

Supplement **2**:

TrustOhio: Penetration and Vulnerability Testing Services
Security Auditing Services

(Pre-qualified Contractors)

Table of Contents

1.0	Penetration / Vulnerability Testing Requirements	4
1.1	General Testing Methods, Standards and Reporting Conventions	4
1.2	External Sources and Standards	5
1.3	Penetration / Vulnerability Mobilization	5
1.4	Penetration / Vulnerability Setup	6
1.5	Penetration / Vulnerability Testing	6
1.6	Penetration / Vulnerability Completion Activities	7
2.0	Infrastructure Security Audit Services	7
2.1	Infrastructure Review Services	7
2.2	Critical Infrastructure or Systems Security Implementation Process Review Services	8
2.3	Infrastructure Role / Permission Audits	9
3.0	State of Ohio Responsibilities (PVT and Audit Services)	9
4.0	State Project Delivery, Management, Methodology and Approach Requirements	10
4.1	Project Management and Coordination Services	10
4.2	Create and Maintain Project Plan	11
4.3	Project Review Check Point	13
4.4	Meeting Attendance and Reporting Requirements.	13
4.5	Utilize OIT's Document Sharing/Collaboration Capability	14
4.6	Project Delivery, Role and Responsibility Requirements	14
4.7	Cooperation with State and State Contractors	15
4.8	Knowledge Transfer and Handoff to State	15
4.9	Future Project Services Pricing Response and Rate Card	15
5.0	Schedule of Deliverables and Work Products	15
5.1	Delivery and Deliverable Standards	16
5.2	Schedule of Key Project Management Work Products	16
6.0	Assumptions	17
6.1	Support Requirements	17
6.2	Pre-Existing Materials	17
6.3	Commercial Materials	17
7.0	State Staffing Requirements	18
7.1	Contract Staffing and Key Activities	18
7.2	Staffing Plan and Time Commitment	19

Supplement Two contains scope of work to identify and contract with multiple qualified firms for conducting independent expert level penetration testing and network auditing services on existing Networks Statewide, as well as next generation capabilities arising as a result of the implementation of the work in Supplement One. In addition, Supplement Two contains provisions for inclusion of State resources, students and academics in the work to foster “hands on” and “real life experience” application of the skills, tools and methods developed within the incubation of leading edge capabilities within Supplement One. Based on the State’s evaluation, **multiple qualified firms may be identified and pre-qualified** to perform this work on an emerging or contracted Statement of Work basis based upon State needs.

The Statement of Work Solicitation Process. Services will be awarded via the Solicitation process. All SOW Solicitations will be issued by the Office of Information Technology. The SOW Solicitation will be released to pre-qualified pools of Contractors from Supplement Two or Supplement Three most closely matching the scope of work. A single pre-qualified Contractor will be selected to perform the work contained in each SOW Solicitation. The selected prequalified Contractor may partner with one or more subcontractors. All subcontractors shall be identified within the pre-qualified Contractor’s proposal submitted in response to the SOW Solicitation. The steps identified below describe the process of a Statement of Work Solicitation.

When determined to be in the best interest of the State, OIT will issue a Statement of Work Solicitation for work specified in this RFP. A Contractor will not be required to respond to every Statement of Work Solicitation issued as a result of this Contract, but they will be expected to respond to a majority of the Statement of Work Solicitations issued for each of the Supplement Two or Supplement Three they are awarded during the course of a fiscal year. Should a Contractor not respond to a majority of the Solicitations issued, it may be removed from the list of pre-qualified Contractors.

The Statement of Work Solicitation Content. Each SOW Solicitation shall contain a Project Statement of Work that will include, but not be limited to, the following components, which will be defined in each SOW Solicitation. The State may revise or refine the SOW Solicitation format and content requirements as needed.

Content. Each Statement of Work Solicitation will contain the sections listed below:

- Background information for the deliverables-based project, including:
 - a. Agency information
 - b. Project name
 - c. Project objective
 - d. Project description
 - e. Project schedule
 - f. Project milestones
 - g. Bill to Address
- Scope of Work
 - h. Description of scope of work (in and out) and project requirements
 - i. Description of constraints, assumptions
 - j. Contractors Work Effort Requirement – The Contractor’s full-time regular employees must perform at least ___% of the effort required to complete the Work. The Contract may use its personnel or subcontractor personnel to meet the remaining ___% of the effort.
 - k. Detailed description of deliverables
 - l. Deliverable acceptance criteria
 - m. Description of roles and responsibilities
 - n. Expected duration
 - o. Restrictions on location of data & work
 - p. Resource Requirement
 - q. Reports
- Deliverables Management
 - r. Submission/format
 - s. Reports and meetings
 - t. Period of performance
 - u. Performance expectations

- v. Pricing and payment schedule
- State Staffing Plan
- SOW Response Submission Requirements
 - w. Response format, content requirements
 - x. Staffing plan, personnel resumes, time commitment, organizational chart
 - y. Contingency plan, if applicable
 - z. Work plan, project plan
 - aa. Fee Structure including estimated work effort for each deliverable
 - bb. Cost summary
- Communication Plan
- SOW Evaluation Criteria
- SOW Solicitation Schedule
- Risk management plan (may include issues management)
- Quality management plan
- Project schedule (WBS using MS Project or compatible)
- Limitation of Liability (Identification of Limitation of Liability applicable to the specific SOW Solicitation. Unless otherwise stated in this section of the SOW Solicitation, the Limitation of Liability will be as described in Attachment Four, Part Four of the Contract General Terms and Conditions.

Note: In the case of an emergency, the Department of Administrative Services may suspend the competitive procurement process pursuant to Section 125.061 of the Ohio Revised Code.

1.0 Penetration / Vulnerability Testing Requirements

Once, as a result of this RFP, the State determines the qualified pool of Contractor(s) eligible to perform the work, the State may issue a Statement of Work in consideration of its needs. This Statement of Work may contain the specific scope, domains, infrastructure elements, demarcation points, access levels, duration, type(s) of testing required and other elements to serve as a definitive scope of Work. Contractors will assemble a quotation including all elements pertinent to the work, a project plan, applicable deliverables, State resource requirements and a final, firm fixed price to the State for the work.

In general:

Vulnerability Testing should be designed to Identify, rank, and report vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system or infrastructure element and potential risks posed by known vulnerabilities, ranked in accordance with NVD/CVSS base scores associated with each vulnerability. External vulnerability scans must be performed by the Contractor and the risks ranked in accordance with the CVSS. Internal vulnerability scans may be performed by the Contractor and risks ranked in accordance with a mutually agreeable risk-ranking process as compliant with PCI DSS Requirement 6.1. Tests may include external vulnerability scan conducted from outside the State as well as internal vulnerability scan conducted from inside the State; and

Penetration Testing should be designed to identify ways to exploit vulnerabilities to circumvent or defeat the security features of system or infrastructure components. The Contractor will provide a description of each vulnerability verified and/or potential issue discovered and more specific risks that vulnerability may pose, including specific methods how and to what extent it may be exploited. Examples of vulnerabilities include but are not limited to SQL injection, privilege escalation, cross-site scripting, or deprecated protocols.

The Contractor performing the work, shall propose tools, methods and experienced personnel to address the following:

- Application and Network Level Testing
- Authentication, Roles and Permissions
- Web Applications and Mobile Access
- Segmentation of Infrastructure Elements, Systems and Application Tiers
- Social Engineering Means and Methods
- Third-Party Hosted and Cloud Environments

1.1 General Testing Methods, Standards and Reporting Conventions

The State, in consultation with the Contractor, will indicate which of the following general methods to be tested (listed in increasing depth and intrusiveness):

- 1) **Lightweight Testing:** designed as a broad scope test across internal and external State infrastructure and system elements that is designed to identify weaknesses in devices, configurations, rules, implementations, systems or network level devices as well as rudimentary access and authorization of userids or identity credentials. In general, this testing shall be oriented around performing a network assessment and full PV scan around a set of State-defined IP range(s), host(s) or Internet access/egress points;
- 2) **Targeted Testing:** which are designed to test specific infrastructure elements including domains, subnetworks, groups of system elements (e.g., “web servers”, “web services”, “application servers”, “network services”, “database servers” and the like) against specific threat sources, tools and methods. Under this form of testing,

the Contractor will be provided limited knowledge and technical details as to the underlying composition of State systems and infrastructure elements as well as boundary conditions and elements as discovered or generally available using public or State provided sources. In general, this testing shall be oriented around specific elements of the State's application and systems architecture around a set of State defined business systems or functions such as Web Portals, Integration / Workflow Servers, ERP or Web Commerce/Interaction Portals.

- 3) **Focused Testing:** in which specific attack activities such as social engineering, phishing, obtaining non-public materials useful to perform exploits or attacks and other methods as to camouflage the source, target, methods and means of the attack as well as leveraging elements as contained in either of Lightweight or Targeted testing methods. As part of Focused Testing, the Contractor will assess the State's security defenses, identification and defense methods and procedures as well as incident response capabilities. In general, this testing shall be oriented around focused attempts at gaining systems or administrative access to elements of the State's IT portfolio inclusive of infrastructure elements, systems, processes, procedures and the like in keeping with "ethical hacking" under a controlled and confidential process.

The Contractor performing the work, will augment the preceding General Testing Methods with Contractor specific or proprietary methods, means, tools and techniques to provide the Testing Service in a complete and thorough manner.

1.2 External Sources and Standards

Wherever possible, the Contractor (in addition to Contractor specific or proprietary elements) will incorporate the use of the National Vulnerability Database (NVD) which is the U.S. government repository of standards based vulnerability management data. This data is designed to enable automation of vulnerability management, security measurement, and compliance (e.g. FISMA). In addition, the following industry standard references should be included as applicable:

- Common Vulnerabilities and Exposure (CVE)
- Common Weakness Enumeration (CWE)
- Bugtraq ID (BID)
- Open Source Vulnerability Database (OSVDB)

The Contractor, under a State-authorized Statement of Work, wherever possible, in addition to Contractor specific or proprietary elements must incorporate the use of the Common Vulnerability Scoring System (CVSS) which is designed to provide an open framework for communicating the characteristics and impacts of IT vulnerabilities.

1.3 Penetration / Vulnerability Mobilization

The Contractor, under a State-authorized Statement of Work, will:

- Assemble its team members, tools and methods required to perform the work;
- Publish a project plan inclusive of all activities, work products, deliverables and State requirements (e.g., staff, access, networks, infrastructure elements etc.);
- Confirm the scope(s), method(s), timing, frequency and other elements required to successfully perform the work;
- Verify the required access (if applicable) within the State or externally; and
- Conduct a Project Kickoff including all project team personnel.

The State will:

- Assemble its team members, tools and methods required to participate in and support the work;

- Provide access to required work location(s) and infrastructure element(s) as agreed; and
- Notify security, application and infrastructure personnel as well as agency and IT leadership (if appropriate) as well as State vendor(s) as to the general scope and timing of the work and test(s).

The Contractor, under a State-authorized Statement of Work, will produce the following deliverables unless otherwise authorized by the State:

Deliverable 001. Document Agreed to Test Conditions, Methods, Scope and Boundaries Report including:

- Agreed to Project Plan, Approach and Project Roles/Responsibilities
- Technical Details
- Infrastructure Elements, Assets, Address Ranges, IP Details
- Manual, Automated, Social Methods
- Test Period (Begin, End Dates)
- Methods and Expected Results

1.4 Penetration / Vulnerability Setup

The Contractor, under a State-authorized Statement of Work, will:

- Perform, assemble or configure applicable manual method attack(s) and test(s);
- Perform, assemble or configure applicable automated or script based attack(s) and test(s);
- Perform, assemble or configure applicable attempts at gaining access via social engineering using a variety of public and/or State provided details to augment manual and/or automated methods; and
- Confirm to the State-identified point of contact that all methods are ready for performance of Penetration / Vulnerability testing as agreed with the State and seek the approval of the State point of contact to proceed.

Deliverable 002. Ready to Test Indication, State Authorization to Proceed with Testing

- All Contractor Provided Elements Ready for Test Execution
- All State Provided Elements Ready for Test Execution
- State Written Authorization to Proceed

1.5 Penetration / Vulnerability Testing

The Contractor, under a State-authorized Statement of Work, will:

- Perform applicable manual method attack(s) and test(s);
- Perform applicable automated or script based attack(s) and test(s);
- Perform applicable attempts at gaining access via social engineering using a variety of public and/or State provided details to augment manual and/or automated methods;
- Complete all agreed to steps and methods under the State-agreed general method of the test.

Deliverable 003. Confidential Vulnerability Assessment Report

- Containing all Success/Failures and Issues or Weaknesses Detected During Test
- Method of Obtaining Access and (to the extent possible) a Root Cause Analysis
- Relative Exposure details (e.g., system access, data access, privileges, elements exposed)

Deliverable 004. Evidence Report

- Evidence collected from the penetration test used to determine the Contractor's conclusion(s) and recommendations. Evidence is considered all information that supports the Contractor's conclusions about the effectiveness of the security controls and the environment's overall security posture.
- The Contractor must follow a systematic process to securely collect, handle, and store evidence. Examples of evidence include but are not limited to screenshots, raw tool output (i.e., NMAP, burp suite, Nessus, TCPDump, Wireshark, etc.), acquired dumps in case of exploitation (e.g., database files, logs, configuration files etc.), photos, recordings, and anything that may support the final conclusions of the penetration test report.
- It should be noted that if State data is acquired during the penetration test, it must be kept to a minimum. For example, a database full of State data should not be maintained on the Contractor's machines or systems.

1.6 Penetration / Vulnerability Completion Activities

Upon completion of the contracted test period, or at the direction of the State, the Contractor will have the following responsibilities:

Deliverable 005. Test Completion Report

- Conduct a test completion report meeting where the details, methods, duration and other aspects of the PVT are reported to the State;
- Handoff of all results, findings and details associated with the test inclusive of successes, failures, issues or weaknesses to the State with (to the extent possible) Root Cause Analysis of the underlying access weakness

Deliverable 006. State Data and Information Destruction Certification

- The Contractor will, at the conclusion of the project and presentation of the Test Completion Report, immediately destroy any and all State-specific elements provided for the Test, or discovered during the test from all Contractor equipment and files (electronic, paper or otherwise) and issue a certification to the State attesting that no sensitive State data or information pertaining to the test is in the possession of the Contractor, present in any Contractor systems, or maintained by any Contractor team members as a group or individually in any form.
- All data destruction and sanitization of equipment is to be performed using procedures consistent with NIST special publication 800-88.

2.0 Infrastructure Security Audit Services

From time to time, in conjunction with PVT projects or as a preventative set of measures, the State may require Infrastructure Security Audit Services. These services are to review State security positions on a defined set of systems assets, security configuration / implementation details, operational processes and procedures to administer and maintain security elements of State systems and infrastructure and develop assessments as to real or potential vulnerabilities with respect to the implementation of Security within these systems and infrastructure.

The Contractor working under a State agreed Statement of Work will conform to the following elements.

2.1 Infrastructure Review Services

The Contractor, under a State-authorized Statement of Work, will:

- Conduct an assessment and identify all methods and locations associated with the implementation, operation and maintenance of security credentials with State infrastructure and systems;

- Determine all means and methods by which root/administrative (privileged) access is granted, updated or revoked based on State determined parameters;
- Determine all means and methods implemented (or required to be implemented) to comply with State security policies and commercial best practices;
- Identify all access controls, or the absence thereof, for State-restricted or critical infrastructure, systems, services or data;
- Review network level configuration and implementation standards, designs and implementation artifacts to determine if State security policies are implemented and administered in keeping with OEM/commercial best practices (at a device level), State security policy, and in a manner as to be repeatable, extensible and consistent across the enterprise; and
- Review and identify potentially excessive, overlapping, or inconsistent permissions or access privileges within State identity stores and directory structures associated with State identified critical systems and infrastructure elements;

Deliverable 007. Confidential Infrastructure or Systems Vulnerability Assessment Report

- Containing all success/failures and issues or weaknesses detected during review
- Relative exposure details (e.g., system access, data access, privileges, elements exposed)
- Specific achievable recommendations as to method(s) or action(s) the State needs to take to address and remediate any identified security elements pertinent to infrastructure or State systems to comply with the more stringent of State security policies and commercial best practices.

2.2 Critical Infrastructure or Systems Security Implementation Process Review Services

The Contractor, under a State-authorized Statement of Work, will:

- Review the technical, operational control and audit/verifiability processes of access controls, or the absence thereof, for State-restricted or critical infrastructure, systems, services or data;
- Review network level configuration and implementation processes to determine if State security policies are implemented and administered in keeping with OEM/commercial best practices (at a device level), State security policy, and in a manner as to be repeatable, extensible and consistent across the enterprise;
- Perform an end-to-end process review to ensure that all required State approvals and prerequisites are met and followed prior to the creation of trusted or privileged access to critical State systems and infrastructure elements associated with the “on-boarding”, “updates” and “off-boarding” of such access when granted or revoked; and
- Perform an assessment as to the efficacy and completeness of security control processes in light of the risk and criticality of State systems and infrastructure assets.

Deliverable 008. Confidential Infrastructure or Systems Process Assessment Report

- Containing all process success/failures and issues or weaknesses detected during review
- Relative process and policy exposure details (e.g., system access, data access, privileges, elements exposed as a result of inadequate policies, processes or controls)
- Specific achievable recommendations as to method(s) or action(s) the State needs to take to address and remediate any identified security elements pertinent to infrastructure or State systems to comply with the more stringent of State security policies and commercial best practices.

2.3 Infrastructure Role / Permission Audits

The Contractor, under a State-authorized Statement of Work, will:

- Review the technical, operational control and audit/verifiability processes of role/permission controls, or the absence thereof, for State-restricted or critical infrastructure, systems, services or data;
- Review network level configuration and implementation processes to determine if State security policies are implemented and administered at the role/permission level in keeping with OEM/commercial best practices (at a device level), State security policy, and in a manner as to be repeatable, extensible and consistent across the enterprise;
- Perform an end-to-end process review to ensure that all required State approvals and prerequisites are met and followed prior to the creation or assignment of trusted or privileged roles and permissions associated with critical State systems and infrastructure elements associated with the “on-boarding”, “updates” and “off-boarding” of such access when granted or revoked; and
- Perform an assessment as to the efficacy and completeness of security control processes at the role and permission level in consideration of all users of a State system or infrastructure element in light of the risk and criticality of State systems and infrastructure assets.

Deliverable 009. Confidential Infrastructure or Systems Process Assessment Report

- Containing all process success/failures and issues or weaknesses detected during review
- Relative process and policy exposure details (e.g., system access, data access, privileges, elements exposed as a result of inadequate policies, processes or controls)
- Specific achievable recommendations as to method(s) or action(s) the State needs to take to address and remediate any identified security elements pertinent to infrastructure or State systems to comply with the more stringent of State security policies and commercial best practices.

3.0 State of Ohio Responsibilities (PVT and Audit Services)

The State will be responsible for the following:

- The State will provide appropriate resources and contacts to assist in assessing our strategies, environment, and security workflow.
- Key stakeholders will participate in interviews, onboarding processes, and deliverable reviews.
- The State will provide appropriate IP addressing schemas, updated network diagrams, and other technical information needed for the Project. This information must be kept secured by the Contractor in accordance with existing NDAs that are maintained with the State of Ohio. GEB: What if the Contractor doesn't have an existing NDA with the State?
- Appropriate resources will be provided to review the asset classification and prioritization documents and to assist in the process of documenting the identification, classification, and prioritization of critical systems and data.
- The State will provide network use descriptions, policies, and other information to provide an understanding of what is normal and permissible network traffic.
- The State will provide response policies, guidelines, and contacts, aligned with local/state/federal law and regulations. The State will define and direct the response and communicate this to the Contractor. The contact list will identify the proper State resources for notification and escalation that have the authority to make decisions and to triage events and identify additional State resources that may be needed.
- Security representatives will be designated to participate in briefings or after action reports.

- The Contractor will organize and arrange for State representation at knowledge transfer sessions.
- Unless otherwise agreed, the State will respond within three to four business days after the Contractor's request for any other documentation or information needed to provide the Services.
- State personnel will use appropriate collaboration tools with the Contractor for hosted meetings, documentation management, instant messaging, desktop sharing and use of collaborative spaces.

4.0 State Project Delivery, Management, Methodology and Approach Requirements

The Contractor will provide the State with Contractor's recommended methodology and approach to the Proof of Concept project and any projects that arise following the successful completion of the Proof of Concept as a result of this RFP. The Contractor will provide training to State team members on use of the methodology so that State team members may complete their work in accordance with the responsibilities in this SOW.

The State acknowledges that certain situational factors may prevail that require modification, deletion or augmentation of all deliverables in this RFP. Should the State require deviation from these deliverables, the State and Contractor agree to meet prior to the commencement of any work to develop a Statement of Work or IDA (if applicable) that details all required deliverables as required by the State. Absent this written direction from the State, the Contractor must complete all deliverables in this Supplement as required by the State.

The State maintains a project management and reporting methodology that is used at varying levels for complex, transformational information technology projects. This methodology is designed to provide a substantive and objective framework for the reporting and review of projects to impacted stakeholders and, should the need arise; identify the need for corrective action for one or many of the participants in a project (e.g., State, Contractor, customer, stakeholder).

The State acknowledges that various contractors that may do business with the State may maintain unique or proprietary project management methodologies, but seeks to ensure that the overall project is delivered to the State as contracted. Therefore, a minimum project management reporting standard has been created to serve the State's project management and oversight needs while not adversely impacting or influencing Contractor-provided delivery methodologies.

The Contractor must provide a summary Project plan as requested by the State. For purposes of a summary project plan specific phase and gate dates, effort and costs are a sufficient minimum.

Contractors must, at a minimum, include all deliverables and milestones within their proposed project plans that occur within this Supplement in the context of their proposed methodologies both within their proposal and at a commencement of any project as a Contractor performing the work following the award of this Contract during the project mobilization phase:

4.1 Project Management and Coordination Services

The Project will follow the governance structure defined by the State. Project management will include the activities to manage the Project including directing the Project team according to the Project work plan, reporting status, managing issues, assessing quality, leading project meetings, and monitoring schedule and scope changes. The Project team will produce project status reports on a weekly basis. The format of status reports will be mutually agreed to by the State and the Contractor during the first week of the Project.

The Contractor will, in conjunction with an authorized Statement of Work arising from this Supplement:

- Be responsible for the coordination and delivery of the overall Project;
- Ensure that an appropriate "Project Kickoff" occurs and that all integrated work plans are agreed to by the State from project commencement;

- Ensure that all efforts have an effective version control mechanism for all documents within the project document library that will be maintained on a State provided Microsoft SharePoint site;
- Work with the State leadership to ensure that the Project is staffed appropriately;
- Ensure that required testing activities across both technical and operational components are completed to minimize Project risk; and
- Collaborate with the task areas to ensure appropriate cross-team communication and delivery.

For purposes of the Project, “Perform” means that the party assigned the task has the duty and ultimate responsibility to take all appropriate steps to complete or facilitate the identified task unless otherwise provided for between the parties, subject to the supporting party completing its interdependent responsibilities. The term, “Support” means that the party has the duty and responsibility to provide ancillary support or assistance which may be necessary to enable the party providing the “Perform” task to complete that task unless otherwise provided for by the parties. The designation, “-” means that the party has no responsibility for the task, unless otherwise agreed by the parties.

Key Tasks	State	Contractor
Conduct Project kick-off meeting	Support	Perform
Create a Work Breakdown Structure (WBS)	Support	Perform
Create and Maintain a project work plan and any related deliverable sub plans	Support	Perform
Review Deliverables and manage the State’s approvals	Perform	Support
Review Deliverables and manage the Contractor’s approvals	Support	Perform
Prepare and conduct project meetings	Support	Perform
Prepare and conduct stakeholder meetings	Perform	Support
Create Project Status Reports adhering to the PMO policies	Support	Perform
Report and manage issues and risks	Support	Perform
Monitor and report schedule and scope changes	Support	Perform
Identify State stakeholders and manage expectations	Perform	Support
Assist with on-boarding for the Contractor resources	Support	Perform
Assist with on-boarding for the State resources	Perform	Support
Confirm State Project staffing	Perform	Support
Confirm Contractor Project staffing	Support	Perform
Confirm Project governance	Perform	Support
Initiate Production Acceptance Criteria (“PAC”) process	Support	Perform
PAC – Provide planned checkpoint review dates	Support	Perform

4.2 Create and Maintain Project Plan

The Contractor must submit a detailed Project plan, in electronic and paper form, to the State Project Manager for approval within twenty business days after the State issues a purchase order or other written payment obligation under the Contract.

Deliverable 010. Master Project Plan

The Project plan should include the following (at a minimum):

- Project Integration;
- Project Scope;
- Project Time;
- Project Quality;
- Project Staffing;
- Project Communications;
- Project Risks/Issues; and

- Project Procurement.

The Contractor must lead a planning session which ensures the following:

- A common understanding of the work plan has been established;
- A common vision of all deliverables has been established;
- A critical path has been established that identifies all major milestones, dependences (both internal and external to the Project), resources by name and resource assignments and is complete and inclusive of the entire work effort from commencement until conclusion of all contracted activities; and
- Clarity on scope of overall project and the responsibilities of the Contractor has been defined and agreed to by the State that includes a common understanding of the business, process, technical and other elements of the overall implementation as required.

Thereafter, the Contractor must:

- Formally update the Project plan, including work breakdown structure and schedule, and provide the updated Project plan as part of its reporting requirements during the Project; and
- Ensure the Project plan allows adequate time and process for the development for the State's review, commentary, and approval.

The State will determine the number of business days it needs for such reviews and provide that information to the Contractor after award and early in the development of the Project plan. Should the State reject the plan or associated deliverables, the Contractor must correct all deficiencies and resubmit it for the State's review and approval until the State accepts the Deliverable at no additional cost to the State.

At minimum, the Contractor must develop a proposed Project plan(s) as part of its Proposal, which will include the following:

- **A summary Work breakdown structure;** Scope statement that includes the Work objectives and the Work Deliverables and milestones associated with completion of all of the Work with specific provisions for the work contained and as required by the Proof of Concept project;
- The Contractor must provide a **detailed Project plan as a Microsoft Project Gantt chart (in native MS Project file “.mpp” format)**, showing all major Work tasks on a week-by-week schedule, with proposed team members (by name for Key Personnel and by role for other Project team members) and indications of State participation requirements in the Project(s) to serve as the basis for managing and delivering the Work. The schedule must clearly demonstrate how the Project will become fully operational by the delivery date. Within this detailed plan, the Contractor must give dates for when all Deliverables and milestones will be completed and start and finish dates for tasks. The Contractor also must identify and describe all risk factors associated with the forecasted schedule;
- **The Contractor will indicate who (State or Contractor) is assigned responsibility** for each Deliverable within the work breakdown structure to the level at which control will be exercised;
- Performance measurement baselines for technical scope, budget adherence, deliverable assembly, production and approvals in the context of the overall schedule;
- Description of the Contractor's proposed organization(s) and management structure responsible for fulfilling the Contract's requirements and supporting the Work, in terms of oversight and control;
- A summary of required State staff and their expected roles, participation and level of effort by project area (e.g., functional, technical, business) as well as role within each Project phase (e.g., Requirements, Design, Construction, Testing, Deployment);

- Description of the review processes for each milestone and Deliverable (e.g. mandatory design review) and a description of how the parties will conduct communication and status review;
- Description of the Project issue resolution process including an escalation plan; and
- Description of the approach to manage subcontractors effectively, if the Contractor is proposing subcontractors.

4.3 Project Review Check Point

Upon completion of the baselined Project plan and on a quarterly basis throughout the Project, the Contractor, in conjunction with State Project team staff, must deliver a presentation to the State. At a minimum, the presentation must address any known State or Contractor issues or concerns, including but not limited to the following:

- Project scope, budget and schedule;
- Any changes to key named resources assigned to the Project;
- Project readiness including key issues and risk from their current status;
- Project status including variance from baseline for key milestones, tasks, deliverables (significant work products) and project closure;
- The Contractor's Methodology, approach, and tools to achieve the Project requirements and report the status, completeness and agreement for documented project management and implementation approaches (e.g., Project management plan, communication plan, requirements traceability, implementation approach and methodology); and
- Roles, responsibilities, and team expectations for all Parties.

Upon completion of the presentation, the State will immediately assess the health of the project and determine next steps for moving forward with the Project, within one week of the meeting, which may include the following:

- Continue the Project;
- Terminate the Contract; or
- Suspend the Contract.

See Suspension and Termination language in Attachment Four for remedies for failure to deliver the proposed work.

Note: There may be additional Project reviews conducted by the State on an as needed basis throughout the term of the Contract to assess Project health and ensure the Project is progressing successfully.

4.4 Meeting Attendance and Reporting Requirements.

The Contractor's project delivery approach must adhere to the following meeting and reporting requirements:

- Immediate Reporting - The Project Manager or a designee must immediately report any Project staffing changes to the State Project Representative;
- Attend Weekly Status Meetings - The State and Contractor Project Managers and other Project team members must attend weekly status meetings with the Project Representative and other members of the Project teams deemed necessary to discuss Project issues. These weekly meetings must follow an agreed upon agenda and allow the Contractor and the State to discuss any issues that concern them;
- Provide Weekly Status Reports - The Contractor must provide written status reports to the State Project Representative at least one full business day before each weekly status meeting; and
- At a minimum, weekly status reports must contain the items identified below:

- Updated GANTT chart, along with a copy of the corresponding Project plan files (i.e. MS Project) on electronic media acceptable to the State;
- Updated critical path analysis with the aforementioned GANTT chart and an accompanying PERT chart;
- Status of currently planned tasks, specifically identifying tasks not on schedule and a resolution plan to return to the planned schedule;
- Issues encountered, proposed resolutions, and actual resolutions;
- The results of any tests;
- A problem tracking report must be attached;
- Anticipated tasks to be completed in the next week;
- Task and Deliverable status, with percentage of completion and time ahead or behind schedule for tasks and milestones;
- Proposed changes to the Project work breakdown structure and Project schedule, if any;
- Planned absence of Contractor staff and the expected return date;
- System integration/interface activities; and
- The Contractor's proposed format and level of detail for the status report is subject to the State's approval.

4.5 Utilize OIT's Document Sharing/Collaboration Capability

In conjunction with the delivery of the Project, coincident with the start of the project through its conclusion, the Contractor must use the State-provided and hosted document management and team collaboration capability (Microsoft® SharePoint™) to provide access through internal State networks and secure external connections to all project team members, approved project stakeholders and participants. In conjunction with the utilization of this tool, the Contractor must:

- **Ensure that any records, files, documents, spreadsheets and work products that contain confidential security information are marked on every page with “This document contains confidential security records covered under ORC 149.433 and is not subject to public disclosure” prior to providing such documents to the State in any form.**
- Structure the document management and collaboration pages and data structures in such a manner as to support the overall requirements of the Project;
- Store all documents in machine readable, editable and native formats (e.g., XLSx, PPTx, VSD, DOCx) as opposed to proprietary, non-editable, image format or PDF based renderings;
- Be responsible for the maintenance and general upkeep of the designer configurations of the tool in keeping with commercially reasonable considerations and industry best practices as to not adversely impact the project delivery efforts performed by the Contractor and State; and
- At the conclusion of the project, or upon request of the State, ensure that the State is provided a machine readable and comprehensive backup of the SharePoint™ database(s) contained within the tool that is owned by the State and not proprietary to the Contractor or otherwise required by the State to maintain ongoing project documentation and artifacts (i.e., Contractor is to remove all Contractor proprietary or non-State owned or licensed materials from the tool).

4.6 Project Delivery, Role and Responsibility Requirements

The State has organized its requirements for responsibilities of the State and Contractor based on the anticipated activity areas required to analyze, design, implement and deploy the solution as well as those requirements and activities required to support the deployment of the overall solution. Should a Contractor, as a result of the review of these requirements in light of their proposed approach, require additional roles or clarity, the Contractor must

indicate the additional requirements of the State and provide a high level rationale for the same as part of their response.

The responsibility matrices included throughout the remainder of this section identify Key Tasks to be performed as part of this project. Each Key Task has been assigned to a party and the level of responsibility for each party is designated as either a "P" for Perform, "S" for Support or designated "-" for no responsibility.

Note: If the Contractor's recommended methodology does not align with the responsibility matrices below, the Contractor shall present matrices which do align with the Contractor's methodology. The Contractor must also demonstrate that the recommended methodology and the responsibility matrices comply with the State's need to: (1) know the Contractor has a complete understanding of the State's requirements, (2) the Contractor's design and development efforts are in line with the State's requirement for the solution, (3) monitor the Contractor's progress during the project, (4) know the project risk is acceptable and is managed effectively by the Contractor, (5) have accurate and complete technical documentation regarding the solution (as designed and as delivered), and (6) know the solution delivered and deployed by the Contractor has been adequately tested and meets the State's requirements.

4.7 Cooperation with State and State Contractors

Contractor will cooperate with the State in its attempts at transferring, replacing or augmenting the services responsibilities to another provider in a manner in keeping with not adversely affecting the provision of ongoing services and other projects being performed concurrent with this project.

4.8 Knowledge Transfer and Handoff to State

The Contractor will perform knowledge transfer support as a Knowledge Transfer Package (KTP) to the State at the commencement of the project to support knowledge transfer to the State. In general, the KTP will include, at a minimum the following work products as a deliverable:

Deliverable 011. Knowledge Transfer Package (KTP)

The KTP Deliverable will include, at a minimum:

- Final Requirements Traceability Matrix for the Project as delivered including all scope, boundary, exception and assumption information as agreed by the State;
- A list of all tests performed with results (positive, negative or inconclusive) as performed;
- Detailed P/V test cases and demonstration of successful completion of same;
- Complete engagement administration documentation that represent the system as tested; and
- Complete documentation sufficient for the State or a State's vendor to remediate the system in the State's infrastructure environments inclusive of Production, DR, Demo/Training etc.

4.9 Future Project Services Pricing Response and Rate Card

Offerors must provide a Rate Card, by project personnel role and experience level as well as technical role and experience level that is binding over the Contract term. The Contractor may not propose rates (blended or otherwise) in any Project SOW that differ from this rate card as allowed under any contract arising from this RFP.

5.0 Schedule of Deliverables and Work Products

To support the execution of the Project and provide supporting follow-on documentation, the Contractor will create and deliver to the State the following set of Deliverables and Work Products. The State Project Lead will serve as the representative for coordinating respective internal reviews of the subject Deliverable(s) and Work Products for sign off by the State. The Contractor should modify or propose other deliverables based on their solution or

methodology characteristics. Any differences proposed to the ones listed below should include an explanation in the Contractor's response.

5.1 Delivery and Deliverable Standards

- The Contractor will define, document and submit all standards they intend to utilize in the performance of this project. Once the State approves these standards, variances to standards must be approved by the State prior to implementation of other than standard practices.
- The Contractor's work and deliverables will be in accordance with the Contractor's standards (e.g., testing methodology, project management, etc.).

5.2 Schedule of Key Project Management Work Products

In addition to the deliverables identified throughout this Supplement, the Contractor will provide the following Project Management work products.

Name	Key Project Management Deliverable / Work Product Descriptions
Kickoff Meeting Presentation	Documents the governance for the Project, roles, approach, timeline, and deliverables in a presentation format to be presented to the Project team.
Project Execution Methodology	This is a detailed description of Contractor's project management approach as well as the requirements gathering and analysis, design, build, test, deploy and run methodologies the Contractor follows, standards the Contractor intends to apply to this Project, and any applicable tool sets. Contractor must address topics such as: <ul style="list-style-type: none"> • Risk and Issue Management • Resource Management • Change Control • Test Methodology
Work Breakdown Structure (WBS)	This document is a hierarchical decomposition of the project into phases, deliverables and work packages. In the work breakdown structure supplied, sufficient detail needs to be presented and maintained over the course of the project to track the earned value against the proposed costs and work efforts. This WBS will be reflected in the Project workplan.
Resource Plan	The resource plan must specify resources required, by type, over the duration of the Project. Contractor must identify all required resources (Contractor, State or otherwise) to complete the Project, except where otherwise specified in this document, and include all costs for those resources that are to be provided by the Contractor. Sample roles should be inclusive of Developers, Business Analysts, Administrators, Security Analysts, Database Administrators, or any other roles deemed necessary by the Contractor. The Contractor will specify the percent of time each resource will perform their role on State premises.
Organization Structure	This is an org structure reflecting a high-level org structure that incorporates both Contractor and State resources. Roles to address may include any of the following: <ul style="list-style-type: none"> • Sponsors and Stakeholders • Project Management • Quality Assurance • Team Structure and Leads
Project Workplan	Documents the tasks required to complete the Project, the responsible party for the task, task dependencies, and the resources, duration and work hours required. This plan should include key milestones and phases. The project work plan should be in an acceptable format for the State (e.g., MS Project). The Contractor's project manager will work with the State's project manager to ensure an acceptable Project workplan is completed and accepted as baseline within 20 business days after the Kickoff Meeting.
Technical Requirements	All recommended changes to the State's original technical requirements and rationale for the changes. These requirements should be elaborated upon as required to support the development of the technical specification and design.
Communication Plan	This specifies typical project stakeholders, communication frequency, and communications vehicles. It must also include the approval process for communications, and how the approval process may differ based on target audience.
Knowledge Transfer Plan	A plan defining the activities and roles required to perform knowledge transfer of the operations and support of the solution.

Name	Key Project Management Deliverable / Work Product Descriptions
Test Strategy	This is the overall test strategy which includes: <ul style="list-style-type: none"> • Tests to be completed • Test environments • Test tools • Defect tracking • Test approach
Master Test Plan	This documents the plan, scripts (including expected results) and schedule required to execute the various tests phases, including but not limited to Security Testing, Vulnerability Testing, and Audit Testing.
Test Results	These documents are the presentation of the results from a particular testing Phase inclusive of substantiation of Contractor testing of all elements as required by the State and contained in the agreed scope of Testing.

6.0 Assumptions

The Offeror must list all the assumptions the Offeror made in preparing the Proposal. If any assumption is unacceptable to the State, the State may at its sole discretion request that the Offeror remove the assumption or choose to reject the Proposal. No assumptions may be included regarding the outcomes of negotiation, terms and conditions, or requirements. Assumptions should be provided as part of the Offeror response as a stand-alone response section that is inclusive of all assumptions with reference(s) to the section(s) of the RFP to which the assumption is applicable. **Offerors should not include assumptions elsewhere in their response.**

6.1 Support Requirements

The Offeror must describe the support it wants from the State other than what the State has offered in this RFP. Specifically, the Offeror must address the following:

- Nature and extent of State support required in terms of staff roles, percentage of time available, and so on;
- Assistance from State staff and the experience and qualification levels required; and
- Other support requirements.

The State may not be able or willing to provide the additional support the Offeror lists in this part of its Proposal. The Offeror therefore must indicate whether its request for additional support is a requirement for its performance. If any part of the list is a requirement, the State may reject the Offeror’s Proposal if the State is unable or unwilling to meet the requirements.

6.2 Pre-Existing Materials

The Offeror must list any Pre-Existing Materials it owns that will be included in a Deliverable if the Offeror wants a proprietary notice on copies that the State distributes. For example, the Offeror may have standard user interfaces or standard shells that it incorporates in what is otherwise custom software. (See the Ownership of Deliverables section of the General Terms and Conditions.) The State may reject any Proposal that includes pre-existing materials for a custom solution, if the State believes that such is not appropriate or desirable for the Project.

6.3 Commercial Materials

The Offeror must list any commercial and proprietary materials that the Offeror will deliver that are easily copied, such as Commercial Software, and in which the State will have less than full ownership (“Commercial Materials”). Generally, these will be from third parties and readily available in the open market. The Offeror need not list patented parts of equipment, since they are not readily copied. If the Offeror expects the State to sign a license for the Commercial Material, the Offeror must include the license agreement as an attachment. If the State finds any provisions of the license agreement objectionable and cannot or does not negotiate an acceptable solution with the licensor, regardless of the reason and in the State’s sole discretion, then the Offeror’s Proposal may be

rejected. If the State is not going to sign a license, but there will be limits on the State's use of the Commercial Materials different from the standard license in the General Terms and Conditions, then the Offeror must detail the unique scope of license here. Unless otherwise provided in this RFP, proposing to use Commercial Materials in a custom solution may be a basis for rejection of the Offeror's Proposal, if the State, in its sole discretion, believes that such is not appropriate or desirable for the Project. Any deviation from the standard license, warranty, and other terms in Attachment Four also may result in a rejection of the Offeror's Proposal.

If the Offeror proposes a Deliverable that contains Commercial Software or other Commercial Materials with terms that differ from the terms in Attachment Four for Commercial Software and Commercial Materials, then those terms must be detailed here, and any proposed separate agreement covering those items must be included in the Offeror's Proposal. This is required even if the State will not be expected to sign the agreement. Any deviation from the standard terms in Attachment Four may result in a rejection of the Offeror's Proposal.

7.0 State Staffing Requirements

As this project is an enterprise offering supported by DAS/OIT and includes agency participation in the Proof of Concept Project identified herein, the following table represents the State's minimum commitments to this Project. Should, based on the experience of the Contractor additional roles be required of the State, the Contractor will identify these roles, provide rationale and include a summary description of the skills and competencies required for each position. Note all roles (State minimum or otherwise) must be included in the Contractor Staffing Plan as required in this section of the Supplement. For all State roles marked "as required," Contractor s are to include (within their proposal) the staffing level required of the State to ensure that the Contractor project is supported adequately.

The State will provide a dedicated State Project Lead to serve as the Contractor's day-to-day point of contact for the Project. This role will be staffed throughout the duration of the Project. The State Project Lead will facilitate process and policy decisions in support of the Project schedule. State personnel assigned to the Analyze Phase will maintain consistent involvement throughout the duration of the Project. These individuals will be accessible and available to participate as agreed upon in the approved Project plan.

Project Area	State Trust Ohio Core Team (DAS/OIT)
Overall Project Management / Point of Reporting & Coordination	1 FTE
Security Advisor (State CISO Office)	1 FTE (design phases), part-time advisory thereafter
State Network Lead	Up to 1 FTE as required
State Cloud Technical Lead	Up to 1 FTE as required

7.1 Contract Staffing and Key Activities

The Contractor is to consider the roles provided by the State as well as those proposed that are required for the Proof of Concept Project based upon the details, the key activities, proposed time commitments required for each role, and the percent of the proposed time the role will be on the State's premises performing work. The Contractor, as part of its response, will identify all roles that are required to be performed (by phase), the work location(s) for the team and requirements for performing these roles off-site at a Contractor location or on State premises (e.g., Project Manager, business analysis, technical lead, functional lead, etc.). Contractor are to propose a combined team organization (i.e., State and Contractor) designed to deliver the project to the State as per the requirements in this Supplement.

Contractor Team Organization, Key Personnel and Work Location(s) –Proof of Concept

Role #	Contractor Role	Role Activity	FT/PT	% Time On Site
Startup / Analyze Phase				

Role #	Contractor Role	Role Activity	FT/PT	% Time On Site
		[insert rows as required]		
Setup Phase				
		[insert rows as required]		
Testing Phase				
		[insert rows as required]		
Completion Phase				
		[insert rows as required]		

7.2 Staffing Plan and Time Commitment

The Contractor's staffing plan and time commitment response must include the following information:

- An organizational chart including any subcontractors and key management and administrative personnel assigned to this Project.
- A contingency plan that shows the ability to add more staff if needed to ensure meeting the Project's due date(s).
- The number of people onsite at State location(s) at any given time to allow the State to plan for the appropriate workspace. Contractor **Note:** The following table is provided as an **example** of what the State expects the Contractor to provide in the Proposal response for this requirement.

Illustrative Contractor Staffing Plan

Project Week	1	2	3 – 6 (Variable Depending on Scope)						7	8
Phase	Startup / Analyze	Setup Phase	Testing Phase						Completion Phase	
State (Agency Team)	2	3	3	3	3	3	3	3	2	1
Contractor Team (Onsite)	2	3	3	3	3	3	3	3	2	1
Contractor Team (Remote)	2	6	6	6	6	6	6	6	2	1
State Infrastructure Team	2	3	3	3	3	3	3	3	2	1
State Security	2	2	2	2	2	2	2	2	2	1
Total Contractor	4	9	9	9	9	9	9	9	4	2
Total State	6	8	8	8	8	8	8	8	6	3

Contractor are encouraged to add additional roles and responsibilities as appropriate based on their proposed Project Staffing Plan to highlight the involvement of their proposed team and inclusion of State resources in the Project to help ensure its success. The number of FTEs depicted in the above table are provided as an **illustrative example** and in no way connotes State expectations as to the level, duration or involvement of the State or Contractor in this project.

A statement and a chart that clearly indicates the time commitment of the proposed Project Manager and the Contractor's Key Project Personnel, inclusive of the Project Manager and the Contractor's proposed team members for this Work during each phase of the Project, the System Development Life Cycle associated with the Project, and the commencement and ongoing operation of the Service.

The Contractor also must include a statement indicating to what extent, if any, the candidates may work on other projects or assignments that are **not** State related during the term of the Contract. The State may reject any Proposal that commits the proposed Project Manager or any proposed Key Project Personnel to other projects during the term of the Project, if the State believes that any such commitment may be detrimental to the Contractor's performance.

In addition, the Contractor's proposal must identify all Key Project Personnel who will provide services as part of the resulting Contract. The Key Project Personnel are identified in each applicable Supplement. The State expects that the proposed named Key Project Personnel will be available as proposed to work on the Project. Resumes must be provided for all Key Project Personnel. Representative resumes are **not** acceptable. The resumes will be used to supplement the descriptive narrative provided by the Contractor regarding its proposed Project team.

The resume (2-page limit per resume) of the proposed Key Project Personnel must include:

- Proposed Candidate's Name
- Proposed role on this Project
- Listings of completed projects (a minimum of two references for each named Key Project Personnel) that are comparable to this Project or required similar skills based on the person's assigned role/responsibility on this Project. Each project listed should include at a minimum the beginning and ending dates, client/company name for which the work was performed, client contact information for sponsoring Directors, Managers or equivalent level position (name, phone number, email address, company name, etc.), project title, project description, and a detailed description of the person's role/responsibility on the project.
- Education
- Professional Licenses/Certifications/Memberships
- Employment History