federal executives informed about project status, risks, and recommendations, ensuring transparency and supporting effective, informed decision-making. This independent oversight helps ensure that all project aspects align with state goals and regulatory requirements.

NTT DATA's Risk Assessment Experience During this Engagement

NTT DATA performs the following security risk assessment activities under this contract.

- Assess all security deliverables, such as System Security and Privacy Plan, Configuration Management Plan, Incident Response Plan, Disaster Recovery Plan, Business Continuity Plan, logical and physical architecture and network diagrams to ensure compliance with the vendor's contract and state requirements. Furthermore, NTT DATA provides detailed mitigation recommendations to the state and vendors when non-compliance and risks are identified.
- Work with the agency Chief Information Security Officer (CISO) to curate security standards across NIST, MARS-E, SSA, and IRS regulations for internal processes and system vendor requirements. This NTT DATA developed tool enables any state to identify the most stringent control based on the data within each module.
- Collaborate with the state and vendors to ensure security protocols are in place on both the state and vendor side ahead of test events and operations.
- Conduct third-party security assessments required under the current Centers for Medicare and Medicaid Services (CMS) Streamlined Modular Certification (SMC) guidance and produce subsequent Security Assessment Report (SAR) along with Vulnerability Reports that include detailed mitigation recommendations for the state and system vendor.
- Produce monthly assessment reports to inform the project team, sponsors, and the Centers for Medicare and Medicaid Services (CMS) about the project's status, including security-related risks and mitigation progress.

Figure 9: Risk Assessment Experience - Oregon

State and Project Name	Contract Term
Oregon Independent Quality Management Services (iQMS)	2016 – Ongoing

Project Description, Size, and Composition

NTT DATA delivers Independent Quality Management Services (iQMS) to numerous Oregon state agencies to ensure effective oversight, quality standards, and risk management for complex IT projects. Our services include Quality Management Planning, Quality Control, Quality Assurance, and, importantly, comprehensive risk assessments.

Risk assessment is a key part of NTT DATA's approach. This process involves identifying risks related to project execution, technology integration, and regulatory compliance. By evaluating these risks early and throughout the project lifecycle, NTT DATA is able to develop proactive mitigation strategies, ensuring that potential challenges are addressed and projects stay on track.

NTT DATA's iQMS experience includes work with the Oregon Health Authority on Health Information Technology Portfolio Modernization, as well as with the Department of Revenue and Department of Education. Our risk assessment practices are central to providing project visibility, maintaining quality standards, and increasing the likelihood of project success by identifying and managing risks proactively.

NTT DATA's Risk Assessment Experience During this Engagement
The Oregon iQMS contract involves providing independent Quality Management Services (iQMS) for various projects within the state. These services include security risk assessment and independent security solution testing. NTT DATA currently provides these services to projects spanning health and human services departments. The projects are as follows: • Oregon Department of Human Services (DHS) ONE System Cloud Migration: Migrating the benefits enrollment system, ONE Infrastructure, from an on-premises environment to a cloud environment. • Oregon DHS Provider Time Capture Project: Implementing a solution to meet the Electronic Visit Verification (EVV) requirements of the 21st Century CURES Act. • Oregon Department of Justice (DOJ) Child Support Refactoring Project: Replacing the end-of-life framework with a modern child support system framework. • Oregon OHA Program Integrity System: Implementing a new integrity system. • Oregon OHA MMIS Infrastructure Replacement Program: Transitioning Oregon's Medicaid Management Information System (MMIS) from an on-premises setup to a cloud services provider. • Oregon OHA The WIC Information System Tracker (TWIST) to Web Project: Transitioning the WIC information system to a web-based application.

Figure 10. Risk Assessment Experience - Wyoming

State and Project Name	Contract Term
Wyoming Department of Health, Division of Healthcare Financing Comprehensive Security Testing Services (CSTS) for Infrastructures and Applications	2023 – Ongoing
Project Description, Size, and Composition	
NTT DATA provides Comprehensive Security Testing Services (CSTS) to the Wyoming Department of Health's Division of Healthcare Financing. Our services cover thorough security assessments of both applications and infrastructure, adhering to NIST SP 800-53 standards. The testing includes source code reviews (SAST), web application vulnerability scanning (DAST), infrastructure scanning, and professional penetration testing, with a special emphasis on API security. A central aspect of CSTS is detailed risk assessments. These involve identifying potential security risks, evaluating their likelihood and impact, and prioritizing them by severity. NTT DATA uses the Common Vulnerability Scoring System (CVSS) to accurately score and communicate the risk level of each vulnerability. Every finding is vetted to remove false positives, clearly explained in plain English, and accompanied by specific remediation guidance. The approach aims to protect the confidentiality, integrity, and availability of Wyoming's IT assets, and aligns with both the Department of Health's and State of Wyoming's security standards and guidelines. NTT DATA encourages developer involvement to ensure relevant and actionable findings, and their industry-certified consultants ensure the highest security testing standards. Through these comprehensive and risk-focused assessments, NTT DATA helps enhance the department's security posture with minimal operational disruption.	
NTT DATA's Risk Assessment Experience During this Engagement	
The NTT DATA team comprises technical specialists with expertise in a full range of legacy and modern technologies, as well as highly skilled strategists, data scientists, analysts, and engineers. Our expertise encompasses a comprehensive suite of consulting services in risk management, privacy, security, and regulatory compliance. We have a proven track record of partnering with organizations to identify, assess, and mitigate risks, while ensuring adherence to industry standards and legal requirements. Our team conducts thorough security testing and vulnerability assessments across 18 Department of Health systems. This includes both technical and procedural evaluations to help safeguard sensitive information and maintain the integrity of critical infrastructure. Our services include: • We systematically scan network devices, servers, and other infrastructure components to identify security weaknesses, misconfigurations, and missing patches that could be exploited by attackers. • Our team utilizes automated tools and manual techniques to detect vulnerabilities within web and mobile applications, ensuring that applications are resilient against common threats such as injection attacks, cross-site scripting (XSS), and insecure authentication. • We assess systems against relevant regulatory frameworks (such as HIPAA, NIST, and state-specific health regulations) to verify that all compliance requirements are met and provide actionable recommendations to address any gaps.	

- Our ethical hackers simulate real-world attacks to evaluate the effectiveness of existing security controls. This rigorous testing uncovers potential entry points and assesses the potential impact of a security breach.
- We perform in-depth reviews of application source code to identify security flaws, logic errors, and other vulnerabilities that automated scanning may not detect, helping to ensure secure software development practices.
- We analyze user roles and permissions to confirm that access controls are properly implemented, reducing the risk of unauthorized access to sensitive information and critical system functions.
- Our team evaluates the design, implementation, and effectiveness of security controls in place throughout the organization, providing detailed assessments and recommendations for improvement.

By integrating these services, we help the Department of Health maintain a robust security posture, proactively address emerging threats, and achieve ongoing compliance with relevant standards and regulations.

The following sections cover our comprehensive risk assessment and mitigation services designed to help the State of Idaho agencies and Participating Entities identify potential risks, evaluate their likelihood and impact, and develop effective strategies to minimize or eliminate those risks. Our services are crucial in protecting the state's assets and ensuring business continuity by proactively addressing potential threats.

NTT DATA's approach involves a thorough analysis of potential dangers, allowing us to take proactive steps to manage these risks effectively. Our experienced professionals work closely with clients to assess vulnerabilities, prioritize risks, and implement tailored mitigation strategies. Our security practice also monitors emerging threats through weekly threat briefings to stay current or potential risks to our customers. By doing so, we ensure that organizations are well-prepared to face challenges and maintain operational resilience in the face of uncertainties.

Furthermore, we offer the following responses to Category 1 related requirements from the Scope of Work.

SOW General Requirement 2.1.1 *Data Encryption and Data Location Requirements*
Non-Public Data: All Non-Public Data (includes PII and any other Data that the Purchasing Entity requires to be protected) provided by a Purchasing Entity to the Contractor must be encrypted at rest and in transit with controlled access. Unless otherwise provided in the Participating Addendum or the Purchasing Entity's Purchase Order, the Contractor is responsible for encryption of the Non-Public Data. All encryption shall be consistent with validated cryptography standards such as the current standards in FIPS 140-2, Security Requirements for Cryptographic Modules, or the then-current NIST recommendation.
All Data shall be considered Non-Public Data by the Contractor unless the Purchasing Entity has identified Data it deems as Public Data to the Contractor. The level of protection and encryption for all Non-Public Data shall be identified in the Purchasing Entity's Purchase Order.

Data Location: Any data centers used by the Contractor for activities related to the services required in this RFP must be located within the Continental United States and storage of Data at rest shall be located solely in data centers located within the Continental United States. The Contractor shall not allow its personnel or subcontractors to store Data on portable devices, except for devices that are used and kept only at its data centers located within the Continental United States. Each data center used by the Contractor to support Participating Addenda must be within a physical security perimeter to prevent unauthorized access, and physical entry controls must be in place so that only authorized personnel have access to Data.

NTT DATA implements a data protection strategy as part of its Zero Trust Architecture, which includes Secure Sockets Layer/Transport Layer Security (SSL/TLS) decryption and data encryption. The company uses multiple layers to consistently and dynamically protect data, regardless of whether a user is in the office, working from home, or on the road. Additionally, NTT DATA complies with applicable regulations concerning its presence in different geographies or client locations. Internal compliance teams monitor and review the relevant regulations for appropriateness.

Protection of Non-Public Data by NTT DATA: NTT DATA employs detailed strategic approaches to protect non-public data, such as personally identifiable information (PII) and protected health information (PHI). Our approach ensures that data is encrypted both at rest and in transit, adhering to validated cryptography standards like FIPS 140-2 and the latest NIST recommendations.

Encryption at Rest: Data at rest is protected using the Advanced Encryption Standard (AES) with at least 256-bit encryption. This ensures that sensitive information stored in databases and file systems remains secure from unauthorized access. Encryption keys are managed within secure modules to enhance security, and access to these keys is tightly controlled.

Encryption in Transit: When data is transmitted over networks, NTT DATA employs strong encryption protocols such as Transport Layer Security (TLS) 1.2 to ensure the confidentiality and integrity of the information. This includes communications containing PII and PHI, which are encrypted to prevent unauthorized interception and access during transmission.

Compliance with Standards: NTT DATA's encryption practices comply with federal and state regulations, including HIPAA and other data protection laws. We ensure adherence to FIPS 140-2 by using validated cryptographic modules and following NIST guidelines for cryptographic standards. Our commitment to these standards reinforces that data protection measures are strong and effective against current and emerging threats.

Ongoing Monitoring and Improvement: We regularly review and update our data protection strategies to adapt to changes in the threat landscape and technological advancements. This includes performing periodic security assessments and audits to verify the effectiveness of encryption and access control measures, ensuring the continuous protection of Non-Public Data.

Data Centers: NTT DATA does not use data centers for activities related to the services required in this RFP. All personnel are located within the Continental United States.

Portable Devices: NTT DATA has strict policies concerning portable devices. Laptops are encrypted by default using a strong encryption mechanism. No other devices are allowed.

NTT DATA is dedicated to protecting sensitive information, giving clients confidence that their data is secure and compliant with the highest industry standards. NTT DATA implements a strong set of control measures that underscore its commitment to safeguarding the state's sensitive information. These measures are designed to address a wide array of security challenges and ensure that client data remains protected against both current and emerging threats.

Through these multifaceted efforts, NTT DATA not only demonstrates its dedication to protecting sensitive information but also reassures clients that their data is secure and compliant with the highest industry standards. This commitment has built trust and fostered long-term partnerships with our clients that confidently rely on NTT DATA for their security needs. At NTT DATA, each employee has responsibility for security. NTT DATA has well-defined and documented Information Security roles and responsibilities for all job roles. These are communicated through multiple channels, e.g., employee meetings, compliance training, security training and the Global Code of Business Conduct. These channels are provided for all the employees, including managers and executives. In addition, management roles and responsibilities are updated in security policy program architecture and governance.

SOW Requirement 2.2.1 *The Contractor must perform vulnerability assessments, privacy impact and policy assessments, and evaluation and analysis of internal controls critical to the detection and elimination of vulnerabilities to the protection of Data, as defined by a Purchasing Entity. Services include but are not limited to: • Implementation of risk assessments and mitigation strategies in alignment with published, mainstream information security frameworks and standards.*
• Compliance assessment of the Purchasing Entity's disclosure responsibilities for Data. This includes compliance with applicable federal, state, and local regulations, and standards governing the protection of information.
• Evaluation of threats and vulnerabilities to Data in the Purchasing Entity's current environment, including any proprietary systems.
• Prioritization of threats and weaknesses identified by an assessment and cost evaluation.
• Review of, and recommendations for the improvement and/or creation of information security policies.

NTT DATA's approach starts with implementing risk assessments and mitigation strategies. We align these efforts with industry's best practices (e.g., NIST Risk Management Framework) and the required information security frameworks and standards for the State of Idaho. When conducting compliance assessments, NTT DATA examines the Purchasing Entity's

disclosure responsibilities for data, which significantly impacts the development and implementation of data governance strategies. This examination ensures that all data handling practices align with legal and regulatory requirements, thereby minimizing the risk of non-compliance. NTT DATA's engagements are highly customizable, allowing us to adapt our assessment services to the specific needs of the client. For example, law enforcement and supporting agencies require Criminal Justice Information Services (CJIS) compliance but a child protection agency may not require this level of compliance. Providing agency specific services ensures that our solutions are not only compliant but also tailored to optimize the client's operational efficiency and strategic goals. We are committed to adhering to the specific policies and procedures of the Purchasing Entity. By aligning our assessments with agency-specific regulations and standards, we ensure that all recommendations and implementations support the state's legal framework and organizational objectives. This alignment helps the Purchasing Entity maintain compliance with state laws while also enhancing their overall data security and privacy posture.

NTT DATA performs in-depth analysis of threats and vulnerabilities in the Purchasing Entity's current environment, including any proprietary systems. Our methodology encompasses both automated and manual assessments to identify potential security weaknesses. We employ advanced tools and techniques to reveal vulnerabilities that could jeopardize data integrity, confidentiality, or availability. Our approach includes using automated vulnerability scanners like Tenable Nessus and Nmap to identify potential security issues within networks and host systems. These tools allow us to create an inventory of systems, determine operating systems, and identify software and open ports. Additionally, we conduct manual testing guided by standards such as OWASP, NIST SP 800-115, and PTES, which allows us to focus on specific vulnerabilities that automated tools might miss.

Our methodology also incorporates the use of specialized tools for web application testing, including Burp Suite and OWASP Zap, to perform dynamic application security testing (DAST) and assess APIs for security weaknesses. For cloud environments, we use tools like Prowler to conduct security assessments and audits across platforms such as AWS, Azure, and Google Cloud Platform, ensuring compliance and enhancing security posture.

By combining these tools and techniques with manual validation and risk analysis, we ensure a detailed assessment that identifies and prioritizes vulnerabilities based on potential impact and likelihood of exploitation. This integrated approach not only highlights existing vulnerabilities but also provides actionable insights for mitigating risks effectively.

Prioritizing threats and weaknesses are a key component of NTT DATA's approach. By conducting a thorough risk analysis, we examine factors such as potential impact, likelihood of exploitation, and the sensitivity of the affected systems. This enables us to effectively prioritize vulnerabilities and ensure that the most critical threats are addressed promptly, providing maximum protection for the state's data assets.

NTT DATA conducts Privacy Impact Assessments (PIAs) using a structured methodology to identify, assess, and mitigate privacy risks associated with personal data handling. The process begins with planning and scoping to define the assessment's objectives and scope. We then create data flow diagrams to visualize data handling and identify potential privacy risks. Our team conducts risk identification and analysis through interviews, document reviews, and technical assessments, evaluating risks based on their likelihood and impact. For each identified risk, we develop tailored mitigation strategies, including data protection measures and policy revisions. NTT DATA provides a comprehensive PIA report detailing findings and recommendations for improving privacy practices and ensuring regulatory compliance. We emphasize continuous monitoring and improvement to adapt to changes and maintain effective privacy controls. This approach helps organizations safeguard personal data and maintain stakeholder trust.

NTT DATA also provides thorough reviews and recommendations for improving or creating information security policies. Our team collaborates closely with the Purchasing Entity to develop or enhance policies, processes, standards, and training plans. This ensures that the organization not only meets compliance requirements but also fosters a sustainable security culture.

Figure 11. Actionable Security Recommendations

Example	Risk	Recommendation
Data Breaches	Unauthorized access to sensitive data.	Implement strong encryption protocols, multi-factor authentication, and regular security audits to protect data integrity and confidentiality. *Protecting sensitive data from unauthorized access requires a multi-layered approach. Our measures go beyond mitigating security risks to ensure compliance with legal requirements and reinforce stakeholder trust in the ability to manage and protect critical information.*
Compliance Violations	Non-compliance with regulatory standards like Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), and California Consumer Privacy Act (CCPA)	Conduct regular compliance audits and training sessions for employees to ensure adherence to relevant laws and regulations. *Our proactive approach not only mitigates risk but also positions us as a trustworthy and responsible entity in the industry.*
System Downtime	Unexpected system failures leading to operational disruptions.	Establish a disaster recovery plan and invest in redundant systems to minimize downtime and maintain business continuity. *This ensures business continuity, protects critical data, and reduces the potential impact of outages.*
Insider Threats	Malicious or negligent actions by employees.	Implement strict access controls, monitor user activities, and conduct background checks to mitigate insider threats. *Our methods involve a multi-layered approach that combines technical, managerial, and operational controls, which significantly reduce the risk of insider threats and foster a more secure environment.*
Phishing Attacks	Employees falling victim to phishing scams.	Conduct regular cybersecurity awareness training and deploy email filtering solutions to reduce the risk of phishing attacks. *Together, these measures significantly reduce the risk of successful phishing attacks and help protect the organization's data, reputation, and operations.*
Outdated Technology	Security vulnerabilities due to obsolete software and hardware.	Regularly update and patch systems and consider adopting cloud-based solutions for improved scalability and security. *By combining these, the state reduces exposures to vulnerabilities associated with obsolete software and hardware, safeguards critical assets, and better position themselves to respond to evolving cyber threats.*
Lack of Incident Response Plan	Delayed response to security incidents.	Develop a comprehensive incident response plan and conduct regular drills to

Example	Risk	Recommendation
		ensure readiness in the event of a security breach. *An effective incident response capability is not just a documented plan but a living program that includes regular practice, evaluation, and improvement.*

Our experience collaborating with various public sector entities uniquely positions us to deliver tailored solutions that meet the specific needs of the State of Idaho and other Participating Entities. Our extensive experience in state government projects, particularly in Medicaid Management Information Systems (MMIS) and health and human services (HHS) modernization, provides us with a profound understanding of the regulatory and operational complexities that state agencies face. NTT DATA's Enterprise Advantage Framework, a mature and flexible set of methodologies, is specifically developed for state clients. This framework provides our team with proven tools, templates, and processes that promote agility and consistency, enabling us to integrate, monitor, and control work effectively.

Our strong local presence in Idaho, combined with a dedicated team of professionals who have extensive knowledge of Idaho's vision and goals, further enhances our ability to deliver solutions that are not only technically sound but also strategically aligned with the state's objectives. This unique blend of national expertise and local insight allows NTT DATA to offer Idaho unparalleled support in achieving its modernization and security goals. Additionally, we are committed to extending our services to other Participating Entities by fostering collaborative partnerships and ensuring seamless integration across all stakeholders. Our approach includes tailored strategies, shared resources, and coordinated efforts to address the diverse needs of each entity, thereby enhancing the overall effectiveness and efficiency of the modernization initiative.

***SOW Requirement 2.2.2** The Contractor must design and develop business processes, procedures, and business applications in response to risk assessments.*

NTT DATA is prepared to design and develop business processes, procedures, and business applications in response to risk assessments. Our methodology is rooted in a NIST-based understanding of risk management principles, enabling us to convert risk assessment findings into actionable security strategies, business processes, procedures and applications that drive success.

To initiate the process, NTT DATA conducts a thorough analysis of existing applicable processes and procedures. This involves gathering information through detailed documentation reviews, visual verification, stakeholder interviews, and compliance with federal regulations and industry standards. By doing so, we identify compliance issues and potential vulnerabilities that could impede the agency's ability to achieve its objectives.

Our collaborative approach facilitates the alignment of applicable security controls with strategic goals, risk management priorities, and relevant regulations. Leveraging insights from risk assessments and audits, which may be conducted by us or provided by the state, we develop resilient processes, which includes mapping workflows that incorporate risk management strategies, that can adapt to the evolving risk landscapes like our work in Arkansas listed above in **Figure 4**.

Throughout the development process, NTT DATA emphasizes the importance of documentation and training. We ensure that all new processes and applications are thoroughly documented, providing clear guidance. Additionally, we conduct a thorough training session to empower staff to utilize new tools and processes effectively, thereby maximizing the return on investment.

***SOW Requirement 2.2.3** The Contractor must provide a comprehensive final written report within one (1) week of conclusion of the engagement (or as otherwise determined by the Purchasing Entity) that at a minimum includes detailed risk statements, explanations, and recommendations for mitigating identified risks.*

In response to the RFP requirement for a comprehensive final written report, NTT DATA is committed to delivering a thorough and insightful document within one week of concluding the engagement. This report will contain detailed risk statements, explanations, and actionable recommendations tailored to mitigate identified risks effectively. Our approach is rooted in a NIST based methodology that integrates industry's best practices and methodologies that leverage our extensive experience across sectors. This detailed approach to identifying, assessing, and mitigating security risks supports the goals of organizations to effectively manage their security and privacy challenges. By doing so, we ensure that the report not only meets the specified requirements but also provides valuable insights into enhancing the Purchasing Entity's risk management framework. This commitment to quality and precision reflects our dedication to supporting the organization's strategic objectives and operational needs.

Examples of these best practices that are integral to our approach include:

- NIST SP 800-37 Risk Management Framework (RMF), the NIST SP 800-53 Security and Privacy Controls, the NIST SP 800-30 Guide for Conducting Risk Assessments.
- Continuous Monitoring and Risk-Based Approach: NTT DATA implements continuous monitoring practices to provide real-time insights into the security posture. This involves using automated tools to track system activities and configure alerts for potential security incidents, ensuring that risk management processes are proactive and adaptive.
- Comprehensive Reporting and Stakeholder Engagement: NTT DATA emphasizes clear communication of findings, risks, and recommended remediation actions throughout the assessment process. Our collaborative approach ensures that stakeholders are engaged and informed, enhancing the effectiveness of security control assessments.

Figure 12: Risk Mitigation Strategies

In the report, NTT DATA includes a section dedicated to risk statements, where each identified risk is described in detail. This section provides the necessary context for understanding the nature of the risks and their potential impact on the organization's operations and objectives. Essentially, risk statements describe what could go wrong, and risk factors explain why it might go wrong. Example statements can be found in **Figure 13** and **Figure 14.**

Figure 13. Risk Statements

Example Risk Statement	Explanation
Passwords are not enforced on a system that contains regulated data.	Not enforcing strong passwords is significant and can lead to various security vulnerabilities, including but not limited to unauthorized access, breaches, account compromise, and regulatory non-compliance.
A system containing unencrypted HIPAA data in the agency's Demilitarized Zone (DMZ).	The risk of having unencrypted HIPAA data in the Demilitarized Zone (DMZ) is significant and can lead to severe security and compliance issues, including unauthorized access, data exposure, data breach, regulatory non-compliance, and loss of data integrity.
Backups not running on a system that contains unemployment data.	The risk of backups not running on a system containing unemployment data is considerable and can lead to several critical issues like compliance and regulatory issues, inability to recover the system, legal penalties, and loss of citizen trust.

Following the risk statements, NTT DATA provides detailed explanations of each risk. This includes outlining the underlying factors that contribute to the risk, the potential consequences if the risk materializes, and any interdependencies that may

worsen the situation. Our explanations are backed by data and evidence gathered during the assessment, ensuring the report is informative and actionable.

Figure 14. Risk Factors

Example Risk Factors	Recommendation
Passwords are not enforced on a system that contains regulated data.	To mitigate these risks, it is crucial to implement strong encryption protocols for both data at rest and data in transit. This includes using industry-best encryption algorithms, managing encryption keys securely, and regularly updating encryption practices to address evolving threats.
A system containing unencrypted HIPAA data in the agency's Demilitarized Zone (DMZ).	To mitigate these risks, it is essential to encrypt all PHI stored and transmitted within the DMZ. Implementing strong encryption protocols, such as AES-256, and maintaining a strong security posture with firewalls, intrusion detection systems, and regular security audits can help protect sensitive data and ensure compliance with HIPAA requirements.
Backups not running on a system that contains unemployment data.	Implement a resilient backup strategy that includes regular, automated backups of all critical data. This strategy should ensure that backups are stored securely, both onsite and offsite, and are regularly tested to verify their integrity and effectiveness in data restoration processes.

The recommendations section of the report is tailored to the specific needs of the Purchasing Entity. NTT DATA provides practical and prioritized mitigation strategies for each risk, considering the organization's resources, capabilities, and strategic goals. Our recommendations are designed to address not only the immediate risks but also to enhance the organization's overall risk management framework, fostering long-term resilience.

To ensure clarity and usability, NTT DATA presents the report in a format that is complete and accessible to stakeholders at all levels. We include visual aids, such as charts and graphs, to illustrate key points and enhance understanding. Additionally, we provide an executive summary that highlights the most critical findings and recommendations, offering a quick reference for decision-makers.

NTT DATA's experience in delivering similar reports to various governmental clients highlights our capability to meet and exceed the expectations of the Purchasing Entity. Our commitment to quality, accuracy, and timeliness guarantees that the final written report acts as a valuable tool for informed decision-making and effective risk management.

SOW Requirement 2.2.4 *Upon request by the Purchasing Entity, the Contractor may be asked to provide consultation services for development of terms for third-party contracts, including those with cloud-based providers.*

NTT DATA is well-prepared to offer consultation services for developing terms for third-party contracts, including those with cloud-based providers, at the request of the Purchasing Entity. Our methodical and strategic approach is supported by our extensive industry knowledge and proven methodologies, ensuring that contract terms align with the agency's objectives and regulatory requirements.

Our process begins with a detailed analysis of the current contract environment, identifying specific needs related to third-party engagements that include but are not limited to Key Performance Indicators (KPIs), Key Risk Indicators (KRIs), Service Level Agreements (SLAs) and written and automated reporting requirements. This involves reviewing existing contracts, industry standards, and regulatory frameworks to understand the landscape fully. We collaborate closely with the Purchasing Entity to comprehend their strategic objectives, risk tolerance, and compliance requirements. This partnership enables us to customize contract terms that effectively address these factors.

NTT DATA's team of experienced consultants excels in drafting and reviewing contract terms across a broad range of areas, including data security, service level agreements, and compliance with relevant laws and regulations. For cloud-based

providers, we ensure that contracts incorporate provisions for data protection, access controls, service availability, and incident response protocols, leveraging our experience in managing cloud transformations and infrastructure design. Our consultants utilize our Enterprise Advantage Framework and insights from our extensive experience in negotiating with cloud providers, so that our clients receive fair and balanced agreements.

Throughout the negotiation process, NTT DATA provides strategic advice and support to secure favorable terms. Our consultants have a proven track record of successfully negotiating contracts that meet client needs while maintaining positive vendor relationships. Additionally, we offer continuous support to manage and oversee third-party relationships, monitoring contractual obligations so they are fulfilled, and potential issues are addressed promptly. This proactive management strategy helps mitigate risks and enhances the overall effectiveness of third-party engagements.

NTT DATA's extensive experience in providing similar consulting services to governmental and private sector clients highlights our capability to deliver tailored solutions that meet the specific needs of the Purchasing Entity. Our commitment to quality, client satisfaction, and regulatory compliance supports the alignment of terms developed for third-party contracts with the organization's strategic objectives and operational requirements.

Category 1 – Risk Assessment and Mitigation Services – Experience and Qualifications
(2nd bullet) (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.*

SOW Requirement 2.3 Personnel Qualifications. *The roles below define the minimum qualifications that the role must have for the work performed under this category. These roles also correlate to Offerors response for Attachment 07 and Attachment 09.*
2.3.1 Security/Technology Senior Analyst*: 5+ years of professional experience. Strong technical and/or security skills. Experienced in specific areas, relative to the project. Able to plan and coordinate the technical tasks and work necessary for delivery of services. Able to design and oversee completion of deliverables. Can manage and coach staff and provide QA over the process and work product, as it relates to risk, security and/or technical matters. Strong communications, analysis skills, troubleshooting, and issue resolution skills. Security or technology certification.*
2.3.2 Business Process/ Risk Management Senior Consultant: *5+ years of professional experience. Deep knowledge of business processes, industry issues, and/or risk management. Understands big picture and able to prioritize issues, based on data discovery and experience. Can provide recommendations related to security and technology matters. Able to supervise large and diverse teams and provide QA over the process and work product. Often serves as a technical subject matter specialist. Strong communication and facilitation skills.*
2.3.3 Project Manager: *5+ years of professional experience. Project Management and Business process subject matter experts. Skills and experience in managing engagement work efforts, scoping and assigning work, and managing engagement budgets. Tracks and communicates project status and demonstrates project value. Project management certification.*

OFFEROR'S STAFF EXPERIENCE AND QUALIFICATIONS:

NTT DATA has a deep bench of information security specialists supporting federal and state government clients across financial services, insurance, technology, and healthcare sectors. Our expertise spans privacy, security, and compliance consulting, as well as security, integration and modernization services. We are capable of building and testing enterprise environments and securing them in accordance with the NIST standards for information security and risk management.

For this engagement, we have assembled a team of experts with extensive security knowledge and a commitment to providing ethical security risk assessment services for the State of Idaho and Participating Entities.

NTT DATA requires staff performing Category 1 Risk Assessment and Mitigation Services to have a minimum of five years of professional experience along with industry-standard certifications such as CISSP, CISA, CISM or CRISC, ensuring foundational cybersecurity expertise. Our team has hands-on experience in risk assessments, developing mitigation strategies, and using both automated and manual techniques for vulnerability analysis. They excel in preparing detailed reports with actionable recommendations aligned with NIST SP 800-53 and ISO 27001 frameworks.

NTT DATA performs rigorous background checks to ensure the integrity of individuals handling sensitive information. Our commitment to excellence is demonstrated by our ability to deliver projects on time and within budget, as evidenced in the

Statewide or Large Consortium Contracts, Section F of this proposal.

By leveraging our deep bench of technical specialists, we will complete the proposed cybersecurity project in compliance with the State of Idaho's and other Purchasing Entities' policies and procedures, within the required timeframe.

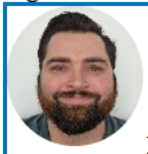
As **Figure 15** provides insight into the quality of our team and the certifications that we require and possess. We are committed to professional development and support certification and recertification efforts for our team members to maintain and grow our talent pool for these engagements.

Figure 15. NTT DATA Staff Certifications

NTT DATA Staff Certifications	Counts as of March 2025
Certified Ethical Hacker (CEH)	11
Certified Information System Auditor (CISA)	11
Certified Information Systems Security Professional (CISSP)	31
Certified in Risk and Information Systems Control (CRISC)	8
CompTIA Security+	46
Project Management Professional (PMP)	113

Below are representative bios to show that our staff meet and exceed the minimum qualifications for roles named under requirement 2.3 of the SOW.

Figure 16: Representative Bio – Security/Technology Senior Analyst



BILL HAHAJ – Security/Technology Senior Analyst

Security Areas of Expertise: Vulnerability Assessment, Penetration Testing

Role/Responsibility: QA oversight responsible for coordinating technical tasks, reporting, and performing vulnerability assessments and penetration testing.

Qualifications:
Information Security professional with a 15+ year career that includes five years focused on application security within high-security government and military environments. Proven ability to develop and enforce security best practices, leverage automation to improve team efficiency, collaborate effectively with development teams, and perform risk assessments and audits to ensure compliance with regulations. US Army veteran with experience planning and executing projects in challenging environments during three overseas deployments.

Certifications:
- CISSP, Certification #584671, November 2016

States Served: Florida, Hawaii, Oregon, Wyoming

Figure 17: Representative Bio - Business Process/Risk Management Senior Consultant

UCHE ONUKWUBIRI – Business Process/Risk Management Senior Consultant

Security Areas of Expertise: NIST FIPS/ NIST 800-53

Role/Responsibility: Technical subject matter expert responsible for IT security auditing, and IT risk assessment and management.

Qualifications:
IT security and risk management professional with over 10 years of experience supporting healthcare, telecommunications, state and federal government sectors. He has led critical initiatives including the State of Hawaii MARS-E audit, Tennessee's statewide Business Impact Assessment, and cybersecurity assessments for the State of

Virginia and Wyoming. Uche specializes in IT security auditing, risk assessment, and project management, bringing expertise in NIST, FISCAM, HIPAA, and ITIL frameworks. He effectively engages with multiple levels of stakeholders to provide security and technology recommendations. His certifications include CISA, PMP, and CRISC, underscoring his commitment to delivering strategic solutions in cybersecurity, compliance, and governance for state and local government.

Certifications:
- CISA – Certified Information Systems Auditor (ISACA), #18151608, October 2018
- CRISC – Certified in Risk and Information Systems Control (ISACA), #242620764, August 2024
- Project Management Professional (PMP) #2787631, August 2020

States Served: Hawaii, Tennessee, Virginia, Wyoming

Figure 18: Representative Bio - Project Manager

PAUL GOSNELL – Project Manager

Security Areas of Expertise: Information Security, IT Auditing & Consulting, Ethical, Hacking/Penetration Testing, Threat Intelligence, Software Development

Role/Responsibility: Project management and business process subject matter expert responsible for managing work efforts, assignments and budget in addition to performing vulnerability assessments and penetration testing.

Qualifications:
- Paul has over 20+ years of experience in IT Risk Management. He Advises state CISOs on compliance to meet standards for data security and privacy.
- Provides consultation on information security practices based on client maturity, preferences, and highest-value information security functions.
- Managed cross-functional teams in multiple locations and assignments throughout the United States.
- Works with state project leadership to advise on program and project budget management, project management, vendor management, business collaboration, and strategic initiatives.
- Expertise in budget management, project management, vendor management, business collaboration, and strategic initiatives.
- Security framework expertise in NIST SP 800-53, MARS-E, FedRAMP, NIST CSF, IRS 1075, ISO 27001, and HITRUST.

Certifications:
- GIAC Security Leadership Certification, GSLC #220256, May 2023
- Certified in Risk and Information Systems Control, CRISC #232108436, March 2023
- AWS Certified Cloud Practitioner, Validation # KCN98XXLJ111QN96, February 2021
- Certified Information Systems Security Professional, CISSP # 483215, November 2019
- Project Management Professional, PMP # 1251896, April 2009
- Advanced Systems Engineer (EDS), March 2002
- Systems Engineer Development Program (EDS), May 1998

States Served: Alabama, Arkansas, Connecticut, Delaware, Florida, Georgia, Idaho, Illinois, Maryland, New Hampshire, New Mexico, New York, Oklahoma, Oregon, Puerto Rico, Rhode Island, South Carolina, Texas, Virginia, Vermont, Wisconsin, and Wyoming

Category 1 – Risk Assessment and Mitigation Services – Experience and Qualifications
(3rd bullet) (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.*

OFFEROR'S SLA's:

NTT DATA is committed to delivering high-quality Risk Assessment and Mitigation Services, ensuring that all client expectations are met or exceeded. Our Service Level Agreements (SLAs) below are designed to provide clear guidelines for service performance, response times, and accountability in managing risks. We work collaboratively with each Purchasing Entity to modify and finalize SLAs for each contract, ensuring that they are tailored to meet specific needs and objectives.

NTT DATA-SLA-01: Response Times and Service Commitments

NTT DATA commits to timely responses to customer inquiries and support requests. Our initial response times of one day ensure prompt attention to client needs, with critical issues receiving immediate escalation and resolution. We track response times as part of our SLA compliance with agreed-upon standards. Our Contract Manager, Patti Garofalo, is the point of contact for all customer inquiries. She is available via email or phone throughout the day.

Objective: Ensure timely and effective communication between NTT DATA and the Purchasing Entity through the designated contact person.

Figure 19. NTT DATA-SLA-01: Response Times and Service Commitments

NTT DATA's Responsibilities	Purchasing Entity Responsibilities
• The NTT DATA Contact must respond promptly to communications from the Lead State, ensuring all inquiries and requests are addressed in a timely manner. • NTT DATA must notify the Lead State of any changes to the Proposal Contact within 24 hours to maintain seamless communication and continuity. • NTT DATA Executive Leadership will oversee and monitor the timely response of the NTT DATA Contact, ensuring adherence to the communication standards outlined in this SLA. • NTT DATA Executive Leadership will also ensure that changes to the Offeror's Proposal Contact are promptly communicated to the Lead State within the specified 24-hour timeframe.	• The Purchasing Entity will monitor the responsiveness of the NTT DATA Contact and document any communication issues or delays, discussing them with NTT DATA to identify areas for improvement.

NTT DATA-SLA-02: Data Ownership and Security

NTT DATA acknowledges that all rights, titles, and interests in the Purchasing Entity's data are owned by the Purchasing Entity. We are committed to meeting or exceeding the security policies, standards, and regulatory obligations defined in the Participating Addendum and associated Purchase/Work Orders. Our security measures are robust, designed to protect sensitive or protected information and prevent any compromise through breaches.

Objective: To ensure the confidentiality, integrity, and availability of all data managed by NTT DATA on behalf of the Purchasing Entity.

Figure 20. NTT DATA-SLA-02: Data Ownership and Security

NTT DATA's Responsibilities	Purchasing Entity Responsibilities
• NTT DATA shall implement and maintain robust security measures that comply with the Purchasing Entity's security policies and standards. Security audits will be conducted annually to verify compliance. • Regular security assessments and audits shall be conducted to ensure adherence to security policies and standards.	• The Purchasing Entity shall provide NTT DATA with access to relevant security policies and standards to ensure compliance. • The Purchasing Entity shall promptly communicate any updates or changes to security policies that may affect NTT DATA's obligations.

NTT DATA-SLA-03: Breach Notification

In the event of a suspected or actual breach, NTT DATA will immediately notify the Purchasing Entity upon discovery. This prompt notification ensures that appropriate actions can be taken to mitigate any potential impact.

Objective: To establish a rapid response protocol for notifying the Purchasing Entity of any suspected or actual data breaches.

Figure 21. NTT DATA-SLA-03: Breach Notification

NTT DATA's Responsibilities	Purchasing Entity Responsibilities
• NTT DATA must notify the Purchasing Entity immediately, and no later than four (4) hours after the discovery of a suspected or actual data breach. • NTT DATA shall maintain an incident log and provide regular updates to the Purchasing Entity on the status of breach investigations.	• The Purchasing Entity shall designate a primary point of contact to receive breach notifications and coordinate response efforts. • The Purchasing Entity shall provide NTT DATA with procedures for reporting and responding to data breaches to ensure alignment with internal protocols.

NTT DATA-SLA-04: Expert Service Delivery
NTT DATA ensures that trained experts with the necessary experience and qualifications perform all services. Our team is composed of professionals who possess the skills outlined in the staff experience and qualifications section of our response.

Objective: To ensure that all services provided by NTT DATA are performed by trained experts who possess the necessary experience and qualifications.

Figure 22. NTT DATA-SLA-04: Expert Service Delivery

NTT DATA's Responsibilities	Purchasing Entity Responsibilities
• All services must be delivered by professionals with expertise in their respective fields, ensuring high-quality outcomes. • NTT DATA will maintain records of qualifications and certifications for all personnel involved in service delivery. • Regular performance evaluations will be conducted to ensure that services are delivered to the highest standards of quality and expertise.	• The Purchasing Entity shall provide any additional requirements or preferences regarding personnel qualifications to ensure alignment with organizational needs. • The Purchasing Entity shall communicate any concerns or feedback related to service delivery to NTT DATA for resolution and continuous improvement. • The Purchasing Entity will have the right to review qualifications and certifications to verify compliance with the requirements outlined in Attachment 07.

NTT DATA-SLA-05: AICPA SOC 2 Compliance
NTT DATA complies with a wide array of standards, including the applicable laws and regulations in our operating regions, the SOC 1 and SOC 2 auditing framework, and specific domain standards, such as those from the Health Information Trust Alliance (HITRUST) and HIPAA, and the ISO/EIC 27001:2013 standard for information security management systems. We can provide certifications, if applicable, for the Risk Assessment and Mitigation Service that NTT DATA delivers to the State of Idaho.

Objective: To ensure ongoing compliance with relevant standards, including AICPA SOC 2 and NIST 800-53.

Figure 23. NTT DATA-SLA-05: AICPA SOC 2 Compliance

NTT DATA's Responsibilities	Purchasing Entity Responsibilities
• NTT DATA shall maintain compliance with specified standards and provide audit results to the Purchasing Entity within six (6) months of completion. Compliance assessments shall be conducted at least once every two (2) years. • NTT DATA shall provide regular compliance reports and facilitate third-party audits as required.	• The Purchasing Entity shall inform NTT DATA of any specific compliance requirements unique to their organization or industry. • The Purchasing Entity shall review the audit results provided by NTT DATA and collaborate on any necessary remediation efforts.

NTT DATA-SLA-06: Legal Requests and Data Access
NTT DATA will contact the Purchasing Entity immediately upon receipt of any legal requests, such as electronic discovery,

litigation holds, or subpoenas, that might require access to the Purchasing Entity's data. We will not respond to such requests without first notifying the Purchasing Entity, unless we are legally prohibited from doing so.

Objective: To ensure prompt communication with the Purchasing Entity upon receipt of legal requests that may impact data security or access.

Figure 24. NTT DATA-SLA-06: Legal Requests and Data Access

NTT DATA's Responsibilities	Purchasing Entity Responsibilities
• NTT DATA must contact the Purchasing Entity immediately, and no later than one (1) business day, upon receipt of electronic discovery, litigation holds, or similar legal requests. • NTT DATA shall maintain a communication log for all legal requests and provide updates to the Purchasing Entity as necessary.	• The Purchasing Entity shall provide NTT DATA with contact information for designated representatives authorized to receive and respond to legal requests. • The Purchasing Entity shall establish protocols for handling legal requests to ensure timely and coordinated responses with NTT DATA.

NTT DATA-SLA-07: Service Customization and Collaboration
We recognize that a Purchasing Entity may choose to customize the services ordered. NTT DATA retains the ability to provide all services under the Master Agreement, including any renewals. We will work closely with the Purchasing Entity to develop a detailed Statement of Work for each Order, which will include a task list, deliverables, timeframes, and staffing levels.

Objective: To ensure the flexible and efficient customization of services ordered by the Purchasing Entity, while maintaining the ability to provide all services available under the Master Agreement.

Figure 25. NTT DATA-SLA-07: Service Customization and Collaboration

NTT DATA's Responsibilities	Purchasing Entity Responsibilities
• NTT DATA shall maintain the capability to provide all services available under this Category throughout the entire Master Agreement term, including all renewals. • NTT DATA shall collaborate with the Purchasing Entity to develop a detailed Statement of Work for each Order, which includes a detailed task list, deliverables, timeframes, estimated level of effort, and staffing levels. • NTT DATA shall accommodate amendments to Orders as requested by the Purchasing Entity, ensuring flexibility and responsiveness to changing needs. • All documentation and communication must be clear, relevant, and easily understood by laypersons, with all call center operations remaining within the contiguous United States. • NTT DATA and Purchasing Entity shall conduct regular reviews to assess the effectiveness of service customization and address any issues or improvements needed. • NTT DATA shall provide periodic reports detailing service delivery, order amendments, and collaboration efforts with the Purchasing Entity.	• Provide clear and detailed customization requirements and collaborate with NTT DATA to develop the Statement of Work. • Communicate any changes or amendments to Orders in a timely manner. • Ensure that all necessary information and access are provided to facilitate efficient service delivery by NTT DATA. • Review and provide feedback on service delivery and collaboration efforts to support continuous improvement.

NTT DATA-SLA-08: On-Site Service and Travel Costs
If services are performed on-site, NTT DATA will adhere to the Purchasing Entity's travel policy for cost reimbursement, as specified in the Order. Our approach ensures transparency and compliance with established guidelines.

Objective: To ensure transparency and compliance with the Purchasing Entity's travel policy for cost reimbursement when services are performed on-site by NTT DATA.

Figure 26. NTT DATA-SLA-08: On-Site Service and Travel Costs

NTT DATA's Responsibilities	Purchasing Entity Responsibilities
• NTT DATA shall adhere to the Purchasing Entity's travel policy for all on-site services, ensuring that travel costs are reimbursed as specified in the Order. • NTT DATA will ensure that all travel arrangements and expenses comply with the established guidelines set forth by the Purchasing Entity. • NTT DATA will maintain detailed records of all travel-related expenses incurred during the provision of on-site services. • The Purchasing Entity will review submitted travel expense reports to ensure compliance with the travel policy and address any discrepancies. • NTT DATA will conduct regular audits of travel expenses to verify adherence to the travel policy and ensure transparency in cost reimbursement.	• Provision of Travel Policy: The Purchasing Entity shall provide NTT DATA with a detailed copy of the travel policy, including any specific guidelines or requirements for cost reimbursement. • Order Specification: The Purchasing Entity shall specify in the Order any conditions or limitations related to travel reimbursement to ensure clarity and mutual understanding. • Review and Approval: The Purchasing Entity shall promptly review and approve submitted travel expense reports, ensuring they are in accordance with the established travel policy. • Communication: The Purchasing Entity shall communicate any updates or changes to the travel policy to NTT DATA in a timely manner to ensure continued compliance.

NTT DATA-SLA-09: Communication and Documentation
NTT DATA is committed to working collaboratively with the Purchasing Entity, producing documents that are relevant, accurate, and understandable by laypersons. We prioritize clear communication and strive to ensure that all documentation is accessible to all stakeholders involved.

Objective: To ensure that NTT DATA works collaboratively with the Purchasing Entity to produce relevant, accurate, and easily understandable documents, prioritizing clear communication for all stakeholders.

Figure 27. NTT DATA-SLA-09: Communication and Documentation

NTT DATA's Responsibilities	Purchasing Entity Responsibilities
• NTT DATA collaborates closely with the Purchasing Entity to develop documentation that meets the needs of all stakeholders, ensuring accuracy and relevance. • All documents produced by NTT DATA must be written in clear, layperson-friendly language to ensure accessibility and understanding by all parties involved. • Regular feedback sessions will be held between NTT DATA and the Purchasing Entity to review the clarity, accuracy, and relevance of documentation. • NTT DATA will conduct periodic reviews of communication practices to ensure ongoing adherence to clarity and accessibility standards.	• The Purchasing Entity shall provide NTT DATA with any specific guidelines or preferences regarding documentation style and content to ensure alignment with organizational standards. • The Purchasing Entity shall participate in feedback sessions to provide insights and suggestions for enhancing document clarity and relevance. • The Purchasing Entity shall communicate any specific stakeholder needs or considerations that may impact the development of documentation.

Through these commitments, NTT DATA ensures a strong partnership with the Purchasing Entity, delivering high-quality services while safeguarding the integrity and security of the entity's data and processes.

Category 1 – Risk Assessment and Mitigation Services – Experience and Qualifications
(4th bullet) 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.*

OFFEROR'S VALUE-ADDED SERVICES:

NTT DATA is committed to delivering exceptional value beyond the standard scope of work outlined in Category 1 – Risk Assessment and Mitigation Services. **Figure 28** illustrates the core value-added cybersecurity services proposed, highlighting essential capabilities such as penetration testing, vulnerability retesting, and third-party risk management—key components for strengthening the organization's security posture and regulatory compliance.

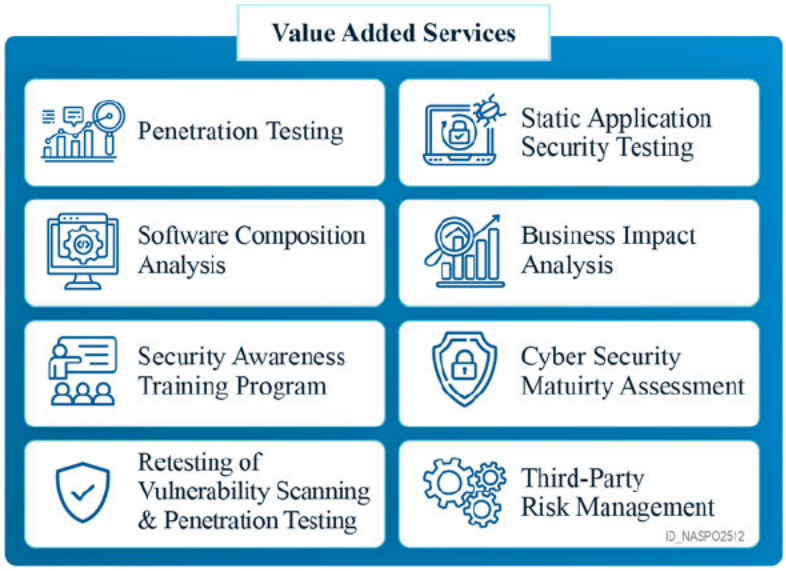


Figure 28: Value-Added Services

Our value-added services are designed to enhance and complement the core offerings, ensuring the State receives exceptional solutions that address evolving challenges and leverage innovative approaches. By offering additional services tailored to the unique needs of each client, NTT DATA will ensure that they not only receive the required services but also strategic enhancements that support long-term success and resilience. These services are designed to equip organizations with the necessary tools and insights to proactively manage risks and optimize their overall performance.

Penetration Testing: Our services have been developed to simulate cyberattacks in a controlled environment by mimicking the techniques, tactics, and procedures (TTPs) used by hostile actors to exfiltrate data. We uncover weaknesses in the network, applications, and systems to understand the security posture, prioritize vulnerabilities based on risk, and help organizations implement the necessary defenses to mitigate threats. **Figure 29** provides a high-level view of the methodology.

Key aspects of a penetration test include:

- **Types**:
  - Black box: Security assessment conducted without prior knowledge of the target system's internal workings
  - Grey box: Security assessment conducted with partial knowledge of the target system's internal workings.
  - White box: Security assessment performed with full knowledge of the target system's architecture, source code, and internal operations.

Figure 29: Penetration Testing Methodology

- **Scope:** Before the test begins, the scope is defined to determine which systems, networks, and applications will be tested. This includes identifying the boundaries and constraints of the test.
- **Reconnaissance:** Testers gather information about the target system, including details about its architecture, technologies used, and potential entry points. This phase involves passive and active information gathering techniques.
  - **Scanning:** Tools are used to identify open ports, services, and other network characteristics that could be vulnerable to attack. Scanning helps in understanding the target's landscape.
- **Attack (Exploitation):** This phase involves actively attempting to exploit identified vulnerabilities to gain unauthorized access or control over the system. Testers use various techniques and tools to mimic real-world attack scenarios.

- **Post-exploitation**: After gaining access, testers may try to escalate privileges, maintain access, or further explore the system to understand the potential impact of an attack.
- **Reporting:** A detailed report is generated, outlining the vulnerabilities discovered, the techniques used to exploit them, and recommendations for remediation. The report provides actionable insights to help improve the security posture.
- **Retest (Remediation and Follow-up)**: Based on the report, organizations should address the identified vulnerabilities and implement recommended security measures. A follow-up test may be conducted to verify the effectiveness of these changes.

NTT DATA's penetration testing methodology incorporates the best practices and standards, including the Open Web Application Security Project (OWASP) Testing Guide, Penetration Testing Execution Standard (PTES), and the Technical Guide to Information Security Testing and Assessment (NIST SP 800-115), to deliver thorough penetration tests on network infrastructures and web interfaces that encompass:

Static Application Security Testing (SAST): Our services have been developed to test software for security vulnerabilities by analyzing the source code, binaries, or bytecode before the program is run. This approach allows developers to identify and fix security issues early in the development lifecycle, typically during the coding phase, which can be more cost-effective than addressing vulnerabilities after deployment. **Figure 30** provides a high-level view of the Static Application Security Testing Process

Key features of SAST include:

- **Static Analysis:** Unlike dynamic testing methods, SAST analyzes the code without executing it, focusing on the structure and syntax to identify potential security flaws.
- **Early Detection:** By integrating SAST into the development process, developers can catch vulnerabilities as they write code, reducing the risk of security issues in production.
- **Wide Coverage:** SAST can detect a broad range of security vulnerabilities, including SQL injection, cross-site scripting (XSS), buffer overflows, and insecure coding practices.
- **Integration with Development Tools:** SAST tools can often be integrated with Integrated Development Environments (IDEs), build systems, and Continuous Integration/Continuous Deployment (CI/CD) pipelines, facilitating seamless security checks.
- **Automated and Repeatable:** SAST tools automate the process of scanning code for vulnerabilities, making it easy to perform regular checks and maintain consistent security standards.
- **Compliance and Reporting:** SAST tools typically provide detailed reports on detected vulnerabilities, assisting organizations in meeting compliance requirements and improving overall security posture.

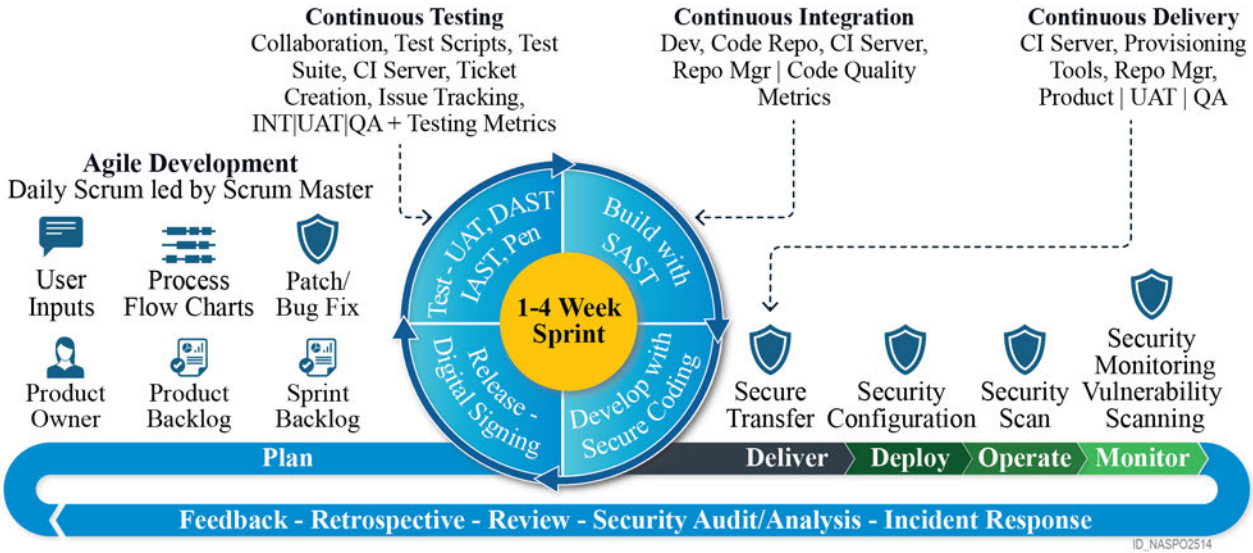


Figure 30: Static Application Security Testing Process

By using our SAST service, organizations can improve the security of their applications, reduce the cost and complexity of fixing vulnerability, and enhance their ability to comply with security standards and regulations.

Software Composition Analysis (SCA): Our services have been developed to identify and manage open-source components within a software application. As modern software development frequently involves the use of open-source libraries and components, SCA tools help organizations ensure that these components are used securely and in compliance with licensing requirements.

Key aspects of Software Composition Analysis include:

- **Identifying Components:** SCA tools scan the software to detect all open-source components and third-party libraries that are being used.
- **Vulnerability Detection:** The tools check the identified components against vulnerability databases to identify known security vulnerabilities that may affect the software.
- **License Compliance:** SCA tools review the licenses of the open-source components to ensure compliance with the legal requirements and obligations associated with their use.
- **Version Management:** The analysis helps in tracking the versions of components being used, which can be crucial for maintaining updates and patches.
- **Risk Assessment:** SCA provides insights into potential risks associated with using certain components, helping organizations make informed decisions about their software supply chain.
- **Reporting and Alerts:** SCA tools typically provide reports and alerts to inform developers and security teams about vulnerabilities, license issues, and other risks, enabling them to take corrective actions.

By using our SCA service, organizations can reduce the risk associated with open-source components, maintain compliance with legal obligations, and improve the overall security posture of their software applications. **Figure 31** provides a high-level view of the Software Composition Analysis Process

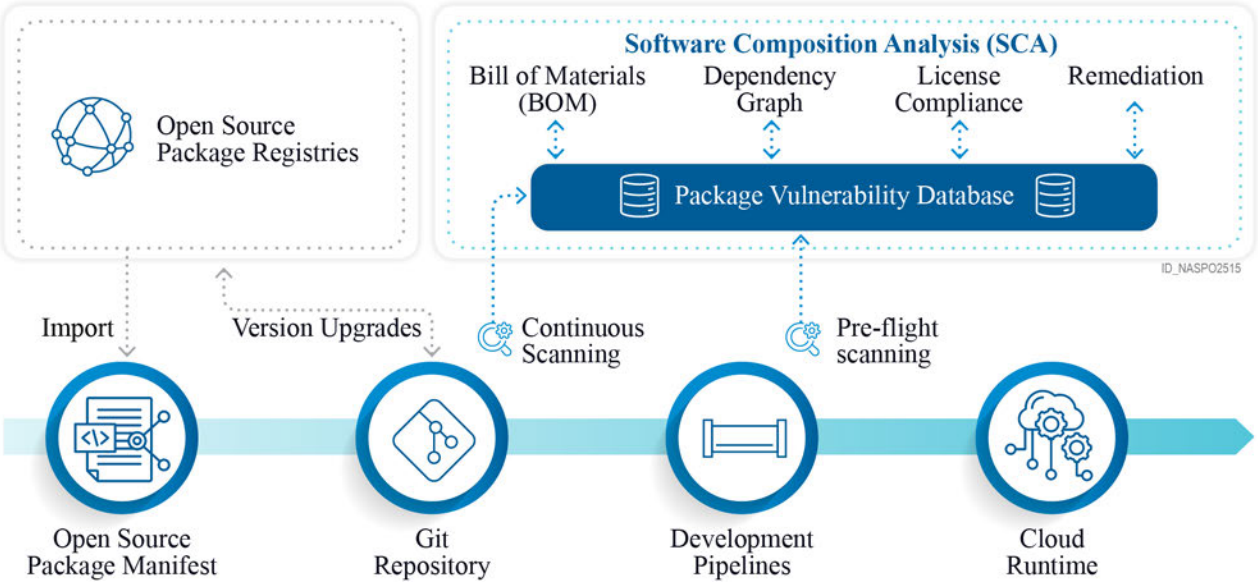


Figure 31: Software Composition Analysis Process

Retesting of Vulnerability Scanning and Penetration Testing: Our services are designed to verify that vulnerabilities identified in previous scans have been effectively remediated by the parties responsible. This retesting step is essential to confirm that the original risks have been appropriately addressed and that security measures are functioning as intended. Our independent assessment provides several key benefits: it validates the effectiveness of remediation efforts, helps maintain compliance with security standards and regulations, and supports an ongoing improvement cycle in security

practices. By ensuring no new issues have been introduced during the remediation process, we offer confidence in the overall security posture. **Figure 32** provides a high-level view of the Vulnerability Assessment and Penetration Testing (VAPT) Process

- **Retesting of Vulnerability Scanning:** Our service provides a thorough process to confirm that previously detected vulnerabilities have been effectively addressed and are no longer present. This ensures that patches, updates, or configuration changes have been correctly implemented. The process begins with a rescan, where another automated scan is conducted using the same tools and settings as the initial vulnerability scan. Next, a comparison is made between the retest results and the original scan results to verify that the previously identified vulnerabilities have been resolved. Finally, verification is performed to ensure that remediated vulnerabilities are not reappearing and to check for any new vulnerabilities that might have been introduced.
- **Retesting of Penetration Testing**: Our service provides validation whether vulnerabilities exploited during the initial penetration test have been properly mitigated and that security controls are effective in preventing similar attacks. This process begins with a review of the remediation steps taken to address the vulnerabilities identified during the initial test. Following this, a re-exploitation attempt is made using the same techniques to ensure that the vulnerabilities can no longer be exploited. Additionally, expanded testing may be conducted to ensure that remediation efforts have not introduced new vulnerabilities or weakened other parts of the system. This overall approach ensures the robustness of security controls and the overall security posture.

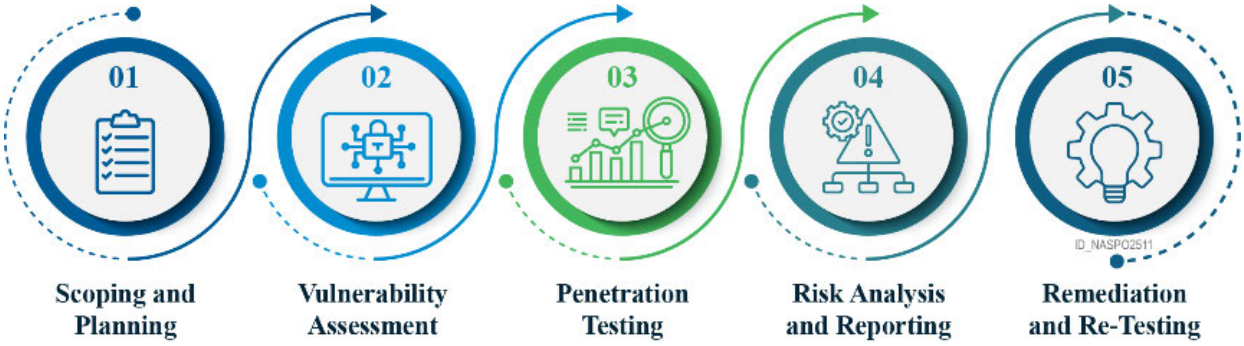


Figure 32: Vulnerability Assessment and Penetration Testing (VAPT) Process

Retesting is an essential part of the vulnerability management lifecycle because it verifies the success of remediation efforts and helps maintain a strong security posture. Regular retesting also supports continuous improvement in security processes and helps organizations adapt to evolving threats.

Business Impact Analysis: NTT DATA provides an extensive Business Impact Analysis (BIA) to help organizations safeguard their critical operations against unforeseen disruptions. **Figure 33** shows the risks of skipping a Business Impact Analysis, underscoring its importance in avoiding financial, operational, and reputational harm. Leveraging our expertise in risk management and business continuity planning, NTT DATA conducts detailed assessments to identify essential business functions, evaluate potential impacts of interruptions, and establish recovery priorities. By analyzing dependencies along with the RTO (Recovery Time Objective) and RPO (Recovery Point Objective), NTT DATA provides tailored strategies to enhance organizational resilience by leveraging a comprehensive methodology that combines business continuity and disaster recovery (BC/DR) principles with advanced risk and gap analyses. NTT DATA's approach involves creating a detailed business continuity plan (BCP) that addresses potential disruptions and outlines recovery strategies. This plan is continuously updated and validated through regular testing and exercises, ensuring that it remains effective and relevant. For example, NTT DATA has successfully developed and maintained BC/DR plans for over 50 clients, including major organizations like the Texas Department of Transportation and healthcare firms. Our BIA service not only aids in resource allocation and preparedness but also ensures compliance with regulatory standards, empowering businesses to maintain continuity and protect vital interests in the face of adversity.

- **Initiation and Planning**: NTT DATA begins the BIA process by collaborating with key stakeholders to define the scope and objectives of the analysis. This involves understanding the organization's business model, operational structure, and strategic goals. During this phase, we also establish a project plan and timeline, ensuring alignment with client's expectations and priorities.

- **Data Collection**: Utilizing surveys, interviews, and workshops, NTT DATA gathers detailed information about business processes, functions, and resources. This step involves engaging with various departments to understand critical operations, dependencies, and the impact of potential disruptions.
- **Impact Assessment**: NTT DATA analyzes the collected data to evaluate the potential impact of disruptions on business operations. This assessment includes quantifying financial losses, operational downtime, reputational damage, and compliance risks. We also identify the maximum acceptable downtime for each function.
- **Recovery Prioritization**: Based on the impact assessment, NTT DATA helps the organization establish recovery priorities. This involves determining which business functions and processes should be restored first to minimize overall impact and ensure continuity.
- **Strategy Development**: NTT DATA develops tailored strategies to enhance organizational resilience. These strategies include recommendations for resource allocation, technology investments, process improvements, and contingency planning to mitigate identified risks.
- **Documentation and Reporting**: The findings and recommendations are compiled into a comprehensive BIA report. This document provides a clear roadmap for implementing recovery strategies and serves as a reference for future business continuity planning efforts.
- **Review and Updates**: NTT DATA emphasizes the importance of regular reviews and updates to the BIA. As business operations, technologies, and external conditions change, we work with organizations to ensure the BIA remains relevant and effective, facilitating ongoing resilience and preparedness.

Figure 33: Business Impact Analysis

Security Awareness Training Programs

NTT DATA has been actively involved in providing security training within state agencies, aligning new security processes with the overarching goals and strategies of the agencies. **Figure 34** explains the importance of Security Awareness Training, which is vital for reducing risk, gaining leadership support, and fostering a culture of security across the organization. By leveraging information gathered from stakeholder analysis, NTT DATA designs training content that directly meets the identified gaps and needs. Customized training programs are designed to educate employees about recognizing and responding to security threats. These programs can be tailored to address specific organizational needs, improving overall security posture by reducing the risk of human error.

- **Needs Assessment**: NTT DATA begins by conducting a thorough assessment to understand the organization's specific security challenges, risks, and goals. This involves engaging with key stakeholders to identify the types of security threats employees may encounter and determine the areas where training can have the most impact.

- **Curriculum Development**: Based on the assessment of needs, we will develop a customized training curriculum that addresses the unique security concerns of the organization. This curriculum is designed to be relevant, engaging and covering topics such as threat recognition, response protocols, and best practices for maintaining security.
- **Content Creation**: NTT DATA creates training materials, including presentations, handouts, and interactive modules, tailored to the organization's specific requirements. The content is designed to be accessible and understandable, ensuring employees at all levels can grasp the concepts and apply them in real-world situations.
- **Interactive Learning**: To reinforce learning and encourage active participation, NTT DATA incorporates interactive elements such as simulations, role-playing exercises, and quizzes. These activities help employees practice their skills in recognizing and responding to security threats effectively.
- **Evaluation and Feedback**: After the training, NTT DATA gathers feedback from participants to evaluate the effectiveness of the program. This feedback is used to assess the impact of the training on employees' ability to recognize and respond to security threats and to identify areas for improvement.
- **Follow-Up and Support**: NTT DATA provides follow-up support to ensure employees continue to apply the knowledge and skills gained from the training. This may include refresher courses, updates on emerging threats, and ongoing access to resources for continued learning.

Figure 34. Security Awareness Training

Cybersecurity Maturity Assessments

NTT DATA has a long history of conducting cybersecurity assessments that deliver actionable insights and recommendations to enhance security frameworks. **Figure 35** illustrates the value of conducting an Information Security Maturity Assessment, which is essential for improving governance, increasing visibility, aligning with policies, and driving measurable returns on security investments. Our experience spans various sectors and aligns with industry best practices, including standards such as NIST, ISO, and OWASP. Through our engagements, NTT DATA has consistently demonstrated the ability to improve the maturity of organizations' cybersecurity practices. NTT DATA conducted a complete MARS-E assessment, which included a thorough review of the application and security infrastructure posture. This assessment provided the Department of Children & Families

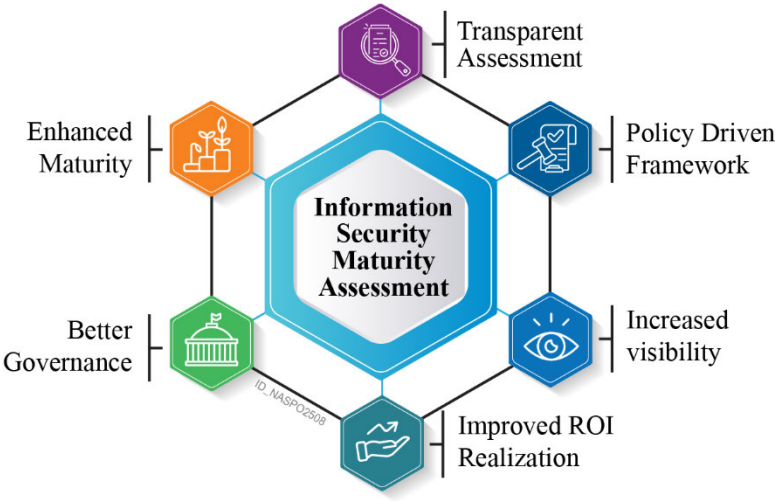


Figure 35. Information Security Maturity Assessment

(DCF) with risk guidance and remediation strategies that significantly improved their security without imposing substantial resource constraints. NTT DATA conducts assessments to evaluate the maturity of the State cybersecurity practices. This service provides actionable insights and recommendations for improving security frameworks and aligning them with industry's best practices.

- **Preparation and Planning**: NTT DATA begins by understanding the organization's objectives, scope of the assessment, and specific areas of concern. This involves initial meetings with key stakeholders to set expectations and tailor the assessment process to the organization's needs.
- **Data Collection**: NTT DATA collects relevant data on the organization's cybersecurity policies, procedures, technologies, and practices. This may involve reviewing documentation, interviewing personnel, and analyzing existing security tools and systems.
- **Maturity Model Selection**: Depending on the industry and specific requirements, NTT DATA selects an appropriate cybersecurity maturity model or framework (e.g., NIST Cybersecurity Framework, CIS Controls) to benchmark the organization's practices.
- **Assessment Execution**: Using the selected maturity model, NTT DATA evaluates the organization's cybersecurity practices across various domains, such as governance, risk management, incident response, and technical controls. This involves identifying strengths, weaknesses, and gaps in the current security posture.
- **Analysis and Insight Generation**: NTT DATA analyzes the assessment findings to provide insights into the organization's cybersecurity maturity level. We identify areas where improvements are needed and highlight strengths that can be leveraged for future enhancements.
- **Recommendations Development**: Based on the insights gained, NTT DATA develops actionable recommendations for improving the organization's security framework. These recommendations are aligned with best practices and tailored to address specific gaps and vulnerabilities.
- **Reporting and Presentation**: NTT DATA compiles the assessment findings and recommendations into an extensive and thorough report. This report is presented to stakeholders, providing a clear understanding of the current maturity level and outlining a roadmap for improvement.
- **Feedback and Iteration**: NTT DATA seeks feedback from the organization on the assessment process and findings. This feedback is used to refine recommendations and ensure they are practical and aligned with the organization's strategic goals.
- **Advisory Support and Follow-Up**: NTT DATA offers ongoing advisory support to help the organization implement the recommended improvements. This may include follow-up assessments, guidance on specific initiatives, and updates on emerging cybersecurity trends and threats.

Third-Party Risk Management

NTT DATA will assess and manage risks associated with third-party vendors. **Figure 36** outlines the core components of third-party risk management—identification, assessment, mitigation, and monitoring—which are vital for minimizing vendor-related risks and protecting organizational assets. This includes evaluating vendor security practices and ensuring compliance with contractual obligations related to data protection and privacy.

- **Vendor Identification and Classification**: NTT DATA begins by identifying all third-party vendors that have access to the organization's data or systems. Vendors are then classified based on the level of risk they pose, which might depend on factors such as the type of data they handle and their access to critical systems.
- **Risk Assessment**: NTT DATA conducts a thorough risk assessment for each vendor. This includes evaluating the vendor's security practices, policies, and procedures related to data protection and privacy. The assessment looks for potential vulnerabilities and assesses the likelihood and impact of various risks.
- **Due Diligence and Compliance Evaluation**: NTT DATA performs due diligence to ensure that vendors comply with relevant regulatory requirements and contractual obligations. This includes reviewing certifications, audit reports, and compliance with standards.

- **Security Questionnaire and Review**: Vendors may be required to complete detailed security questionnaires that cover aspects such as data encryption, access controls, incident response plans, and business continuity measures. NTT DATA reviews the responses to identify any gaps or areas of concern.
- **On-site Visits and Audits**: For high-risk vendors, NTT DATA may conduct on-site visits or audits to verify the implementation of security measures and ensure that the vendor adheres to agreed-upon practices. This provides a deeper understanding of the vendor's security posture.
- **Contractual Safeguards**: NTT DATA ensures that contracts with vendors include appropriate safeguards and clauses related to data protection and privacy. This might involve specifying security requirements, data handling protocols, breach notification procedures, and penalties for non-compliance.
- **Ongoing Monitoring and Management**: Risk management is an ongoing process. NTT DATA sets up mechanisms for continuous monitoring of vendor performance and compliance. This can include regular security reviews, updates on risk assessments, and the establishment of clear communication channels for reporting and addressing security issues.

Figure 36. Third Party Risk Management

- **Risk Mitigation and Remediation**: If any risks or issues are identified, NTT DATA works with the vendor to implement mitigation strategies and remediation plans. This may involve additional security measures, process improvements, or, in some cases, reevaluating the vendor relationship.
- **Reporting and Documentation**: Throughout the process, NTT DATA maintains detailed documentation of assessments, findings, and actions taken. This documentation supports transparency, accountability, and provides a record for future reference or audits.

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

- **(ME) Category 2 – Offeror's Experience. Describe your company's experience,** demonstrating that your company has a minimum of five (5) years of experience providing services similar in scope and size to the Category 2 Incident Response Services required in Attachment 02 Scope of Work. Provide specific examples that illustrate the specific services furnished and the size, composition, etc. of the entities for whom you have provided services that you are using to demonstrate that your experience meets this minimum requirement.
- **(ME) Category 2 Contractor Staff – Experience and Qualifications. Describe in detail the experience and qualifications** that you will require for your Contractor staff who will be performing Category 2 Incident Response Services, see Attachment 02, Section 3.9 for minimum qualifications. Include relevant certifications (such as, but not limited to, SANS Certified Incident Handler (GCIH), EC-Council Incident Handler (ECIH) and ENCASE certified) and any areas of specialization.
- **(ME) Category 2 Customer Service Representatives – Qualifications.** All call center customer service representatives must have excellent customer service skills and be able to communicate clearly in English. **Describe in detail the minimum qualifications and training** for customer service representatives to be used in servicing the NASPO ValuePoint Master Agreement.
- **(ME) SLA's.** Describe your company's SLA's surrounding Category 2 Services. Include response times, responsibilities of both the Contractor and Participating Entity and any other relevant information surrounding the levels of service.
- **Value-Added Services.** Describe any services related to Category 2 that were not included in the SOW that your company can offer. Prices for any Value-Added Services must be detailed in your response to Attachment 09.

OFFEROR'S RESPONSE TO CATEGORY 2:
Not Applicable. NTT DATA is offering a response to category 1 services exclusively, as indicated on page 1.

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.
- **(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.
- **(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.
- **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.

OFFEROR'S RESPONSE TO CATEGORY 3:
Not Applicable. NTT DATA is offering a response to category 1 services exclusively, as indicated on page 1.

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.

OFFEROR'S RESPONSE TO CATEGORY 4:
Not Applicable. NTT DATA is offering a response to category 1 services exclusively, as indicated on page 1.

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.

OFFEROR'S SUBCONTRACTORS:
NTT DATA is committed to delivering high quality services directly through our own experienced and highly qualified team. We will not be utilizing subcontractors, ensuring that all work is performed by NTT DATA employees. This approach allows us to maintain complete control over the quality, consistency, and security of the services provided, ensuring that our clients receive the full benefit of our expertise and resources.

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

- 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.
- 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.
- Describe how you intend to encourage adoption and usage of your Master Agreement by Participating and Purchasing Entities.
- Describe your approach to negotiation of Participating Addenda. Describe the extent to which you will provide Participating Entities flexibility in incorporating entity-specific language into their Participating Addenda. (*e.g.*, Do you require entities to provide statutory citations for their entity-specific language? Are you able to devote resources to simultaneous negotiation of multiple Participating Addenda?)
- Describe your ability to provide products and services immediately upon execution of a Master Agreement and Participating Addenda.
- 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.

OFFEROR'S EXPERIENCE WITH STATEWIDE OR LARGE CONSORTIUM CONTRACTS:

(ME) Offeror's Experience with Statewide or Large Consortium Contracts
(1st bullet) *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.*

We have successfully delivered these services to a diverse range of organizations, from small municipalities with limited resources and straightforward IT needs, to large, statewide agencies overseeing thousands of endpoints and operating within complex, multi-cloud environments. Our experience spans supporting local governments that require tailored, cost-effective solutions, as well as enterprise-scale deployments that demand resilient security, seamless integration, and high availability across multiple platforms and cloud providers. This breadth of experience enables us to effectively address the unique challenges and requirements of each client, regardless of their size or technical landscape.

Figure 37. Statewide or Large Consortium Contracts

Contract Agency and Date of Contract	Description
Wyoming Department of Health, Division of Healthcare Financing April 2023 – April 2029	NTT DATA provides Comprehensive Security Testing Services (CSTS) for the Wyoming Department of Health, Division of Healthcare Financing, covering eighteen systems managed by individual task orders. These services enhance the Department's and its vendors' security testing efforts, focusing on risk management by accurately assessing risk profiles, selecting suitable controls, ensuring their proper implementation, and conducting regular validations. **Key Activities and Deliverables:** • Conducted extensive infrastructure and application testing, including vulnerability scanning, penetration testing, control reviews, security control assessments, and audits of security documentation. • Collaborated with the agency and vendors throughout the testing process, with subsequent re-testing of applications when feasible. • Ensured adherence to specific security frameworks as dictated by individual vendor contracts. • Provided comprehensive deliverables, including rules of engagement, security assessment reports (SAR), vulnerability assessment and penetration testing reports (VAPT), and plan of action and milestone reports (POA&M).

Contract Agency and Date of Contract	Description
	• Executed all tasks remotely while maintaining regular communication between NTT DATA's Security team, WDH representatives, and WDH vendors. **Outcomes:** • **Validation of Security Controls:** Ensured that security controls were functioning effectively, confirming adequate protection against security threats. • **Identification of Vulnerabilities:** Uncovered vulnerabilities within applications and infrastructure, allowing for prioritized remediation and reduced risk of exploitation. • **Enhanced Risk Mitigation:** Provided insights for refining risk mitigation strategies, enabling informed decision-making and resource allocation. • **Improved Vendor Collaboration:** Facilitated a shared understanding of security expectations, leading to consistent and effective security practices. • **Continuous Security Improvement:** Periodic retesting ensured continuous evaluation and improvement of security measures. • **Detailed Reporting and Action Plans:** Offered detailed insights and actionable recommendations through comprehensive reports, aiding in tracking progress and planning future security initiatives. The goal of the testing is to strengthen the confidentiality, integrity, and availability of the system and its data, protecting against exploits, malicious actors, data exfiltration, and ransomware attacks. The contract spans from February 2023 to February 2029, with an approximate value of $4,200,000.00.
State of Utah Cloud Solutions Contract – NASPO October 2016 – September 2026	NTT DATA was awarded the NASPO ValuePoint Cloud Solutions contracts, providing a variety of cloud solutions based on Infrastructure as a Solution (IaaS). This cooperative purchasing organization streamlines procurement processes for states, reducing time and costs. NTT DATA has been working with contracting cooperatives since September 2016. **Key Activities and Deliverables:** • Provisioning and configuring virtual machines (VMs) and physical servers for various environments, including Windows, Linux, AIX, and iSeries. This includes operating system installation, patching, upgrades, network connectivity setup, storage allocation, and security group configuration. • Assessing current IT infrastructure, identifying critical workloads, and designing disaster recovery plans. This involves replicating data to secondary sites and conducting regular disaster recovery drills. • Designing and deploying virtual desktop infrastructure (VDI) environments, integrating with directory services for user authentication, and configuring user access policies. • Applying patches and updates, providing 24x7 monitoring, remote troubleshooting, and performing routine maintenance. **Outcomes:** • Data security was a major focus in the RFP, evaluation process, and Master Agreements. • Master Agreements provide access to technical capabilities in cloud environments that meet NIST Essential Characteristics. • The contractual arrangements allow states to procure services on a task-order, project-based approach, mitigating vendor protest risks and enabling predictable pricing and shared resources. • This approach leads to more efficient and effective procurement outcomes. NTT DATA's collaborative approach has empowered states to achieve efficient procurement outcomes through predictable pricing and shared resources. The sales volume for these cloud services is $4,427,415.18.

Contract Agency and Date of Contract	Description
Oklahoma Care Management Consulting January 2020 – June 2024	NTT DATA signed an MSA for the Oklahoma Medicaid Enterprise System (MES) Project, supporting procurement, planning, design, development, implementation oversight of state and federally funded IT systems. The scope expanded to include cloud advisory services for the Oklahoma Health Care Authority's (OHCA) MMIS transition, as well as project management and support for OHCA's Care Management and Electronic Visit Verification (EVV) projects. **Key Activities and Deliverables:** • Enhanced the efficiency and effectiveness of the OHCA modular MES. • Completed projects including Pharmacy Electronic Prior Authorization (ePA), Cloud Advisory Services, Care Management, and EVV. • Utilized NTT DATA's Enterprise Advantage, Testing Advantage, and Certification Advantage. • Addressed a lack of vendor testing by reallocating resources to the User Acceptance Testing (UAT) team, reducing the burden on the state team and allowing for comprehensive testing of the Care Management module. **Outcomes:** • Identified early project risks related to requirements management, leading to governance changes that improved requirements definition and reduced UAT defects. • Led OHCA UAT, uncovering over 500 defects before go-live, ensuring high-quality implementation with minimal post-launch issues. • Provided UAT evidence for CMS and MITRE review, facilitating the Operational Readiness Review (ORR) due to insufficient vendor System Integration Testing (SIT). NTT DATA's involvement ensured that the projects were implemented effectively, with a focus on comprehensive testing and improved governance, ultimately enhancing the quality and success of the OHCA initiatives. The contract spanned from January 2020 through June 2024 with a value of $1,825,524.

(ME) Offeror's Experience with Statewide or Large Consortium Contracts
***(2nd bullet)** Describe how you intend to market your Master Agreement and encourage participation among potential Participating Entities, including state governments.*

NTT DATA works with a variety of state agencies—some of them participate in NASPO. Our growth and work with these agencies is the result of a combination of key wins and smart investments in an experienced and talented sales and management team, as well as a dedicated, professional support operations team. Many of our client relationships have been established for more than a decade, spanning numerous projects and services provided. NTT DATA will leverage these teams to promote support for this contract.

Specifically, our plan is to establish a marketing campaign to promote the contract to participating agencies, like how we would in rolling out a new solution or service. To establish and run this marketing campaign, we will engage our client executives, identify prospects, establish a marketing communication plan, produce campaign materials, execute the marketing communication plan, and measure results.

We will review each of these steps in the rest of this section. Simply put, NTT DATA is a global company with experience, resources, and processes to ensure a successful campaign for security services.

Engage Client Executives: NTT DATA actively works on building an understanding of our client's business and associated security needs. The Client Executive works to understand the specific needs, dependencies, and constraints and the associated timing requirements. This key role is a focal point of marketing the collaborative services to the client. Our leaders work

together to identify prospects, define marketing communication plans, communicating capabilities and measuring the results.

Identify Prospects: If contact information for potential targets is not already available from NASPO, we will capture that information from existing internal contact details and other publicly available sources and store it in a campaign folder in our customer relationship management system. By establishing a campaign, we enable a variety of features that we can use for connecting with prospects, who will likely be participating as agency decision makers. Our marketing campaign will begin with the states interested in participating in this master agreement including Arizona, Colorado, Rhode Island, South Dakota, and Vermont. We will then expand our marketing to other existing clients as well as states seeking these services

Establish a Marketing Communication Plan: At this time, we anticipate two key approaches for promoting this contract. First, NTT DATA will create outreach communication using email and outbound telephone calls to alert prospects to the availability of the contract. In these communications, we will educate prospects on the importance of structured procurement services in government agencies and share ongoing results of the program. By sharing information about the relationship between quality procurements and successful solution deliveries, our goal is to gain interest and acceptance from prospects that do not know much about it. Second, we will prepare relevant information that is similar to our outreach communications for our sales teams. These sales teams will contact prospects directly to discuss our solutions and services and seek to gain commitment for participation.

Produce Campaign Materials: Once we have established a marketing communication plan, NTT DATA will engage our marketing operations team to produce the required materials. This team includes graphic artists and technical writers with a history of producing quality materials.

Execute the Marketing Communication Plan: Once our marketing operations team has produced the materials we need for the marketing campaign, we will distribute them. We will then begin to execute and measure the campaign.

Measure Results: Quarterly, NTT DATA will review the results of the campaign and plan activities for the next quarter, improving our efforts as part of an iterative process.

NTT DATA's marketing approach is differentiated by several key factors:

- **Proven Expertise.** NTT DATA communicates our long-standing history of successfully partnering with state governments to deliver effective procurement projects on time and within budget.
- **Customized Solutions.** We tailor the messaging of our procurement offerings to meet the specific business needs of each client, ensuring that our approach delivers relevant and impactful procurements for each state client.
- **Strong Relationships.** Our established relationships with government officials and agencies enable us to effectively communicate the benefits of the Master Agreement and our team's ability to deliver.
- **Comprehensive Support.** NTT DATA provides ongoing support and guidance to ensure that Participating Entities can fully realize the benefits of the agreement.
- **Transparent Communication.** We prioritize open and transparent communication to build trust and foster collaboration with all stakeholders involved in the agreement.

These differentiators position NTT DATA as a trusted partner for state governments and other Participating Entities looking to leverage the Master Agreement for their strategic initiatives.

(ME) Offeror's Experience with Statewide or Large Consortium Contracts
***(3rd bullet)** 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.*

NTT DATA's dedicated website for the Master Agreement will be designed to provide an all-encompassing and user-friendly experience for Participating Entities. **Figure 38** is a draft example of the website that will be established for this Master Agreement where Idaho is the lead State.

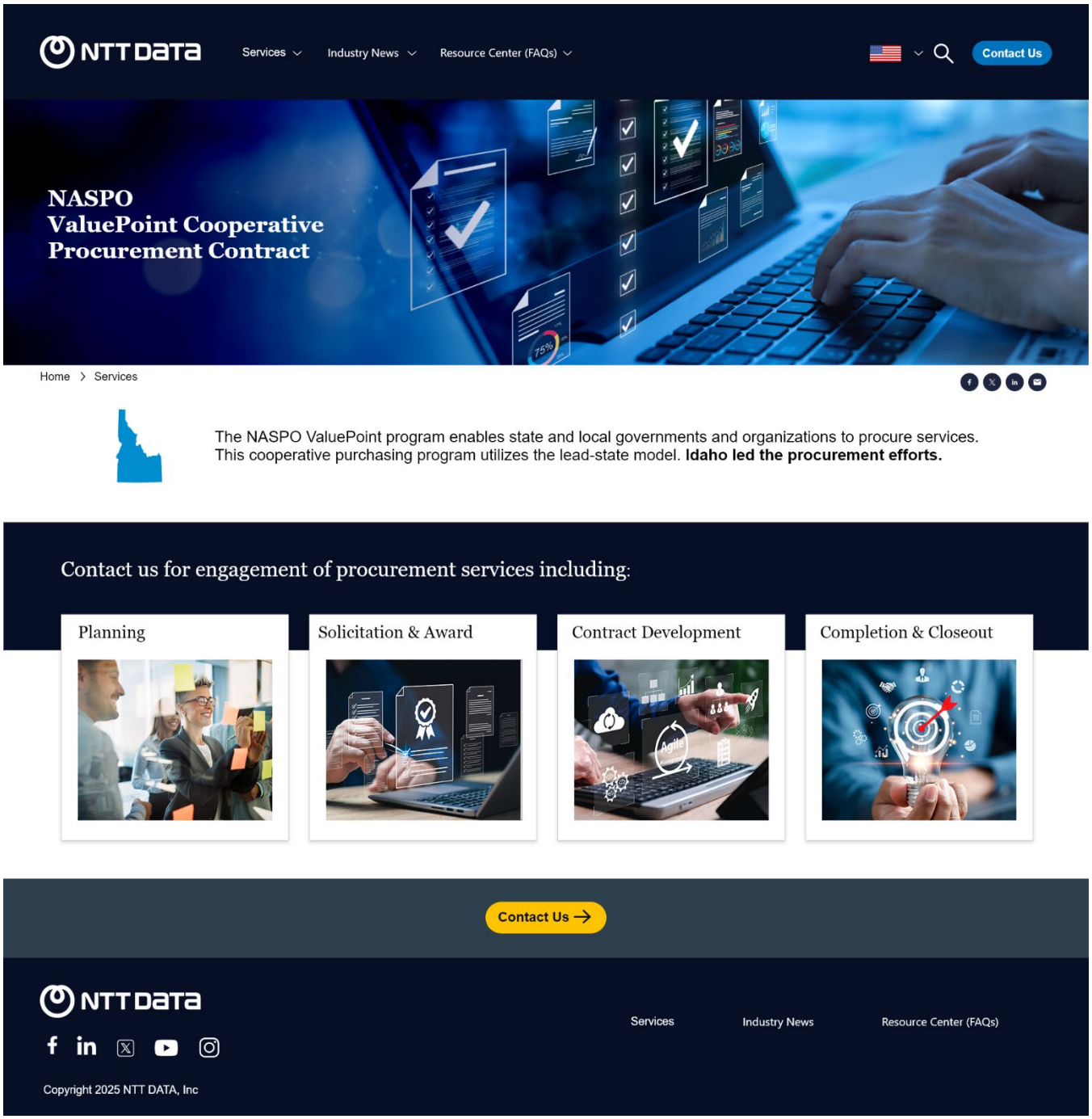


Figure 38: Example NASPO Procurement and IT Research Draft Portal

Key features of the website will include:

- **Customized Price Lists.** The website will offer customized price lists tailored to each Participating Entity. These lists will reflect the specific terms and pricing agreed upon in the Participating Addenda, ensuring that each entity has access to accurate and relevant pricing information.
- **Staff Contact Information.** The website will include detailed contact information for key staff members involved in the Master Agreement. This will facilitate direct communication between Participating Entities and NTT DATA personnel, ensuring that entities can quickly and easily reach out for support or inquiries.

- **Resource Center.** The website will host a resource center containing documentation, FAQs, and training materials related to the Master Agreement. This will provide Participating Entities with easy access to important information and guidance on utilizing the agreement effectively.
- **News and Updates.** A dedicated section for news and updates will keep Participating Entities informed about any changes or developments related to the Master Agreement. This will include notifications about new services, pricing adjustments, and other relevant information.
- **Feedback and Support.** Participating Entities will have the opportunity to provide feedback and request support through the website. This will ensure that entities can communicate their needs and concerns directly to us, facilitating continuous improvement in service delivery.

By incorporating these features, we aim to create a robust online platform that enhances the accessibility and usability of the Master Agreement for all Participating Entities. This approach will ensure that entities can efficiently manage their interactions with NTT DATA and fully leverage the benefits of the agreement.

(ME) Offeror's Experience with Statewide or Large Consortium Contracts
(4th bullet) *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.*

Master Agreement Staff Allocation
The NTT DATA team allocated to this Master Agreement is comprised of individuals with deep industry and cybersecurity service experience. NTT DATA will utilize our Program Directors to facilitate connecting our various State clients with this NASPO ValuePoint Master Agreement.

Program Directors: All of our Program Directors have extensive experience in developing and managing federal, state, and local government grants and contracts. Their expertise includes overseeing procurements (RFPs, ITBs, RFIs, RFQs), defining business functional and non-functional requirements, conducting proposal evaluations, performing market research and analysis, and managing budgets to support strategic HHS IT and programmatic needs.

Staff Training
To ensure that all NTT DATA staff members are familiar with the Master Agreement terms and pricing, NTT DATA will provide in-depth, yet tailored training programs. These programs will cover the specifics of the Master Agreement, including detailed pricing structures, compliance requirements, and service delivery expectations. Training will be tailored to the role-specific needs of each staff category, ensuring that everyone from Project Managers to Technical Specialists have the knowledge necessary to perform their duties effectively.

The Program Director, with support from the Project Manager, will oversee the implementation and adherence to the Master Agreement, ensuring that all aspects are executed according to plan. The Project Manager will structure and align with the business requirements. Writers and editors will focus on development and refinement of procurement content to ensure smooth procurement results.

Program Directors will provide strategic oversight and guidance to ensure that all activities align with the Master Agreement's objectives. By employing a staffing and training strategy, our team is equipped to deliver outstanding service and compliance with the Master Agreement, fostering successful outcomes for all Participating Entities.

(ME) Offeror's Experience with Statewide or Large Consortium Contracts
(5th bullet) *Describe how you intend to encourage adoption and usage of your Master Agreement by Participating and Purchasing Entities.*

To encourage adoption and usage of the Master Agreement by Participating and Purchasing Entities, NTT DATA employs a strategic approach that focuses on clear communication, robust support, and continuous engagement with stakeholders.

Clear Communication and Education:
NTT DATA ensures that all Participating and Purchasing Entities are fully informed about the benefits and components of the Master Agreement. We provide detailed documentation and conduct workshops to explain the terms, benefits, and

procedures associated with the agreement. This helps stakeholders understand how the Master Agreement can meet their specific needs and streamline their procurement processes.

Stakeholder Engagement:
NTT DATA actively engages with Participating and Purchasing Entities through regular meetings, feedback sessions, and collaborative planning. This engagement allows us to tailor our offerings to better meet the needs of each entity and address any potential barriers to adoption. We also gather feedback to continuously improve our services and adapt to changing requirements.

Customization and Flexibility:
The Master Agreement is designed to be flexible, allowing entities to customize services according to their specific requirements. This flexibility encourages entities to adopt the agreement as it can be tailored to fit their unique operational needs and goals. We work closely with each entity to develop Statements of Work that reflect their priorities and objectives.

Demonstrating Value and Success:
NTT DATA shares success stories and case studies from other entities that have benefited from the Master Agreement. By highlighting tangible results and positive outcomes, we demonstrate the value of the agreement and encourage more entities to participate.

Through these efforts, NTT DATA aims to maximize the adoption and usage of the Master Agreement, ensuring that Participating and Purchasing Entities can fully leverage its benefits to achieve their operational and strategic objectives.

(ME) Offeror's Experience with Statewide or Large Consortium Contracts
(6th bullet) *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?)*

NTT DATA employs a flexible and collaborative approach to the negotiation of Participating Addenda, providing Participating Entities with the ability to incorporate entity-specific language as needed. Our approach is centered on understanding the unique requirements and statutory obligations of each Participating Entity. This includes allowing entities to propose specific language that reflects their operational needs and legal requirements. NTT DATA does not require entities to provide statutory citations for their entity-specific language, but we encourage clarity and rationale to facilitate a mutual understanding and agreement.

NTT DATA is committed to devoting the necessary resources to manage the simultaneous negotiation of multiple Participating Addenda. Our experienced negotiation teams are equipped to handle multiple discussions concurrently, ensuring that each Participating Entity receives the attention and customization to meet its specific needs. This capability is supported by our robust project management tools and methodologies which allow us to track progress, manage resources, and ensure timely completion of negotiations.

In providing flexibility, NTT DATA understands that each Participating Entity operates under different legal frameworks and operational contexts. As such, we are open to incorporating entity-specific clauses that align with their statutory requirements and operational goals. This flexibility extends to the inclusion of additional terms that may be necessary to address local policies or procedures, provided they do not conflict with the overarching terms of the Master Agreement.

NTT DATA's negotiation process is guided by principles of transparency, collaboration, and mutual benefit. We strive to create agreements that are fair, equitable, and tailored to the specific needs of each Participating Entity. By maintaining open lines of communication and fostering a spirit of partnership, we aim to build lasting relationships that support the successful implementation and operation of services under the Master Agreement.

Key differentiators of NTT DATA's approach to negotiating Participating Addenda include:

- ***Customizability.*** *The ability to incorporate entity-specific language that meets the unique needs of each Participating Entity.*
- ***Resource Allocation.*** *Commitment to providing dedicated resources for the simultaneous negotiation of multiple*

addenda.

- ***Transparency and Collaboration.*** *Emphasis on open communication and partnership throughout the negotiation process.*
- ***Experience and Expertise.*** *Extensive experience in managing complex negotiations with government entities, ensuring compliance with statutory and operational requirements.*
- ***Proven Methodologies.*** *Utilization of robust project management and negotiation tools to track progress and ensure timely completion of agreements.*

These elements collectively position NTT DATA as a capable and reliable partner for state governments and other Participating Entities seeking to negotiate Participating Addenda under the Master Agreement.

(ME) Offeror's Experience with Statewide or Large Consortium Contracts
(7th bullet) *Describe your ability to provide products and services immediately upon execution of a Master Agreement and Participating Addenda.*

NTT DATA is prepared to provide products and services immediately upon the execution of a Master Agreement and Participating Addenda. Our readiness is a result of key factors that enable us to mobilize quickly and deliver efficiently:

- A robust infrastructure and a skilled workforce that is scalable and adaptable to meet client needs. We have established processes and methodologies that allow us to transition seamlessly from contract execution to service delivery. Additionally, our team is experienced in rapid deployment strategies, ensuring that all necessary resources, tools, and personnel are aligned and ready to commence work as soon as agreements are finalized. This includes having pre-configured templates and frameworks that can be quickly customized to suit the specific requirements of each Participating Entity.
- Advanced project management tools and techniques to coordinate activities across multiple teams and locations, facilitating a cohesive and synchronized start to service delivery. We ensure that all project stakeholders are informed and aligned with the project goals and timelines, which supports a smooth and efficient rollout of services.

Our commitment to quality and customer satisfaction drives us to maintain high readiness levels. This readiness is further supported by our ongoing investments in technology and training, ensuring that our teams are equipped with the latest skills and knowledge to deliver exceptional service from day one.

Key differentiators in NTT DATA's approach include:

- ***Rapid Mobilization.*** *Ability to quickly deploy resources and commence work immediately after contract execution.*
- ***Leveraged Templates and Processes.*** *Robust and adaptable templates supporting quick engagement and deployment.*
- ***Advanced Project Management.*** *Use of sophisticated tools and methodologies to ensure efficient coordination and execution.*
- ***A Broad Network.*** *Strong partnerships and supplier networks to ensure timely procurement and delivery of resources.*
- ***Continuous Improvement.*** *Ongoing investments in technology and training to maintain high levels of service readiness and quality.*

These elements ensure that NTT DATA can effectively meet the immediate needs of our clients upon the execution of the Master Agreement and Participating Addenda.

(ME) Offeror's Experience with Statewide or Large Consortium Contracts
(8th bullet) *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.*

NTT DATA ensures that summary and detailed sales information is promptly, completely, and accurately reported through a detailed, flexible, yet structured approach. This involves implementing a robust data management and reporting framework designed to facilitate seamless data collection and aggregation. Our approach includes the following key components:

- **Central Sales Data Management.** We have a formal contract and sales reporting structure that pools the sales documents for retention and reporting.
- **Standardized Reporting Processes.** We establish standardized processes and templates for our state account leaders to report sales data. This ensures consistency in data collection and facilitates accurate aggregation.
- **Collaborative Partnerships.** We foster strong relationships with our state clients, encouraging open communication and collaboration. This collaborative approach ensures that we are aligned with our reporting objectives and committed to providing timely and accurate data.
- **Compliance Checks and Audits.** We conduct regular compliance checks and audits to verify the accuracy and completeness of the sales data reported. This includes cross-referencing reported data with internal records and addressing any identified issues promptly.
- **Resource Allocation for Data Management.** We have dedicated resources to manage the sales data aggregation and reporting process. These resources are responsible for ensuring compliance with NASPO ValuePoint reporting requirements and addressing any challenges.
- **Scalable Infrastructure**. Our infrastructure is designed to scale with the volume of data, ensuring that we can handle the aggregation and reporting needs of multiple partners simultaneously.

By implementing these strategies, NTT DATA ensures that sales information is reported accurately and efficiently, meeting the compliance requirements of the Master Agreement with NASPO ValuePoint. Our commitment to quality and accuracy in data reporting is a testament to our dedication to maintaining the integrity of our client relationships and delivering exceptional service.

G. (ME) Customer Service

- Identify your customer service hours of operation and when key account staff are available.
- Describe how you handle problem identification and resolution. Describe how you respond to and resolve customer complaints and service issues.
- Describe how you will assess customer satisfaction.

OFFEROR'S CUSTOMER SERVICE:

(ME) Customer Service
(1st bullet) *Identify your customer service hours of operation and when key account staff are available.*

NTT DATA operates customer service during core business hours, typically from 8:00 a.m. to 5:00 p.m. local time, Monday through Friday for the Participating and Purchasing Entities. Our key account staff are available during these hours to address client needs and ensure seamless service delivery. We ensure that designated personnel are accessible for critical support beyond standard hours if required, ensuring that urgent client needs are met promptly.

(ME) Customer Service
(2nd bullet) *Describe how you handle problem identification and resolution. Describe how you respond to and resolve customer complaints and service issues.*

NTT DATA utilizes a methodical approach to effectively identify and resolve problems. Our process commences with the prioritization of customer complaints and service issues. We ensure a comprehensive understanding of the situation from the outset. To address the problem, we develop specific and actionable steps. Our contract manager conducts a thorough investigation to ascertain the root cause and establishes quantifiable objectives to evaluate the effectiveness of the implemented solutions. Throughout the resolution process, we maintain transparent communication with clients, providing regular updates and soliciting feedback to ensure alignment with their expectations. Our objective is to resolve issues promptly and efficiently while ensuring client satisfaction and mitigating recurrence through continuous improvement initiatives.

(ME) Customer Service
(3rd bullet) *Describe how you will assess customer satisfaction.*

NTT DATA assesses customer satisfaction through regular client surveys and the Net Promoter Score (NPS) metric. These tools help us gauge client satisfaction levels and identify areas for improvement. We conduct annual surveys to collect detailed feedback on our services, which inform us of our strategies for service enhancement. Our commitment to maintaining high levels of customer satisfaction is reflected in our consistent achievement of high NPS ratings, indicating strong client trust and the likelihood of recommending our services to others.

Figure 39. Excellent Service

To further ensure customer satisfaction, our contract manager, Patti Garofalo, evaluates customer satisfaction of the services provided. This involves assessing whether deliverables meet the client's expectations and identifying any areas for improvement. By conducting regular contract manager meetings with a focus on customer satisfaction, we ensure that the team is responsive to client needs, maintain high service standards, and build strong, lasting partnerships with the Participating and Purchasing Entities.

Through these measures, NTT DATA ensures that our customer service remains responsive, effective, and aligns with client needs, fostering long-term relationships and successful project outcomes.

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

OFFEROR'S AICPA SOC 2 COMPLIANCE:

NTT DATA possesses equivalent compliance with the ISO/IEC 27001:2013, standard for information security management systems. This complies with a wide array of standards, including the applicable laws and regulations in our operating regions, the SOC 1 and SOC 2 auditing framework, and specific domain standards, such as those from the Health Information Trust Alliance (HITRUST) and HIPAA.

NTT DATA provides information technology managed infrastructure services from its Technology Centers located in Plano, Texas, Florence, Kentucky and Quincy, Washington. NTT DATA is committed to protecting client information. The company's Information Security Management System (ISMS) is applicable to the IT environment, data systems, tools and networks necessary to support NTT DATA Services information technology managed infrastructure services.

NTT DATA is a quality-driven organization that has earned the following quality certification:

- ISO/IEC 27001:2013 is current and the certification number is 0000380406-MSC-UKAS-IND.

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.

OFFEROR'S USE OF AI TECHNOLOGIES FOR PROPOSED WORK:

As part of our penetration testing methodology, and when the engagement explicitly permits its use, we utilize Burp Suite's integrated AI Assistant which is powered by the Claude large language model (LLM). This AI capability assists with request/response interpretation, pattern recognition, and payload generation, thereby accelerating testing overall.

This AI Assistant provides several key advantages:

- **Enhanced HTTP Traffic Analysis**: Rapid identification of potential vulnerabilities in complex API responses and web traffic
- **Contextual Payload Generation**: Creation of tailored test vectors specific to the target application's technology stack
- **Automated Pattern Recognition**: Detection of security anomalies that might be overlooked in manual review
- **Natural Language Query Interface**: Allows security analysts to interact with technical data through conversational queries
- **Efficiency Optimization**: Reduces time spent on repetitive tasks while maintaining testing rigor

Safeguards, Data Privacy and Security Assurances
When used, the AI operates in a secure and privacy-preserving manner. No customer data is stored or used to train any model. All data is processed transiently and purged after the request is completed. The Claude model does not retain or learn from the input provided.

Our privacy safeguards include:

- **Zero Data Retention**: Complete purging of all session data upon completion
- **Isolated Processing Environment**: Segregation of AI processing from persistent storage systems
- **Transparent Operation**: Clear documentation of when and how AI assistance is employed
- **Compliance Verification**: Regular audits to ensure adherence to data handling policies

Protocols, Governance, Reviews and Limitations
The use of AI tooling is always governed by the rules of engagement and subject to client approval. Our governance framework ensures:

- **Explicit Client Authorization**: AI-assisted testing only proceeds with documented client consent
- **Complementary Approach**: AI tools supplement rather than replace skilled human analysis
- **Appropriate Application**: AI assistance is only utilized where it provides meaningful value
- **Documentation of Usage**: Clear recording of when AI was employed during the assessment
- **Verification of Results**: All AI-generated findings undergo intensive reviews and verification before inclusion in reports

Commitment to Excellence
Our integration of AI capabilities represents our commitment to leveraging cutting-edge technology while maintaining the highest standards of security, privacy, and professional integrity. We believe that the thoughtful application of AI-assisted tools, when appropriate and authorized, allows us to deliver more effective security assessments without compromising the quality and reliability our clients expect. Our skills, experience, and knowledge form the foundation of our penetration testing methodology remains central to our approach, with AI serving as a powerful multiplier that enhances, rather than replaces, the critical thinking and creative problem-solving that effective security testing demands.

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:

[redacted]

June 25, 2025
Date

Mitzi Shepherd
Printed Name

Senior Vice President (State, Local and Education)
Title

Mitzi.Shepherd@nttdata.com
Email Address

[redacted]
Phone Number