



Department of Administrative Services

Ohio Benefits Security Control Assessment (SCA)

R E Q U E S T F O R Q U O T A T I O N

State Term Schedule Only

OITRFQ-FY20-002

Table of Contents

INTRODUCTION AND BACKGROUND.....	3
PURPOSE OF THE REQUEST FOR QUOTATION	3
BACKGROUND	3
STATEMENT OF WORK.....	5
ADMINISTRATIVE	8
DUE DATES	8
SCHEDULE OF EVENTS.....	8
INQUIRIES	8
EVALUATION FACTORS FOR AWARD	10
EVALUATION	10
RESPONSES.....	12
GUIDELINES FOR QUOTATION PREPARATION.....	13
QUOTATION SUBMITTAL	13
PROPRIETARY INFORMATION	14
WAIVER OF DEFECTS.....	14
REJECTION OF QUOTATIONS.....	14
TERM AND CONTRACT	14
STATUS REPORTING.....	14
NON-DISCLOSURE AGREEMENT	15
EVALUTATION OF QUOTATIONS	15
APPENDIX A: FRAMEWORK FOR INDEPENDENT ASSESSMENT	17

INTRODUCTION AND BACKGROUND

PURPOSE OF THE REQUEST FOR QUOTATION

Please consider this State of Ohio Department of Administrative Services (DAS) Office of Information Technology (OIT) Request for Quotation for the following project:

Ohio Benefits Security Control Assessment

The State of Ohio is requesting a quotation for a Security Control Assessment (SCA) of Ohio Benefits and associated systems based on Minimum Acceptable Risk Standards for Exchanges (MARS-E) Version 2.0. This effort includes the SCA, Security Assessment Report (SAR), black box penetration test and report, and Remediation Actions Recommendation. Suppliers with extensive experience in the assessment of MARS-E Version 2.0 security and privacy controls and the ability to conduct a black box penetration test are sought for this RFQ. Suppliers interested in competing for this contract are requested to submit quotes for the activities listed in the statement of work.

Please include no more than three (3) resumes for the SCA work and three (3) resumes for the black box penetration test effort, per supplier.

The work must be completed within 90 days from the vendor's receipt of a purchase order.

Vendor's must hold a State Term Schedule (STS) to bid on this request for quotation.

BACKGROUND

To improve health outcomes for residents of Ohio, the Office of Budget and Management (OBM) and Department of Administrative Services (DAS) jointly established the Ohio Benefits Program to implement Ohio's vision for eligibility determination from an agency-centered approach to a consumer self-service model that is efficient, effective, and provides a customer-friendly experience. More specifically, individuals may apply for services or benefits through an externally facing web application, report changes to the application, and manage benefits online. Given the importance of this program to the Ohio Department of Medicaid (ODM) and the Ohio Department of Job and Family Services (ODJFS) operations as well as the coordination required with county agencies, local community stakeholders, and sister State agencies to ensure implementation of a user-friendly Integrated Eligibility (IE) and HHS Business Intelligence (BI) system for State and local workers and promote optimal use of these systems, a multiple release approach was pursued.

Development efforts on the program began in 2013 with the following major releases developed and deployed:

- Release 1 – IE and Health and Human Services (HHS) Business Intelligence (BI) for Medicaid Modified Adjustable Gross Income (MAGI) Program. Implementation occurred in October 2014.

- Release 2 – IE and HHS BI for Adults over 65, Blind or Disabled (ABD) Medicaid.
- Release 3 – IE and HHS BI for Supplemental Nutrition Assistance Program (SNAP) and Temporary Assistance for Needy Families (TANF) or (Cash). The pilot implementation to five counties occurred in October 2017 with statewide production deployment occurred during the third quarter 2018.

The solution is comprised of a packaged software solution, customizations to achieve Ohio Benefits requirements, and components that are created and implemented using Informatica PowerCenter and Multi-Domain Master Data Management products, and custom code and web services programmed using Java and XML.

Ohio Benefits is operated by DAS. It supports eligibility for ODM and related programs, which is very complex. There are more than 100 separate aid categories of eligibility, each with its own criteria limiting who may be covered, and what income or resource limits affect eligibility for coverage. Detailed eligibility information for an enrolled individual is critical during the processing of claims and other services within the entirety of the Medicaid Management Information System, including financial management and reporting. ODM and the sister State agencies contract with Ohio's 88 county departments of ODJFS and other local entities to perform certain program-related functions, including eligibility determination and enrollment, case management, and associated supported services.

Ohio Benefits and its associated systems included in the scope of this effort are:

- Ohio Benefits core systems including Business Intelligence (BI) system
- Enterprise Document Management System (EDMS)
- Integrated Voice Response (IVR)

Operation of these systems is dependent upon continued approval by the Centers for Medicare & Medicaid Services (CMS). To obtain this approval, ODM and DAS must obtain a Systems Control Assessment (SCA) and black box penetration test of Ohio Benefits and its associated systems.

STATEMENT OF WORK

The State is seeking a Supplier to deliver a MARS-E Version 2.0 Security Assessment Report (SAR) following the guidance outlined within the CMS Framework for the Independent Assessment of Security & Privacy Controls (attached as Appendix A) for Ohio Benefits and associated systems. The contract will be for a fixed price (broken down by deliverable) through State Term Schedule (STS) contract and must reflect or be lower than STS rates. The vendor must identify STS labor categories/position titles that will be used to develop each deliverable.

The Contract will be awarded on a Fixed Price arrangement and the work is planned to commence around July 20, 2020 and end within 90 days after the selected vendor receives a purchase order.

The scope of the MARS-E Version 2.0 SAR includes the following:

Scope	Ohio Benefits (incl. BI)	EDMS	IVR
Applications	Service-Oriented Architecture-based Java EE applications and portals, based primarily on the following technology: • Oracle Fusion Middleware • Oracle Policy Automation • Oracle Identity & Access Management • Adobe, Informatica, and IBM Cognos Analytics, SAS BI	Hyland's OnBase platform	CBTS hosted solution
Servers	• 54 physical systems • 132 virtual systems	• Installed on desktop systems at all ODJFS county locations	• 13 physical systems • 35 virtual systems
Users	• 54 internal users • 2,500,000 statewide users	• 3 admin users • 10,000 statewide users	• 3 internal users • 800 statewide users

Each of the above systems are administered by a different contractor and overseen by the Ohio Department of Administrative services. The contractors will be revealed during scope meetings with the selected supplier.

Specifically, the Assessment must:

Adhere to MARS-E Version 2.0 guidance. Refer to the following website for additional information:

<https://www.medicaid.gov/federal-policy-guidance/downloads/CIB-09-23-2015.pdf>

In addition, the security control assessment must incorporate or address each of the elements listed below.

1. Administer the assessment according to the detailed list of required security controls and control enhancements that can be found at <https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/3-MARS-E-v2-0-Catalog-of-Security-and-Privacy-Controls-11102015.pdf>
2. Conduct black box penetration testing against Ohio Benefits and its associated systems noted above (Core systems + BI, EDMS, IVR). Vulnerabilities are to be documented with suggested remediations. Any successful attacks should be documented, as well as detection, response, mitigation, reporting and remediation activities.
3. The assessment of three data centers (Columbus, Hamilton and Cincinnati) and one office site (Columbus).
4. Implementation responsibilities span all project work streams. Communication and coordination with the work stream leads is required.
5. Existing security control implementation details for Ohio Benefits and its' associated systems are contained in the System Security Plan (SSP), which will be provided after award.
6. Judgmental sampling is acceptable and anticipated, where appropriate. Please explain when and where you anticipate using this technique. When the sample-based approach is employed, the State expects 10 percent OR 10 to 25 items for each of the controls, as applicable.
7. Assessment must follow the procedures as outlined in Appendix A: "Framework for the Independent Assessment of Security and Privacy Controls,".
8. The reviews may involve one or more of the contractor organizations and DAS team members. Supporting information will be provided through SharePoint sites and hard copy documentation.

The following deliverables are required:

Deliverable #	Deliverable Name	Deliverable Description
1	Assessment Preparation	Develop, review, and approve a plan to assess the security controls. (See Appendix A for details.)
2	Security Control Assessment	Evaluate the security controls in accordance with the assessment procedures defined in the security assessment plan. (See Appendix A for details.)
3	Penetration Test & Report	Complete a black box penetration test, using tools, processes and rules of engagement reviewed and approved by the State. The results of the penetration test and the subsequent report, including the recommendation for correcting any weaknesses or deficiencies in the implementation and controls must be documented in the Security Assessment Report.
4	Security Assessment Report	Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment. (See Appendix A for details.)
5	Remediation Actions Recommendation	Describe initial remediation actions on security controls based on the findings and recommendations of the Security Assessment Report.

ADMINISTRATIVE

DUE DATES

All quotations are due by 1:00 PM EST, June 22, 2020. Any quotation received at the designated location after the required time and date specified for receipt shall be considered late and non-responsive. Any late quotations may not be evaluated for award.

SCHEDULE OF EVENTS

All times are Eastern Standard Time (EST).

Event	Date
1. RFQ Distribution to Suppliers	June 8, 2020
2. Q&A Period	June 10 – 15 at 8:00 AM
3. Quotation Due Date	June 22, 2020
4. Target Date for Interviews	June 29, 2020
5. Anticipated Decision	July 6, 2020
6. Anticipated Commencement of Work	July 20, 2020

INQUIRIES

Suppliers may make inquiries regarding this RFQ anytime during the Q&A Period listed in the Calendar of Events. To make an inquiry, Suppliers must use the following process:

1. Access the State's Procurement Website at <https://procure.ohio.gov>;
2. From the Quick Links menu on the right, select "**Bid Opportunities Search**;"
3. In the "**Document/Bid Number**" field, enter the RFQ number found on the first page of this RFQ;
4. Select "**Request for Quote**" from the Opportunity Type drop-down;
5. Click the "Search" button;
6. On the Opportunity Search Results page, click on the hyperlinked Bid Number;
7. On the Opportunity Details page, click the "Submit Inquiry" button;
8. On the document inquiry page, complete the required "Personal Information" section by providing:
 - a. First and last name of the prospective Supplier's representative who is responsible for the inquiry,
 - b. Name of the prospective Supplier,
 - c. The Supplier Representative's business phone number, and
 - d. The Supplier Representative's email address;
9. Type the inquiry in the space provided, including:
 - a. A reference to the relevant part of this RFQ,
 - b. The heading for the provision under question, and

- c. The page number of the RFQ where the provision can be found;
- 10. Enter the Confirmation Number at the bottom of the page;
- 11. Click the “Submit” button.

A Supplier submitting an inquiry will receive an email acknowledging receipt. The Supplier will not receive a personalized response to the question nor notification when the State has answered the question.

Suppliers may view inquiries and responses on the State’s Procurement Website by using the “Bid Opportunities Search” feature described above and by clicking the “View Q & A” button on the document information page.

The State usually responds to all inquiries within three business days of receipt, excluding weekends and State holidays. The State will not respond to any inquiries received after 8:00 a.m. on the inquiry end date.

EVALUATION FACTORS FOR AWARD

EVALUATION

Each candidate will be evaluated by their area of specialty and level of experience in the defined discipline or in a related area. The demonstrated familiarity with a variety of the defined disciplines concepts, practices, and procedures as well as their extensive experience and judgment to plan and accomplish goals will be considered. A wide degree of creativity and latitude is expected. The evaluation categories and weights are listed below:

Technical Proposal

- Experience & Education 20
- Communication Skills 10
- Management Skills 10
- Technical Acumen 20
- Deliverable Approach 5
- Deliverable Timeline 5

Cost Summary

- Total Cost of Deliverables 30

To ensure the scoring ratio is maintained, the State will use the following formulas to adjust the points awarded to each offeror.

The offeror with the highest point total for the Technical Proposal will receive 700 points. The remaining offerors will receive a percentage of the maximum points available based upon the following formula:

Technical Proposal Points = (Offeror's Technical Proposal Points / Highest Number of Technical Proposal Points Obtained) x 700

The offeror with the lowest proposed total cost for evaluation purposes will receive 300 points. The remaining offerors will receive a percentage of the maximum cost points available based upon the following formula:

Cost Summary Points = (Lowest Total Cost Proposed for all Deliverables / Offeror's Total Cost Proposed for all Deliverables) x 300

The total points score is calculated using the following formula:

Total Points = Technical Proposal Points + Cost Summary Points

The contractor will not be permitted to substitute personnel for those submitted for RFQ evaluation without the approval of DAS OIT. Note: If a substitution situation occurs, the proposal will be re-evaluated. If the substitution gives the contractor an unfair advantage during the RFQ process, the proposal may be eliminated or the other suppliers will also be given the chance to submit substitutions of personnel also.

All proposals will be evaluated for meeting the requested information. Incomplete proposals will not be reviewed. The proposals that provided the requested information will be evaluated for at least the highest prioritized candidate. The proposals will be scored based on the criteria requested above. We reserve the option to interview the top candidates.

Candidate substitutions between the proposal evaluation and interview periods are highly discouraged (see above). If DAS OIT has other qualified candidates, the contractor's proposal requesting a substitution will be denied at this stage and the proposal will be eliminated from evaluation. If DAS OIT does not have enough qualified candidates due to the substitution, all received proposals will be asked to confirm their candidates, given a couple of days to provide replacements, and the entire process will start over.

RESPONSES

Offeror responses **must** include:

Summary Deliverables or Deliverable Extracts that highlight the Offerors Capability and Experience (in general) and the Capability and Experience of the proposed Candidate(s) (specifically) in similar projects inclusive of tools, systems, training and alignment. Confidential client details should be redacted from these samples.

Deliverable Development Approach summarizes the Offerors approach, which must include the process for conducting security control risk and compliance assessments according to the framework.

One (1) Biographical (4-page maximum) Resume for Each Proposed Candidate that identifies and focuses on the specific disciplines the candidate is qualified for as it relates to this solicitation and other pertinent information.

Any candidate selected for interview will be expected to bring in work products, such as sample deliverables, and other materials developed for other Public and Private Sector clients that:

- Clearly demonstrate the capabilities of the proposed candidate to perform the work. The materials provided must be developed by the proposed team member (as opposed to the firm);
- Showcase candidate-specific innovative approaches, methods and tools used to develop materials for the respective clients – and by extension could be applied to State needs and requirements;
- Highlight meaningful results and successful business outcomes as a result of the candidate's efforts, involvement and creativity; and
- Demonstrate the ability of the candidate to address highly complex, multi-Agency or Enterprise level business problems and present these elements to a variety of technical and non-technical audiences at all levels of the State IT community.

Suppliers may redact confidential identifying information within these items as to preserve the confidentiality of client-specific elements that should not be placed in public domain upon the award of this solicitation.

Answers to the Requirements Outlined in Supplement A: State IT Policy, Standard and Service Requirements **and Supplement S:** State Security, Privacy and Data Handling Requirements.

GUIDELINES FOR QUOTATION PREPARATION

QUOTATION SUBMITTAL

Each Supplier must submit an electronic copy in **PDF Format ONLY** of its quotation (excluding cost information) by email with the email subject clearly marked “[Ohio Benefits Security Control Assessment – OITRFQ-FY20-002” along with the Suppliers name.

The cost information MUST be signed and submitted in a SEPARATE email. The email subject must be clearly marked “Ohio Benefits Security Control Assessment – OITRFQ-FY20-002 Cost Information” along with the Supplier’s name.

Each quotation must be organized in the format described below. Any material deviation from the format outlined below may result in a rejection of the non-conforming quotation. Each quotation must contain an identifiable tab sheet preceding each section of the document. The Quote should be good for a minimum of 45 days.

- Cover Letter
- Supplier contact name, email address, and phone number
- MBE or EDGE Certification – if applicable
- State Term Schedule (STS) Number
- Summary Deliverables or Deliverable Extracts
- Deliverable Development Approach
- Candidate Information:
 - Candidate Resume(s)
 - Discipline Expertise & References – Three References for Each Candidate (Attachment One)
 - Additional Candidate Information (Optional)
- Deliverable Cost & Timeline (Attachment Two in a separate email submission)
A cost basis table included as part of Attachment Two must be completed to show how the fixed deliverable costs in the Deliverable Cost & Timeline table were derived based on STS rates
- Conflict of Interest Statement
- Payment Address
- Proof of Insurance
- W-9 Form

The State will not be liable for any costs incurred by any supplier in responding to this RFQ, even if the State does not award a contract through this process. The State may decide not to award a contract at the State’s discretion. The State may reject late quotations regardless of the cause for the delay. The State may also reject any quotation that it believes is not in its interest to accept and may decide not to do business with any of the Suppliers responding to this RFQ.

Quotations MUST be submitted electronically to the State’s Procurement Representative:

OITAPRRequests@das.ohio.gov

PROPRIETARY INFORMATION

All quotations and other material submitted will become the property of the State and may be returned only at the State's option. Proprietary information should not be included in a quotation or supporting materials because the State will have the right to use any materials or ideas submitted in any quotation without compensation to the Supplier. Additionally, all quotations will be open to the public after the contract is awarded.

The State may reject any Proposal if the Supplier takes exception to the terms and conditions of this RFQ.

WAIVER OF DEFECTS

The State has the right to waive any defects in any quotation or in the submission process followed by a Supplier. But the State will only do so if it believes that is in the State's interest and will not cause any material unfairness to other Suppliers.

REJECTION OF QUOTATIONS

The State may reject any quotation that is not in the required format, does not address all the requirements of this RFQ, or that the State believes is excessive in price or otherwise not in its interest to consider or to accept. The State will reject any Non-STS responses. In addition, the State may cancel this RFQ, reject all the quotations, and seek to do the work through a new RFQ or other means.

TERM AND CONTRACT

- Compensation for work performed must be structured as a **Deliverables-based Fixed Price** through State Term Schedule (STS) contract and must reflect or be lower than STS rates. Vendors submitting a response to this RFQ must use STS labor categories/position titles and associated rates when determining the fixed deliverable cost. In addition to a cost for each deliverable, details must be provided showing how the fixed deliverable costs was derived based on STS rates.
- No additional costs, such as travel, meals, lodging, taxes, parking or other associated costs may be charged separately for this work.
- All contractors shall read, acknowledge and follow agency policies, rules and guidelines.
- All work performed by the supplier shall be deemed a "work-for-hire," and shall be the sole property of the State of Ohio. The supplier may not use such work without DAS OIT's written consent.

STATUS REPORTING

The contractor will provide weekly status reports to the State. The contractor will be responsible for meeting all timelines designated by the assigned Project Manager. Payment for services will be based on deliverable completion subject to the State's

approval of each deliverable. The State will review deliverables and provide feedback or approval for each deliverable within five business days of the receipt of deliverable.

NON-DISCLOSURE AGREEMENT

Both candidate and company may be required to sign a non-disclosure agreement, which prevents disclosure of any data obtained while on the engagement, which can be used to personally identify any parties at any time either during or after the engagement.

EVALUTATION OF QUOTATIONS

Clarifications and Corrections

During the evaluation process, the State may request clarifications from any Supplier under active consideration. It also may give any Supplier the opportunity to correct defects in its quotation. But the State will allow corrections only if they do not result in an unfair advantage for the Supplier and it is in the State's best interest.

Requirements

This RFQ asks for responses and submissions from Suppliers. While each criterion represents only a part of the total basis for a decision to award the contract to a Supplier(s), a failure by a Supplier to make a required submission or meet a requirement will normally result in a rejection of that Supplier's quotation. The value assigned to each criterion is only a value used to determine which quotation is the most advantageous to the State in relation to the other quotations that the State received. It is not a basis for determining the importance of meeting any requirement to participate in the quotation process.

The evaluation process may consist of up to three distinct phases:

1. The procurement representative's initial review of all quotations for defects;
2. The evaluation committee's evaluation of the quotations; and
3. Interviews (mandatory for selected candidates).

Initial Review

The procurement representative normally will reject any incomplete or incorrectly formatted quotation, though the procurement representative may elect to waive any defects or allow a Supplier to submit a correction. If a late quotation is rejected, the procurement representative will not open or evaluate the late quotations. The procurement representative will forward all timely, complete, and properly formatted quotations to an evaluation committee, which the procurement representative will chair.

Committee Review of the Quotations

The State's review committee will evaluate and numerically score each quotation that the procurement representative has forwarded to it.

The evaluation will result in a point total being calculated for each quotation. Those Suppliers submitting the highest-rated quotations may be scheduled for the next phase. The number of quotations forwarded to the next phase will be within the committee's

discretion, but regardless of the number of quotations selected for the next phase, they will always be the highest rated quotations from this phase.

At any time during this phase, the State may ask a Supplier to correct, revise, or clarify any portions of its quotation. The State will document all major decisions in writing and make these a part of the file along with the evaluation results for each quotation considered.

Once the technical merits of a quotation are considered, the costs of that quotation will be considered. But the State may also consider costs before evaluating the technical merits of the quotations by doing an initial review of costs to determine if any quotations should be rejected because of excessive cost. And the State may reconsider the excessiveness of any quotation's cost at any time in the evaluation process.

Interviews

The State may record any presentations, demonstrations and interviews.

Determination of Responsibility

The State may review the highest-ranking Suppliers or its key team members to ensure that the Supplier is responsible. The Contract may not be awarded to a Supplier that is determined to be not responsible. The State's determination of a Supplier's responsibility may include the following factors: The Supplier's and its key team members' experience, past conduct on previous Contracts, past performance on previous Contracts, ability to execute this contract properly and management skill. The State will make such determination of responsibility based on the Supplier's quotation, reference evaluations and any other information the State requests or determines to be relevant.

Changing Candidates

The major criterion on which the State bases the award of the contract is the quality of the Supplier's candidate(s). Changing personnel after the award may be a basis for termination of the contract.

Contract Award Process

It is the State's intention to award one contract under the scope of this RFQ based on the RFQ Calendar of Events schedule, so long as the State determines that doing so is in the State's best interests and has not otherwise changed the award date. Any award decision by the State under this RFQ is final. After the State makes its decision under this RFQ, all suppliers will be notified in writing of the final evaluation and determination as to their quotations.

APPENDIX A: FRAMEWORK FOR INDEPENDENT ASSESSMENT

Please see the attached appendix for the requirements of the CMS Framework for Independent Assessment of Security and Privacy Controls.

ATTACHMENT ONE
Personnel Profile Summary
Candidate References

Supplier Name:

Provide three references for which the **proposed candidate** successfully demonstrated meeting the requirements of the RFQ on projects of similar size and scope within the past five years. The name of the person to be contacted, phone number, company, address, brief description of project size and complexity, and date (month and year) of employment must be given for each reference. These references must be able to attest to the candidate's specific qualifications.

The reference should be a person within the client's organization and not a co-worker or a contact within the Supplier's organization.

If less than three references are provided, the Supplier must explain the reason for the shortage. The State may disqualify the Proposal if fewer than three references are given.

I.

Client Company:	Contact Name: (Indicate Primary or Alternate) Contact Title:
Client Address:	Contact Phone Number: Contact Email Address:
Project Name:	Beginning Date of Expr: Month/Year Ending Date of Expr: Month/Year
Description of services provided that align with the requirements of this project: Description of how client project size and complexity are similar to this project: 	

ATTACHMENT ONE
Personnel Profile Summary
Candidate References continued

11.

Client Company:	Contact Name: (Indicate Primary or Alternate) Contact Title:
Client Address:	Contact Phone Number: Contact Email Address:
Project Name:	Beginning Date of Expr: Month/Year Ending Date of Expr: Month/Year
Description of services provided that align with the requirements of this project: Description of how client project size and complexity are similar to this project: 	

ATTACHMENT ONE
Personnel Profile Summary
Candidate References continued

III.

Client Company:	Contact Name: (Indicate Primary or Alternate) Contact Title:
Client Address:	Contact Phone Number: Contact Email Address:
Project Name:	Beginning Date of Expr: Month/Year Ending Date of Expr: Month/Year
Description of services provided that align with the requirements of this project: Description of how client project size and complexity are similar to this project: 	

ATTACHMENT TWO

Deliverable Cost & Timeline

Deliverable #	Deliverable Name	Deliverable Description	Estimated Timeline (mm/yyyy-mm/yyyy)	Proposed Cost of Deliverable
1	Assessment Preparation	Develop, review, and approve a plan to assess the security controls. (See Appendix A for details.)		\$
2	Security Controls Assessment	Evaluate the security controls in accordance with the assessment procedures defined in the security assessment plan. (See Appendix A for details.)		\$
3	Penetration Test & Report	Complete a black box penetration test, using tools, processes and rules of engagement reviewed and approved by the State. The results of the penetration test and the subsequent report, including the recommendation for correcting any weaknesses or deficiencies in the implementation and controls must be documented in the Security Assessment Report.		\$
4	Security Assessment Report	Prepare the security assessment report documenting the issues, findings, and recommendations from the security control assessment. (See Appendix A for details.)		\$
5	Remediation Actions Recommendation	Describe initial remediation actions on security controls based on the findings and recommendations of the Security Assessment Report.		\$
Total Cost Proposed for all Deliverables				\$

The table immediately below contains a sample of a single row from a completed Cost Basis Table showing multiple resources providing work effort on a single deliverable. The sample row illustrates how the total cost of Deliverable “X” of \$6100.00 was derived based on STS rates and position titles.

Deliverable #	STS Position Title(s)	Estimated Number of hours	STS Hourly Rate(s)	Proposed Cost of Deliverable
X	Project Manager	20	\$90.00	\$1,800.00
	Systems/Data Analyst	40	\$75.00	\$3,000.00
	Technical Writer	20	\$65.00	\$1,300.00
	Total cost of Deliverable x			\$6,100.00

Cost Basis Table must be completed to show how the fixed deliverable costs in the Deliverable Cost & Timeline table above were derived based on STS rates. All compensation will be made based on deliverable acceptance at the fixed prices proposed in the Deliverable Cost & Timeline table and not based on hours worked.

Cost Basis Table

Deliverable #	STS Position Title(s)	Estimated Number of hours	STS Hourly Rate(s)	Proposed Cost of Deliverable
1				\$
2				\$
3				\$
4				\$
5				\$

DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard
Baltimore, MD 21244-1850



Framework for the Independent Assessment of Security and Privacy Controls

Final

March, 2016

Version 2.0

Record of Changes

Number	Date	Reference	A=Add, M=Modify, D=Delete	Description of Change	Change Request #
Version 1.0	07/2014		A	Initial draft release	
Version 1.2	10/2015		M	Address Privacy during the IA	
Version 1.9	01/2016		M	Incorporate Privacy requirements	
Version 2.0	03/2016		M	Incorporate comments and feedback	

Table of Contents

1. INTRODUCTION	3
1.1 Requirements Background.....	3
1.2 Purpose.....	3
2. ASSESSMENT INDEPENDENCE.....	4
2.1 Options for Independent Assessors.....	4
2.2 Purpose of the Independent Security and Privacy Control Assessment	4
3. ASSESSMENT PLANNING.....	6
4. SECURITY AND PRIVACY CONTROL ASSESSMENT METHODOLOGY	7
4.1 Tests and Analyses Performed.....	7
4.1.1 Security Control Technical Testing	8
4.1.2 Network and Component Scanning	8
4.1.3 Configuration Assessment	8
4.1.4 Documentation Review.....	9
4.1.5 Personnel Interviews.....	10
4.1.6 Observations	10
5. SECURITY AND PRIVACY ASSESSMENT REPORTING.....	12
5.1 Suggested Report Structure	12
5.1.1 SAR Content	12
5.1.2 Sample SAR Report Structure	13
APPENDIX A: SAMPLE SECURITY AND PRIVACY ASSESSMENT REPORT (SAR).....	14

1. INTRODUCTION

The State-Based Administering Entities (AE) are custodians of sensitive information such as Personally Identifiable Information (PII) for millions of US citizens. As such, they have a unique responsibility for ensuring its ultimate protection. Through continuous monitoring and regular security and privacy control testing, the AE demonstrates that it meets this responsibility. This *Framework for Independent Assessment of Security and Privacy Controls* provides an overview of the independent security and privacy assessment requirements and the associated Centers for Medicare & Medicaid Services (CMS) reporting process for Administering Entities.

1.1 REQUIREMENTS BACKGROUND

The *CMS Minimum Acceptable Risk Standards for Exchanges (MARS-E)*¹ Security Assessment Control, CA-2, requires all security and privacy controls attributable to a system or application be assessed over a 3-year period. Additionally, the MARS-E Independent Assessor Control, CA-2(1), requires that this assessment be conducted by an “independent assessor,” sometimes referred to as a “third-party” assessor.

The Security and Privacy Control Assessment (SCA) assists CMS information security and privacy staff with understanding the current security and privacy posture of the Affordable Care Act (ACA) information system and its potential impact on the broader ACA program. The SCA also provides the means to identify potential opportunities for supplying targeted technical security and privacy assistance.

1.2 PURPOSE

The framework is designed to accomplish the following objectives:

- Define assessment independence and the independent assessor (Section 2)
- Provide assessment planning considerations (Section 3)
- Provide a basic security and privacy control assessment methodology (Section 4)
- Summarize security and privacy assessment reporting (Section 5)
- Provide a sample security and privacy assessment report (Appendix A)

This document is not intended to provide detailed assessment planning and performance guidance.

¹ https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/

2. ASSESSMENT INDEPENDENCE

The MARS-E security control, CA-2(1), requires the employment of assessors or assessment teams with a CMS-defined level of independence to conduct security and privacy control assessments of the organization's information system. An assessor is independent if there is no perceived or actual conflict of interest with respect to the developmental, operational, and/or management chain associated with the information system and the determination of security and privacy control effectiveness. The AE's designated security and privacy official(s) must ensure that there is a complete separation of duties between the staff associated with the information system and the assessor or assessment team conducting the SCA. Additionally, the AE business or information system owner shall not influence the impartiality of the assessor or assessment team. To maintain the required objectivity and independence, there must be a continual evaluation of the relationships between the staff involved in the information system management and the assessors. The assessor is required to exercise professional due care, including observance of applicable professional standards.²

2.1 OPTIONS FOR INDEPENDENT ASSESSORS

In addition to contracting with an independent assessor to perform the SCA, several other options exist that could meet the independent assessor requirement for the AE. First, an AE may be able to leverage an existing state audit organization as an option for implementing an effective and independent security and privacy assessment program. An audit from a state audit organization meets the MARS-E requirement for an independent assessment if the audit incorporates the evaluation of all security and privacy control requirements specified in MARS-E. A second independent assessment option is to engage staff within the AE department to assess the MARS-E control implementation. The selected staff must have no direct responsibility for the system and/or the security or privacy posture of the system. A third option to meet the independent assessment requirement may be to leverage a current state contract, such as a contract for independent verification and validation services,³ that could be modified to include the independent assessment of MARS-E controls. The AEs may also be able to reuse existing audit reports if the audits meet the requirements of independence and the scope covers all or a portion of the MARS-E security or privacy controls; however, if only a portion of the controls are covered, assessment of the remainder of the controls is required.

2.2 PURPOSE OF THE INDEPENDENT SECURITY AND PRIVACY CONTROL ASSESSMENT

The independent SCA provides an understanding of the following:

- System compliance with MARS-E
- Underlying infrastructure's security posture
- The system and data security and privacy posture

² CMS IS Assessment Procedure, Page 3–4, https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/Assessment_Procedure.pdf

³ For Medicaid and CHIP agencies, see 45 CFR 95.626 at <http://www.ecfr.gov/cgi-bin/retrieveECFR?gp=1&SID=aafafe72e2870be9e12ea494007c7825&ty=HTML&h=L&r=SECTION&n=45y1.0.1.1.52.4.24.14>

- Proper security configuration associated with the database or file structure storing the data
- Systems technical, managerial and organizational adherence to the organization's security and privacy program, policies, and guidance

The purpose of an SCA is to determine whether the security and privacy controls are implemented correctly, operate as intended, and produce the desired outcomes for meeting the security and privacy requirements of the information system. The assessment only reflects the security and privacy posture at the time of the SCA while other MARS-E controls address ongoing monitoring of control implementation.

3. ASSESSMENT PLANNING

AEs are encouraged to develop an assessment strategy and procedure that provides a standardized approach for planning and resourcing the SCA of their information systems and underlying components. AEs are responsible for ensuring that each SCA has:

- Budget and assigned resources suitable for completing the assessment
- Clear objectives and constraints
- Well-defined roles and responsibilities
- Scheduling that includes defined events and deliverables

During planning for the SCA, the AE develops a scope statement that is dependent upon, but not limited to, the following factors:

- System boundaries
- Known business and system risks associated with the information system
- Dependence of the system on any hierarchical structure
- System development phase
- Documented security and privacy control requirements (MARS-E)
- Assessment type
- Legislative cycle

The contract statement of work should also provide support for clarifying findings and making corrective action recommendations after the assessment.

The contract should specify that contractor staff shall execute Non-Disclosure Agreements (NDA) prior to accessing any information related to the security and privacy of the system. Requests to access information should only be considered based on a demonstration of a valid need to know, and not the position, title, level of investigation, or position sensitivity level.

4. SECURITY AND PRIVACY CONTROL ASSESSMENT METHODOLOGY

The SCA methodology described in this document originates from the standard CMS methodology⁴ used in the assessment of all CMS internal and business partner information systems.

Assessment procedures for testing each security and privacy control are in the *MARS-E Document Suite, Version 2.0 Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges*⁵. A detailed assessment plan should be prepared using these security and privacy control assessment procedures. If necessary, modify or supplement the procedures to evaluate the system's vulnerability to different types of threats, including those from the insider, the Internet, or the network. The assessment methods include examination of documentation, logs and configurations, interviews of personnel, and testing of technical controls.

This assessment provides the independent assessor with an accurate understanding of the security and privacy controls in place by identifying the following:

- Application or system vulnerabilities, the associated business and system risks and potential impact
- Weaknesses in the configuration management process such as weak system configuration settings that may compromise the confidentiality, integrity, and availability of the system
- AE policies not followed
- Major documentation omissions and/or discrepancies

4.1 TESTS AND ANALYSES PERFORMED

The SCA includes tests that analyze the application or system and the associated infrastructure. The tests begin with high-level analyses of the application or system and increase in specificity to eventually include an analysis of each supporting component.⁶ Tests and analyses performed during an assessment should include the following:

- Security control technical testing
- Adherence to the organization's security and privacy program, policies, and guidance
- Network and component scanning
- Configuration assessment
- Documentation review
- Personnel interviews
- Observations

⁴ CMS IS Assessment Procedure, https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/Assessment_Procedure.pdf

⁵ Regulation and Guidance, https://calt.cms.gov/sf/projects/cms_aca_program_security_privacy/

⁶ A component is any element supporting the system that includes infrastructure software, hardware, and firmware.

4.1.1 Security Control Technical Testing

Typically, the assessment staff is provided user access to the system to conduct application or system security technical testing. To perform a thorough assessment of the application or system, application-specific user accounts that reflect the different user types and roles are created for the technical assessor. By providing the technical assessor with these accounts, the assessor can test application and system security controls that might otherwise not be tested. The assessors should not be given a user account with a role that would allow access to Protected Health Information (PHI) or Federal Tax Information (FTI) in any application or database.

The technical assessor attempts to expose vulnerabilities associated with gaining unauthorized access to the application or system resources by selecting and employing tools and techniques that simulate vulnerabilities such as buffer overflows and password compromises. The assessor must use caution to ensure no inadvertent altering of important system settings that may disable or degrade essential security or business functions. Since many automated testing utilities mimic signs of attack and/or exploit vulnerabilities, the assessor must identify proposed tools that pose a risk to the computing environment in the assessment plan. Furthermore, any testing that could potentially expose PII, PHI or FTI must be performed under the direct supervision of an authorized individual who is responsible for the data and can monitor the assessor's actions and take appropriate action to protect any data that is exposed.

The following list includes common test procedures and techniques of the technical assessment:

- Examination of the implemented access controls and identification and authorization techniques (e.g., log-on with easily-guessed/default passwords)
- Tests to determine if the system is susceptible to cross-site scripting (XSS), structured query language (SQL) injection, and/or other commonly exploited vulnerabilities
- Attempts to alter database management system settings
- Attempts to access hidden URLs
- Reviews of application-specific audit log configuration settings
- Determination if sensitive information is encrypted before being passed between the system and browser

4.1.2 Network and Component Scanning

In order to gain an understanding of the network and component infrastructure security posture, the SCA includes network-based scans of all in-scope network components to determine ports, protocols, and services running on each component. This provides a basis for determining the extent to which the system control implementation meets security control requirements. The results of these scans are used in conjunction with the configuration assessment.

4.1.3 Configuration Assessment

The purpose of the configuration assessment is to determine if AE security requirements are implemented correctly in the application, system, or system environmental components within the boundary of the application. The process for performing the configuration assessment requires the assessor to:

- Review the implemented configurations for each component against the AE security and privacy requirements

- Review access to system and databases for default user accounts
- Test firewalls, routers, systems, and databases for default configurations and user accounts
- Review firewall access control rules against the AE security requirements
- Determine consistency of system configuration with the AE-documented configuration

4.1.4 Documentation Review

The assessor must review all security and privacy documentation for completeness and accuracy. Through this process, the assessor will gain insight to determine if all controls are implemented as described. The review also augments technical control testing. For example, if the MARS-E control stipulates that the password length for the information system is required to be eight characters, the assessor must review the AE password policy or the System Security Plan (SSP) to make sure the documented password length is eight characters. During the technical configuration assessment, the assessor confirms passwords are actually configured as stated in the AE documentation. Core security documentation for review includes documents in Table 1.

Table 1: Core Security and Privacy Documentation

MARS-E Control Family	MARS-E Control Number	Document Name
Planning (PL)	PL-2: Security System Plan (SSP)	System Security Plan (SSP)
Contingency Planning (CP)	CP-2: Contingency Plan	Contingency Plan (CP)
Contingency Planning (CP)	CP-4: Contingency Plan Testing and Exercises	Contingency Plan Test Plan and Results
Incident Response (IR)	IR-8: Incident Response Plan	Incident Response Plan (IRP)
Incident Response (IR)	IR-3: Incident Response Testing and Exercises	IRP Test Plan
Awareness and Training (AT)	AT-3: Security Training	Security Awareness Training Plan
Awareness and Training (AT)	AT-4: Security Training	Training Records
Security and Assessment Authorization (CA)	CA-3: System Interconnections	Interconnection Security Agreements
Risk Assessment (RA)	RA-3: Risk Assessment	Information Security Risk Assessment (ISRA)
Authority and Purpose (AP)	AP-1: Authority to Collect	Privacy Impact Assessment or other privacy documents
Authority and Purpose (AP)	AP-2: Purpose Specification	Privacy documents and notices including, but not limited to, PIAs and agreements to collect, use, and disclose PII and Privacy Act Statements
Accountability, Audit, and Risk Management (AR)	AR-1: Governance and Privacy Program	Governance documents and privacy policy
Accountability, Audit, and Risk Management (AR)	AR-2: Privacy Impact and Risk Assessment	Documentation describing the AE privacy risk assessment process, documentation of privacy risk assessments performed by the organization

4.1.5 Personnel Interviews

The assessor conducts personnel interviews to validate that security and privacy controls are implemented, staff understand and follow documented control implementations, and updated documentation is appropriately distributed to staff. The assessor interviews business, information technology, and support personnel to ensure effective implementation of operational and managerial security and privacy controls across all support areas. Interviews are customized to focus on control assessment procedures that apply to individual roles and responsibilities and assure proper implementation and/or execution of security and privacy controls.

The SCA test plan identifies the designated subject matter experts (SME) interviewed. These SMEs should have specific knowledge of overall security and privacy requirements as well as a detailed understanding of the system's operational functions. The staff selected for conducting interviews should have the following roles:

- Business Owner(s)
- Application Developer
- Configuration Manager
- Contingency Planning Manager
- Database Administrator
- Data Center Manager
- Facilities Manager
- Firewall Administrator
- Human Resources Manager
- Information System Security Officer
- Privacy Program Manager
- Privacy Officer
- Media Custodian
- Network Administrator
- Program Manager
- System Administrators
- System Owner
- Training Manager

Although the initial identification of interviewees is determined when the assessment plan is prepared, additional staff may be identified as the interview process proceeds.

4.1.6 Observations

During the course of the assessment, the assessor also observes personnel behavior and the in-place, physical environmental controls, as applicable, to determine if staff follow the security and privacy policies, procedures and controls related to the physical environment are in place. For example, the assessor is required to observe:

- Processes associated with issuing visitor badges
- Requests for identification prior to visitor badge issuance
- Handling of output materials, including the labeling and discarding of output

- Equipment placement to prevent “shoulder surfing” or viewing from windows and open spaces
- Physical security associated with media protection, such as locking of telecommunication and wiring closets and access to facilities housing the system

5. SECURITY AND PRIVACY ASSESSMENT REPORTING

At the completion of the assessment, the assessor provides a security and privacy assessment report (SAR) to the AE business owner, who is then responsible for providing the report to CMS via the Collaborative Application Life Cycle Tool (CALT).

5.1 SUGGESTED REPORT STRUCTURE

The SAR structure and content of the report may be different for each AE; however, the information in the report should at a minimum provide the information noted in the next subsection and be consistent with the objectives of the assessment.

5.1.1 SAR Content

The report content should include the following information (*refer to the SAR Sample for additional details required in the report*):

- SCA methodology and testing performed
- Factual findings in accordance with the SCA tests performed
- Management information to render informed decisions regarding the application of resources and staffing to correct system weaknesses and vulnerabilities
- Remediation or compensating control recommendations

The report presents the findings of the assessment annotated in detail with the remediation recommendations for the weaknesses or deficiencies found in the information system security controls implementation. In order to reduce the risks posed to this important health care service and to protect the sensitive information of the citizens who use this service, the assessment team must assign a level of business as well as system risks to each specific finding. The assignment of business and system risk levels should follow the methodology outlined in NIST 800-30 Appendices G, H, and I.⁷ When assigning risk levels, CMS requires only three levels of granularity:

- **High** – a threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, and other organizations
- **Moderate** – a threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, and other organizations
- **Low** – a threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, and other organizations

The CMS reporting guidance for its internal and external partners, *CMS Reporting Procedure For Information Security (IS) Assessments, March 19, 2009 Version 5.0*,⁸ provides detailed information on reporting content.

⁷ NIST 800-30 Appendices G, H and I, http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

⁸ CMS IS Assessment Procedure, https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Downloads/Assessment_Procedure.pdf

5.1.2 Sample SAR Report Structure

The SAR structure should allow the assessor to communicate the assessment results to several audience levels, ranging from executives to technical staff. Appendix A provides a sample SAR, modeled after the SAR template used by CMS.⁹

⁹Document Assessments - Application Finding Report Template, <https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Information-Security-Library.html>

**APPENDIX A: SAMPLE SECURITY AND PRIVACY ASSESSMENT
REPORT (SAR)**

***<System Name>
Security and Privacy Assessment
Report***

<Date Here>

Table of Contents

1.	EXECUTIVE SUMMARY	1
1.1	<System Name> Background	1
1.2	Assessment Scope	1
1.3	Summary of Findings	2
1.4	Summary of Recommendations	3
2.	INTRODUCTION	4
2.1	Assessment Methodology	4
3.	DETAILED FINDING REPORTING	5
3.1	Tests and Analyses	5
3.1.1	Technical Testing Tools	5
3.2	Business Risk Reporting	5
3.2.1	Business Risk Level Assessment	5
3.2.2	Ease-of-Fix Assessment	5
3.2.3	Estimated Work Effort Assessment	6
4.	REPORT FINDINGS	7
5.	DOCUMENTATION LISTS	9

1. EXECUTIVE SUMMARY

The <AE> engaged <Assessor> to perform an onsite security and privacy controls assessment (SCA) of the <System Name>. <Assessor> conducted an assessment to determine:

- If the system is compliant with MARS-E
- If the underlying infrastructure supporting the system is secure
- If the system and data are securely maintained
- If proper configuration associated with the database and file structure storing the data are in place

1.1 <SYSTEM NAME> BACKGROUND

Provide a high-level overview of what the system is and what sensitive data it processes. Also briefly summarize the important, relevant facts about the system's essential business processes.

1.2 ASSESSMENT SCOPE

To determine the potential security and privacy risks to the AE, <Assessor> was tasked with providing a SCA of the <System Name> located at the {YYY Data Center (<Data center abbreviation>) in CITY NAME, STATE}. The application was assessed from <Dates of Assessment>. In accordance with the SCA Test Plan, the <Assessor> performed the following activities:

- *Interviewed selected personnel*
- *Reviewed system baselines*
- *Reviewed network component (switch/router/firewall) configurations*
- *Performed application security testing*
- *Conducted network vulnerability testing*
- *Reviewed database (DB) configuration settings*
- *Reviewed supplied security documentation*
- *Reviewed supplied privacy documentation*
- *Assessed privacy program compliance*

The following MARS-E security control families were the focus of the <System Name> assessment:

- *Access Control (AC)*
- *Awareness and Training (AT)*
- *Audit and Accountability (AU)*
- *Security Assessment and Authorization (CA)*
- *Configuration Management (CM)*
- *Contingency Planning (CP)*
- *Identification and Authentication (IA)*
- *Incident Response (IR)*
- *Maintenance (MA)*
- *Media Protection (MP)*
- *Physical and Environmental Protection (PE)*

- *Planning (PL)*
- *Program Management (PM)*
- *Personnel Security (PS)*
- *Risk Assessment (RA)*
- *System and Services Acquisition (SA)*
- *System and Communications Protection (SC)*
- *System and Information Integrity (SI)*
- *Authority and Purpose (AP)*
- *Accountability, Audit, and Risk Management (AR)*
- *Data Quality and Integrity (DI)*
- *Data Minimization and Retention (DM)*
- *Individual Participation and Redress (IP)*
- *Security (SE)*
- *Transparency (TR)*
- *Use Limitation (UL)*

1.3 SUMMARY OF FINDINGS

SUMMARY OF FINDINGS IS PROVIDED HERE:

Most findings in this document fall into the following areas:

- Access Control:
- Account Management:
- Application Security:
- Auditing and Monitoring:
- Configuration Management:
- Database Management:
- Documentation Updates:
- Identification and Authentication:
- Security Management:
- Software Maintenance:
- System and Information Integrity:
- Authority and Purpose:
- Accountability, Audit, and Risk Management:
- Data Quality and Integrity:
- Data Minimization and Retention:
- Individual Participation and Redress:
- Security:
- Transparency:
- Use Limitation:

1.4 SUMMARY OF RECOMMENDATIONS

For each finding, the Assessor has developed detailed recommendations for improvements that address the findings and the business and system risks. While all findings must be addressed, findings representing a high business risk should be mitigated or closed immediately to reduce the risk exposure. Most of the recommendations in this document fall into the following areas:

EXAMPLE FOLLOWS:

- *Block Unused Ports and Protocols:*
- *Perform Security and Privacy Monitoring:*
- *Strengthen Database Access Controls:*
- *Update Documentation:*

2. INTRODUCTION

2.1 SYSTEM SECURITY AND PRIVACY ASSESSMENT SUMMARY

The Assessor was tasked with conducting a security and privacy controls assessment (SCA) of the <System Name > to determine the overall business and system risk the system presents to the AE operations or ACA program.

Provide summary information here.

2.2 ASSESSMENT METHODOLOGY

Provide the purpose of the assessment including the controls tested and summary of the types of testing that was performed. This is obtained from the SCA test plan.

3. DETAILED FINDING REPORTING

Provides a descriptive analysis of the vulnerabilities identified through the comprehensive SCA process. Each vulnerability is explained, specific risks to the continued operations of the system are identified, the impact of each risk is analyzed, and suggested corrective actions for closing or reducing the impact of each vulnerability are presented.

3.1 TESTS AND ANALYSES

Provide details of testing and analysis performed.

3.1.1 TECHNICAL TESTING TOOLS

Provide a listing of all tools used to perform the technical test.

3.2 BUSINESS AND SYSTEM RISK REPORTING

For each weakness found, the Business and System Risk Level assessment value must be assigned to each Business and System Risk in order to provide a guideline by which to understand the procedural or technical significance of each finding. Further, an Ease-of-Fix and Estimated Work Effort value must be assigned to each Business Risk to demonstrate how simple or difficult it might be to complete the reasonable and appropriate corrective actions required to close or reduce the impact of each vulnerability.

3.2.1 BUSINESS AND SYSTEM RISK LEVEL ASSESSMENT

Management, operational, and technical vulnerabilities representing risks to the secure operation of the <System Name> are detailed as findings. Business and System Risks are technical or procedural in nature, and may result directly in unauthorized access. Each Business Risk has been assigned a Business and System Risk Level value of High, Moderate, or Low. The rating is, in actuality, an assessment of the priority with which each Business Risk will be viewed. The definitions in Table 1 apply to risk level assessment values.

Table 1. Business and System Risk Level Definitions

Rating	Definition of Business and System Risk Rating
High	A threat event could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals and other organizations.
Moderate	A threat event could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals and other organizations.
Low	A threat event could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals and other organizations.

3.2.2 EASE-OF-FIX ASSESSMENT

Each Business and System Risk is assigned an Ease-of-Fix value of Easy, Moderately Difficult, Very Difficult, or No Known Fix. The Ease-of-Fix value is an assessment of how difficult or easy it will be to complete reasonable and appropriate corrective actions required to close or reduce the impact of the vulnerability. The definitions in Table 2 apply to the Ease-of-Fix values.

Table 2. Ease-of-Fix Definitions

Rating	Definition of Ease-of-Fix Rating
Easy	The corrective action(s) can be completed quickly with minimal resources and without causing disruption to the system, or data.
Moderately Difficult	• Remediation efforts will likely cause a noticeable service disruption. • A vendor patch or major configuration change may be required to close the vulnerability. • An upgrade to software may be required to address the impact severity. • The system may require a reconfiguration to mitigate the threat exposure. • Corrective action may require construction or significant alterations to the manner in which business is undertaken.
Very Difficult	• The high risk of substantial service disruption makes it impractical to complete the corrective action for ACA systems without careful scheduling. • An obscure, hard-to-find vendor patch may be required to close the vulnerability. • Significant, time-consuming configuration changes may be required to address the threat exposure or impact severity. • Corrective action requires major construction or redesign of an entire ACA process.
No Known Fix	No known solution to the problem currently exists. The Risk may require the AE to: • Discontinue use of the software or protocol • Isolate the information system within the enterprise, thereby eliminating reliance on the system In some cases, the vulnerability is due to a design-level flaw that cannot be resolved through the application of vendor patches or the reconfiguration of the system. If the system is critical and must be used to support on-going ACA functions, the AE shall conduct, at a minimum, quarterly monitoring, which AE Management shall review, to validate that security incidents have not occurred

3.2.3 ESTIMATED WORK EFFORT ASSESSMENT

Each Business and System Risk has been assigned an Estimated Work Effort value of Minimal, Moderate, Substantial, or Unknown. The Estimated Work Effort value is an assessment of the extent of resources required to complete reasonable and appropriate corrective actions. This value provides input for assisting in the calculating of “Resources required” in the Plan of Action & Milestones (POA&M). The definitions in Table 3 apply to the Estimated Work Effort values.

Table 3. Estimated Work Effort Definitions

Rating	Definition of Estimated Work Effort Rating
Minimal	A limited investment of time [i.e., roughly three (3) days or less] is required of a single individual to complete the corrective action(s).
Moderate	A moderate time commitment, up to several weeks, is required of multiple personnel to complete all corrective actions.
Substantial	A significant time commitment, up to several months, is required of multiple personnel to complete all corrective actions. Substantial work efforts include the redesign and implementation of CMS network architecture and the implementation of new software, with associated documentation, testing, and training, across multiple CMS organizational units.
Unknown	The time necessary to reduce or eliminate the vulnerability is currently unknown.

4. REPORT FINDINGS

The report findings provide a descriptive analysis of the vulnerabilities identified through the comprehensive SCA process. Each vulnerability is explained, specific risks to the continued operations of the system are identified, the impact of each risk is analyzed, and suggested corrective actions for closing or reducing the impact of each vulnerability are presented. The vulnerabilities are ordered in a format that will enable the business owner to develop an efficient and workable action plan to remediate all risks. The Findings are ordered first by Business Risk Level, from High Risk to Low Risk, and then by Estimated Work Effort, from Substantial to Minimal.

(Table 1. <Report Finding> <Short Title> presents a table example to use for each vulnerability found during the SCA.)

Table 1. <Report Finding><Short Title>

1. <Report Finding>	<Short Title>
---------------------	---------------

Applicable Standards:**MARS-E Control Families:** <Security or Privacy Control>**Control Number:** <Reference>**Business Risk Level: (High Risk, Moderate Risk, or Low Risk)**

<Risk Level>

Ease-of-Fix: (Easy, Moderately Difficult, Very Difficult, or No Known Fix)

<Ease of Fix>

Estimated Work Effort: (Minimal, Moderate, Substantial, or Unknown; or a time estimate based on level of commitment and an adequate skill set)

<Level of Effort>

Weakness Description:

<Paragraph> <Report Date>

Finding

<Description>

Impacted components include: <hardware, software and firmware>

Failed Test Description

<Failed Condition>

Actual Test Results

<Actual Result>

Suggested Corrective Action(s):

<Recommendation>

Weakness Status:

<Status>

5. DOCUMENTATION LIST

The following table lists the documentation that <Assessor> requested prior to the onsite visit, as well as documentation provided to <Assessor> during and after the visit. The table includes the document element number, document title or information requested, and comments. Comments may include the name of the individual, organization, or agency that sent or delivered the documents and the date <Assessor> received the documents. – ***This is a sample list, not all inclusive***

Table 4. Documentation Requested/Reviewed

Document Element #	Document/Information Requested	Comments
	Information System Risk Assessment	
	System Security Plan Template (For Security and Privacy Controls)	
	Contingency Plan	
	Interconnection Security Agreement	
	Contingency Plan Test	
	Configuration and Change Management Process	
	Baseline security configurations for each platform and the application within scope and baseline network configurations	
	Security Awareness and training Plan	
	Training Records	
	Incident Response (IR) Procedures	
	Privacy Impact Assessment (PIA)	

Supplement A:

State IT Policy, Standard and Service Requirements

Revision History:

Date:	Description of Change:
1/01/2019	Original Version
10/18/2019	Updated to modify service descriptions, include new services, and remove older services. A new Appendix A - Request for Variance to State IT Policy, Standard or Service Requirements was added.

Contents

1. Overview of Supplement	4
2. State IT Policy and Standard Requirements	4
3. State IT Service Requirements	5
3.1. Requirements Overview	5
3.2. Solution Architecture Requirements	5
3.3. State of Ohio IT Services	5
3.3.1. InnovateOhio Platform	5
3.3.1.1. Digital Identity Products	6
3.3.1.2. User Experience Products	6
3.3.1.3. Analytics and Data Sharing Products	7
3.3.2. Application Services	7
3.3.2.1. Enterprise Document Management Solution (DMS):	7
3.3.2.2. Electronic Data Interchange (EDI) Application Integration:	8
3.3.2.3. Enterprise Business Intelligence (BI):	8
3.3.2.4. Enterprise eLicense:	9
3.3.2.5. ePayment Business Solution:	10
3.3.2.6. Enterprise eSignature Service:	10
3.3.2.7. IT Service Management Tool (ServiceNow):	10
3.3.2.8. Ohio Benefits:	11
3.3.2.9. Ohio Business Gateway (OBG):	11
3.3.2.10. Ohio Administrative Knowledge System (OAKS):	11
3.3.2.11. Enterprise Geocoding Services (EGS):	12
3.3.2.12. Geographic Information Systems (GIS) Hosting:	12
3.3.3. Data Center Services	13
3.3.3.1. Advanced Interactive eXecutive (AIX):	13
3.3.3.2. Backup:	13
3.3.3.3. Data Center Co-Location:	13
3.3.3.4. Data Storage:	13
3.3.3.5. Distributed Systems DRaaS:	13
3.3.3.6. Mainframe Business Continuity and Disaster Recovery:	14
3.3.3.7. Mainframe Systems:	14
3.3.3.8. Metro Site Facility:	15
3.3.3.9. Server Virtualization:	15
3.3.4. Hosted Services	15
3.3.4.1. Database as a Service:	15
3.3.4.2. Database Support:	16
3.3.5. IT Security Services	16
3.3.5.1. Secure Sockets Layer (SSL) Digital Certificate Provisioning:	16
3.3.6. IT Support Services	16
3.3.6.1. Enterprise End User Support:	16
3.3.6.2. Enterprise Virtual Desktop:	17
3.3.7. Messaging Services	17
3.3.7.1. Microsoft License Administration (Office 365):	17

3.3.8. Network Services	18
3.3.8.1. Ohio One Network:	18
3.3.8.2. Secure Authentication:	18
3.3.8.3. Wireless as a Service:.....	18
3.3.9. Telephony Services.....	18
3.3.9.1. Voice Services – VoIP	19
3.3.9.2. Toll-Free Services:.....	19
3.3.9.3. Automatic Caller Navigation and Contact Center Services (ACD/Contact) Centers:	19
3.3.9.4. Call Recording Services:.....	19
3.3.9.5. Conferencing	19
3.3.9.6. Fax2Mail:	19
3.3.9.7. Session Initiation Protocol (SIP) Call Paths:.....	19
3.3.9.8. Site Survivability:	20
3.3.9.9. VoIP related Professional Services and Training:.....	20
Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements	21

1. Overview of Supplement

This supplement shall apply to any and all work, services, locations and computing elements that the Contractor will perform, provide, occupy or utilize in conjunction with the delivery of work to the State and any access to State resources in conjunction with delivery of work.

This includes, but is not limited to:

- Major and minor projects, upgrades, updates, fixes, patches and other software and systems inclusive of all State elements or elements under the Contractor's responsibility utilized by the State;
- Any systems development, integration, operations and maintenance activities performed by the Contractor;
- Any authorized change orders, change requests, statements of work, extensions or amendments to this contract;
- Contractor locations, equipment and personnel that access State systems, networks or data directly or indirectly; and
- Any Contractor personnel, or sub-contracted personnel that have access to State Data as defined below:
 - "State Data" includes all data and information created by, created for, or related to the activities of the State and any information from, to, or related to all persons that conduct business or personal activities with the State, including, but not limited to Sensitive Data.
 - "Sensitive Data" is any type of data that presents a high or moderate degree of risk if released, disclosed, modified or deleted without authorization. Sensitive Data includes but is not limited to:
 - Certain types of personally identifiable information (PII) that is also sensitive, such as medical information, social security numbers, and financial account numbers.
 - Federal Tax Information (FTI) under IRS Special Publication 1075.
 - Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA).
 - Criminal Justice Information (CJI) under Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy.
 - The data may also be other types of information not associated with an individual such as security and infrastructure records, trade secrets, and business bank account information.
- The terms in this supplement are in addition to the Contract terms and conditions. In the event of a conflict for whatever reason, the highest standard contained in the Contract shall prevail.

Please note that any proposed variances to the requirements outlined in this supplement are required to be identified in Appendix A - Request for Variance to State IT Policy, Standard or Service Requirements. Offerors are asked not to make any changes to the language contained within this supplement. In the event the Offeror finds it necessary to deviate from any of the standards or State IT services, a variance may be requested, and the Offeror must provide a sufficient business justification for the variance request. In the event that a variance is requested post award, e.g., a material change to the architecture, the Enterprise IT Architecture Team will engage with the Contractor and appropriate State stakeholders to review and approve/deny the variance request.

2. State IT Policy and Standard Requirements

The Contractor will comply with State of Ohio IT policies and standards. For the purposes of convenience, a compendium of IT policy and standard links is provided in the table below.

Table 1 – State of Ohio IT Policies, Standards, IT Bulletins and DAS Policies

Item	Link
State of Ohio IT Policies	https://das.ohio.gov/Divisions/Information-Technology/State-of-Ohio-IT-Policies
State of Ohio IT Standards	https://das.ohio.gov/Divisions/Information-Technology/State-of-Ohio-IT-Standards
State of Ohio IT Bulletins	https://das.ohio.gov/Divisions/Information-Technology/State-of-Ohio-IT-Bulletins
DAS Policies	100-11 Protecting Privacy 100-12 ID Badges & Visitors Policy 700-00– Technology / Computer Usage Series 2000-00 – IT Operations and Management Series https://das.ohio.gov/Divisions/Administrative-Support/Employees-Services/DAS-Policies

3. State IT Service Requirements

3.1. Requirements Overview

Contractors performing the work under the Contract are required to comply with the standards and leverage State IT services outlined in this document unless the State has approved a variance. See note above in Section 1 regarding instructions to propose variances to the requirements outlined in this supplement.

3.2. Solution Architecture Requirements

Unless stipulated otherwise in the RFP, on premise or cloud-based solutions are permitted by the State. Custom or unique built solutions must comply with State requirements including using the State’s virtualized computing platform (State Private Cloud) or the State of Ohio Enterprise brokered public cloud service and running on databases that comply with the State’s supported database platforms. Custom or unique built solutions are required to include installation of third-party applications on State provided computing platforms which could be on the State-run private cloud or the State-run public cloud. Dedicated server platforms are not compliant with the State’s virtualization requirements. The State provides different storage pools (tiers) of storage with the ability to use and allocate the appropriate storage type based on predetermined business criticality and requirements. Storage pools are designed to support different I/O workloads. Custom or unique built solutions must take advantage of the State’s storage service offerings.

Custom or unique built solutions must be developed in open or industry standard languages (e.g. Java, .NET, PHP, etc.). Applications must be developed with standards-based open application programming interfaces and all available features and functionality accessible via APIs must be disclosed in the proposed solution. Custom or unique built solutions with Open APIs proposed must include periodic updates throughout the project lifecycle and a final update as part of the closure phase.

Cloud-based solutions must utilize as many platform services as possible and comply with State requirements to run in the State of Ohio Enterprise brokered public cloud service. Currently, Microsoft Azure and Amazon Web Services are hosted by DAS OIT for the State of Ohio.

3.3. State of Ohio IT Services

The Department of Administrative Services Office of Information Technology (DAS OIT) delivers information technology (IT) and telecommunication services. DAS OIT is responsible for operating and maintaining IT and telecommunication hardware devices, as well as the related software. This document outlines a range of service offerings from DAS OIT that enhance performance capacity and improve operational efficiency. Explanations of each service are provided and are grouped according to the following solution categories.

3.3.1. InnovateOhio Platform

Executive Order 2019-15D, “Modernizing Information Technology Systems in State Agencies,” established the InnovateOhio Platform (IOP) initiative. IOP focuses on digital identity, the experience of the individual authorized to

access the system (“User”), analytics and data sharing capabilities. The InnovateOhio Platform provides integrated and scalable capabilities that better serve Ohioans.

3.3.1.1. Digital Identity Products

OH | ID - Digital identity solution for Ohio citizens:

Provides single sign-on for disparate systems, enhanced security and privacy, federal and state compliance, and personalized experience. Simple, secure access for citizens. Multiple levels of identity assurance.

- Single Sign-On
- Access Logging
- Real-Time Analytics
- 2-Factor Authentication (2FA)
- Access Management
- Self-Service Portal
- Identity Proofing
- Directory Integration

OH | ID Workforce - Digital identity solution for Ohio workforce

Provides single sign-on for disparate systems, enhanced security and privacy, federal and state compliance, and personalized experience. Simple, secure access for state and county employees, contractors, and external workers. Multiple levels of identity assurance.

- Single Sign-On
- Directory Integration
- Real-Time Analytics
- 2-Factor Authentication (2FA)
- Just-in-Time Provisioning
- User Management
- Access Logging
- Privileged Access Management

ID Platform – Software as a Service (SaaS) identity framework

Provides an authorization layer and allows for the integration and extension of InnovateOhio Platform identity services into applications. Customizable to User needs.

- Fine-Grain Authorization Management
- Real-Time Analytics
- Extendable Services from OH|ID
- Cloud-Based Infrastructure

3.3.1.2. User Experience Products

IOP Portal Builder - Website template accelerator:

An accelerator to easily create modern, responsive and ADA-compliant websites and portals for the InnovateOhio cloud platform. The InnovateOhio Portal Builder is available in a Software as a Service (SaaS) form.

- Standardized Dynamic Templates
- Automated Workflows
- Governance & Access Control
- Optimized Content Search
- ADA-Compliant
- Content Management
- Integration with OH|ID
- Real-Time Analytics
- Aggregate Applications
- Customizable Features
- Mobile Ready
- Site Analytics

IOP myOhio - The State’s Intranet platform

Features intuitive navigation, simplified access to on-boarded business applications, and a modernized, mobile-responsive design. Automates compliance with accessibility standards per Section 508 of the Rehabilitation Act.

- Single Sign-On
- Personalized Content
- Content Management
- Near Real-Time Syndication
- 2-Factor Authentication (2FA)
- Access Logging
- Optimized Content Search
- Application Store
- Mobile Ready
- Automated Workflows
- Real-Time Analytics
- Site Analytics

IOP Digital Toolkit - Free User experience digital toolkit

Reusable components for quick deployment of websites, portals and applications. Universal framework for developers and designers. Consistent and compliant User experiences.

- Mobile Ready
- Real-Time Analytics
- Style Guide
- Customizable Features
- Sample Code
- ADA-Compliant
- Standardized Dynamic Templates

3.3.1.3. Analytics and Data Sharing Products

Applied Analytics

Ohio's applied analytics solution provides the ability to build analytical and reporting solutions and deploy them in the most impactful manner possible by putting data in the hands of Users in their natural workflow. From ideation and solution design to data science and engineering, the applied analytics solution enables the User to move from concept to results.

- Advanced Data Science
- Data Strategy Optimization
- Ideation & Scoping
- Solution Design
- Visual Data Discovery
- Workflow Integration

Big Data Platform

Ohio's data sharing and analytics platform provides public/private cloud deployment models that are secure, flexible, and scalable, powering analytics across data of any type or source to gain deeper insights and drive impactful outcomes.

- Data Sharing
- Diverse Data
- Hybrid Cloud
- Massive Volumes
- Rapid Prototyping
- Real-Time Analytics
- Security & Compliance

Data Management

Ohio's self-service data management suite provides rich and secure capabilities to harness the power of the analytics platform leveraging User friendly and pre-configured technologies. Additionally, the suite supports a bring-your-own-tool approach allowing analysts and data scientists to work on the platform with the technologies they are most comfortable using.

- Audit
- Bring Your Own Tool (BYOT)
- Data Engineering
- Data Exploration
- Data Lineage
- Data Profiling
- Governance & Security
- Pre-Built Pipelines
- Self-Service Support

Please explain how the InnovateOhio Platform will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

3.3.2. Application Services

3.3.2.1. Enterprise Document Management Solution (DMS):

The Enterprise Document Management Solution (DMS) is a standardized, integrated solution for document and content management. The core components of the solution include:

- **Document Management** core capabilities such as: secure check-in / check-out, version control, and index services for business documents, audio / video files, and Environmental Systems Research Institute (ESRI) / Geographic Information Systems (GIS) maps.
- **Image Processing** for capturing, transforming and managing images of paper documents via scanning and / or intelligent character recognition technologies such as Optical Character Recognition.
- **Workflow / Business Process Management (BPM)** for supporting business processes, routing content, assigning work tasks and creating audit trails.
- **Records Management** for long-term retention of content through automation and policy, ensuring legal, regulatory and industry compliance.
- **Web Content Management (WCM)** for controlling content including content creation functions, such as templating, workflow and change management and content deployment functions that deliver content to Web servers.
- **Extended Components** can include one or more of the following: Digital Asset Management (DAM), Document Composition, eForms, search, content and analytics, e-mail and information archiving.

3.3.2.2. Electronic Data Interchange (EDI) Application Integration:

EDI Application Integration service is a combination of Application Integration, Data Exchange and Electronic Data Interchange (EDI) functionality. This service provides application to application connectivity to support interoperable communication, data transformation, and business process orchestration amongst applications on the same or different computing platforms. Business process orchestration between many data formats may be supported including Web Services, XML, People-Soft, FTP, HTTP, MSMQ, SQL, Oracle, Flat File, SAP, DB2, CICS, EDI, HIPAA, HL7, Rosetta Net, etc.

The Data Exchange component allows unattended delivery of any electronic data format via encrypted files over public FTP, FTPS, SFTP, VPN. Application Integration services are offered via:

- **End Points** – also referred to as a mailbox, this is a connectivity point to facilitate the movement or transaction of data between two or more entities.
- **KBs** – represents the size in kilobytes of a message that is transformed or processed. This typically refers to a document or file conversion or a format change.
- **Messages** – a discrete unit of data that is moved or transacted between two or more entities. A message typically represents a business document or a file.

3.3.2.3. Enterprise Business Intelligence (BI):

The State of Ohio Enterprise Business Intelligence (BI) service provides enterprise data warehousing, business and predictive analytics, and decision support solutions. By turning raw data into usable information, BI helps Users analyze policies and programs, evaluate operations, and drive decisions. The core information available for analysis includes:

Health and Human Services Information

- Ohio Benefits
- Medicaid Claims
- Medicaid Enrollment
- Medicaid Financial
- Medicaid Provider
- Long Term Care
- Medicare Claims

- Pharmacy

Financial Information

- General Ledger
- Travel and Expense
- Procure to Pay
- Capital Improvements
- Accounts Receivable
- Asset Management
- Budget/Planning
- Value Management
- Statewide Cost Allocation Plan
- Minority Business Enterprise (MBE) Program/Encouraging Diversity, Growth and Equity (EDGE) Program

Workforce and Human Resources

- Workforce Profile
- Compensation
- State of Ohio Payroll Projection Systems
- ePerformance
- Enterprise Learning Management

3.3.2.4. Enterprise eLicense:

Enterprise eLicense is the State of Ohio's online system used to manage the issuance, certifications, inspections, renewals and administration of professional licenses across the State. The eLicense application is a public/business facing system that is designed to foster the creation and growth of businesses in the State. The system is a central repository for license and certificate data, in addition to managing the generation and storage of correspondence. Secure fee collection is performed through an on-line payment processor, which includes bank transfers, credit cards, and other payment types. Core system capabilities include:

Customer Relationship Manager (CRM)

- Contact Management

Revenue

- Deposit Accounting Revenue Tracking
- Refund and Reimbursement Processing
- Fine and Penalty Tracking

License Administration

- Administration
- Workflow
- Reports

Enforcement

- Enforcement Activities
- Case Management Activities

Online Licensure Services

- Applications
- Renewals
- License Verification
- License Maintenance
- License Lookup Website
- Workflow
- Document Management

- Secure Payment Processing

Other Services

- Continuing Education Tracking
- Examinations
- Inspections
- Complaint Management

3.3.2.5. ePayment Business Solution:

The CBOSS ePayment Gateway solution is a highly flexible payment engine supporting a wide range of payment types: credit cards, debit cards, electronic checks, as well as recurring, remote capture and cash payments. The CBOSS ePayment Gateway solution utilizes a single, common gateway to permit the acceptance of payments from multiple client application sources: Web, IVR, kiosk, POS, mobile, over the counter, etc. Payment processing is supported through multiple credit card gateway options, automated clearing house (ACH) bank processing, and Telecheck services.

The CBOSS ePayment Gateway solution is compliant with the Payment Card Industry Data Security Standard (PCI DSS), the Electronic Fund Transfer Act (EFTA) and is audited to the standards of SSAE16 SOC1 Type II.

3.3.2.6. Enterprise eSignature Service:

OneSpan Sign is Ohio's enterprise solution for eSignatures. The product is a FedRAMP SaaS (Software as a Service) solution, which offers a standardized approach to cloud security. OneSpan Sign's eSignature functions include workflows, tracking, audit logs and protection against forgery/non-repudiation.

OneSpan Sign has an extensive library of open application programming interfaces (APIs) to integrate eSignatures with existing applications and core systems. OneSpan Sign's pre-built, third-party connectors enable the eSignature capabilities into business software products such as Dynamics CRM, Salesforce, Microsoft SharePoint, etc.

3.3.2.7. IT Service Management Tool (ServiceNow):

DAS OIT offers ServiceNow, a cloud-based IT Service Management Tool that provides internal and external support through an automated service desk workflow-based application which provides flexibility and ease-of-use. ServiceNow provides workflows aligning with Information Technology Infrastructure Library (ITIL) processes such as incident management, request fulfillment, problem management, change management and service catalog. These processes allow for the management of related fields, approvals, escalations, notifications and reporting needs.

Standard ServiceNow Features Include:

- **Incident Management** - Manage service disruptions and restore normal operation quickly.
- **Problem Management** - Identify the underlying cause of recurring incidents.
- **Change Management** - Minimize the impact of service maintenance.
- **Configuration Management** - Define and maintain a configuration management database (CMDB) for IT infrastructure.
- **Asset Management** - Manage assets and inventory records.
- **Service Catalog Management** – Automated process for goods and service requests.
- **Knowledge Management** - Gather, store and share knowledge within the organization.
- **Reporting** – Custom reporting.
- **Integration to AD, Event Monitoring, Discovery Tools, Exchange** – Integration to AD, Event Monitoring, Discovery Tools, Exchange – Integration with third-party applications.

- **Customized Portal Pages** – User friendly interface to create engaging and robust portals, dashboards, and applications.
- **Software Asset Management** – End to end software life cycle management on a single platform, to optimize spend and reduce compliance risk.
- **IT Operations Management (ITOM)** - Includes event management, service mapping, discovery, orchestration and cloud management.

3.3.2.8. Ohio Benefits:

Ohio Benefits provides a comprehensive and effective platform for planning, designing, development, deployment, hosting and ongoing maintenance of all State of Ohio Health and Human Services (HHS) Public Assistance Services and Programs.

Ohio Benefits provides superior eligibility services including citizen self-service, efficient workflow management and coordination, an agile and easily manageable rules engine, improved data quality and decision support capabilities. Ohio Benefits supports improvement in State and county productivity, capability and accessibility of benefits to Ohioans through a robust enterprise system. The Ohio Benefits platform provides four distinct technology domains:

1. **Common Enterprise Portal** – User Interface and User Experience Management, Access Control, Collaboration, Communications and Document Search capability.
2. **Enterprise Information Exchange** – Discovery Services (Application and Data Integration, Master Data Management (MDM), Master Person Index and Record Locator Service), Business Process Management, Consent Management, Master Provider Index and Security Management.
3. **Analytics and Business Intelligence** – Integration and delivery of analytics in the form of alerts, notifications and reports.
4. **Integrated Eligibility** – A common Enterprise Application framework and Rules Engine to determine eligibility and benefits for Ohio Public Benefit Programs.

Privacy and security are the foundational blocks of the platform which is compliant with all State and federal standards.

3.3.2.9. Ohio Business Gateway (OBG):

The [Ohio Business Gateway \(OBG\)](#) offers Ohio's businesses a time and money saving online filing and payment system that simplifies business' relationships with government. Ohio businesses can use OBG to access various services and electronically submit transactions and payments. The OBG also offers the ability for business to view historical filings (and payments) and allows for business activities to be provided by a third-party provider of professional accounting services. OBG Electronic Filing also partners with local governments to enable businesses to file and pay selected Ohio municipal income taxes.

OBG Electronic Filing routes data and payment information directly to program administrators so that they may continue to manage the overall account relationship.

3.3.2.10. Ohio Administrative Knowledge System (OAKS):

The Ohio Administrative Knowledge System (OAKS) is the State's Enterprise Resource Planning (ERP) system which provides central administrative business services such as Financial Management, Human Capital Management, Content Management, Enterprise Learning Management and Customer Relationship Management. Core system capabilities include:

Content Management (myohio.gov)

- Centralized Communications to State Employees and State Contractors
- OAKS alerts, job aids and news
- Statewide News
- Password Reset for Active Directory

Customer Relationship Management (CRM)

- Contact / Call Center Management

Enterprise Business Intelligence

- Key Financial and Human Resources Data, Trends and Analysis
- Cognos driven reporting
- Targeted Business Intelligence
- Tableau Analytics and Visualization

Enterprise Learning Management (ELM)

- Training Curriculum Development
- Training Content Delivery
- Training Status Tracking and Reporting

Financial Management (FIN)

- Accounts Payable
- Accounts Receivable
- Asset Management
- Billing
- eSourcing
- Financial Reporting
- General Ledger
- Planning and Budgeting
- Procurement
- Travel & Expense

Human Capital Management (HCM)

- Benefits Administration
- eBenefits
- ePerformance
- Kronos
- Payroll
- Position Management
- Time and Labor
- Workforce Administration

3.3.2.11. Enterprise Geocoding Services (EGS):

Enterprise Geocoding Services (EGS) combine address standardization, geocoding, and spatial analysis into a single service. Individual addresses can be processed in real time for online applications or large numbers of addresses can be processed in batch mode.

3.3.2.12. Geographic Information Systems (GIS) Hosting:

GIS Hosting delivers dynamic maps, spatial content, and spatial analysis via the Internet. Users can integrate enterprise-level GIS with map capabilities and spatial content into new or existing websites and applications.

Please explain how the State's Application Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

3.3.3.Data Center Services

3.3.3.1. Advanced Interactive eXecutive (AIX):

AIX is a proprietary version of the UNIX operating system developed by IBM. DAS OIT runs the AIX operating system on IBM Power hardware, as a physical server or logical partition (LPAR)/virtual server. All of the AIX systems are connected to the DAS OIT Enterprise Storage Area Network (SAN) for performance, general purpose or capacity-based storage. All systems are also provided backup and recovery services.

3.3.3.2. Backup:

The Backup service uses IBM Tivoli Storage Manager Software and provides for nightly backups of data. It also provides for necessary restores due to data loss or corruption. The option of performing additional backups, archiving, restoring or retrieving functions is available. DAS OIT backup facilities provide a high degree of stability and recoverability as backups are duplicated to the alternate site.

3.3.3.3. Data Center Co-Location:

The DAS OIT Co-Location service offers a Tier 3 capable secure data center environment with reliable uptime, power redundancy and redundant cooling to ensure uninterrupted access of critical data and applications in the State of Ohio Computer Center (SOCC). The SOCC is staffed and available to authorized personnel 24x7x365 and is accessible via electronic card key only.

3.3.3.4. Data Storage:

The services covered under Data Storage include:

High Performance Disk Storage service offers high-performance, high-capacity, secure storage designed to deliver the highest levels of performance, flexibility, scalability and resiliency. The service has fully redundant storage subsystems, with greater than five-nines availability, supporting mission critical, externally-facing and revenue-generating applications 24x7x365. High Performance Disk Storage is supplied as dual Enterprise SAN fiber attached block storage.

General Purpose Disk Storage service offers a lower-cost storage subsystem, which is not on a high performance disk. This service supports a wide range of applications, including email, databases and file systems. General Purpose Disk is also flexible and scalable and highly available. General Purpose Disk Storage is supplied as dual Enterprise SAN fiber attached block storage.

Capacity Disk Storage service is the least expensive level of disk storage available from DAS OIT. Capacity Disk is suitable for large capacity, low performance data, such as test, development and archival. Capacity Disk Storage is supplied as dual Enterprise SAN fiber attached block storage or as file-based storage.

3.3.3.5. Distributed Systems DRaaS:

Distributed Systems Disaster Recovery as a Service (DRaaS) offers server imaging and storage at a geographically disparate site from Columbus. The service provides a private Disaster Recovery as a Service solution connected to the State of Ohio Computer Center (SOCC) via the Ohio One Network that will consists of the following:

- Compute to allow expected performance in the event of a complete failover
- 24vCPU per host with 32 host in the environment all licensed with VMWare
- Support of the orchestration and replication environment
- Site connectivity
- Stored images available upon demand

Open Systems Disaster Recovery - Windows (1330 / 100607 / DAS505170/ 3854L) - Open Systems Disaster Recovery – Windows is a service that provides a secondary failover site for Windows based servers within the geographically disparate site. This service provides duplicative server compute and storage to match Server Virtualization and Data Storage capabilities as provisioned at the SOCC. This service is provided through a contracted third party who is responsible for all management and equipment at the facility.

Open Systems Disaster Recovery - AIX (1330 / 100607 / DAS505170/ 3854N) - Open Systems Disaster Recovery – AIX is a service that provides a secondary failover site for AIX based servers within the geographically disparate site. This service provides duplicative server compute and storage to match AIX Systems Services and Data Storage capabilities as provisioned at the SOCC. This service is provided through a contracted third party who is responsible for all management and equipment at the facility.

3.3.3.6. Mainframe Business Continuity and Disaster Recovery:

Business continuity involves planning for keeping all aspects of a business functioning in the midst of disruptive events. Disaster recovery, a subset of business continuity focuses on restoring the information technology systems that support the business functions.

Mainframe Disaster Recovery (DR) services are available for DAS OIT's IBM mainframe environment. Services are made available via IBM's Business Continuity and Resiliency Services, which provides hot site computer facilities at a remote location.

Tests are conducted bi-annually at IBM's hot site location, during which DAS OIT's mainframe computer infrastructure is restored. Once the mainframe system is operational, production applications are restored and extensive tests are conducted to ensure that those applications have been successfully recovered and would be available in the event of an actual disaster.

This service is designed to expand business continuity and disaster recovery capabilities in the most cost effective and efficient manner possible.

3.3.3.7. Mainframe Systems:

DAS OIT's Mainframe Systems services offer an IBM mainframe computer sysplex with a processing speed rating at 5,700 Million of Instructions per Second (MIPS). This mainframe uses the z/OS operating system and the Job Entry Subsystem (JES3). Additionally, the system is connected via fiber to DAS OIT's High Performance Disk Storage, which affords reliable and fast disk access and additional storage capacity when needed.

Services are provided using a wide range of application, transaction processing and telecommunications software. Data security and User authentication are provided by security software packages. Mainframe tape service option is available:

- Mainframe Virtual Tape - Virtual tape technology that optimizes batch processing and allows for better tape utilization using the EMC Disk Library for Mainframe (DLM) virtual tape.

3.3.3.8. Metro Site Facility:

The Metro Site Facility Service provides a secondary, near real-time (measured in ms) failover from the SOCC. This service provides for the facility, site connectivity, on-going support of server images for Disaster Recovery as a Service, and associated services. Metro Site Facilities are for the support of Virtual Server and Data Storage, providing Global/Metro Mirroring at a secondary near real time failover site within the Metro Columbus area.

3.3.3.9. Server Virtualization:

Server Virtualization is the practice of abstracting the physical hardware resources of compute, storage and networking of a host server and presenting those resources individually to multiple guest virtual servers contained in separate virtual environments. DAS OIT leverages the VMware vSphere platform to transform standardized hardware into this shared resource model that is capable providing solutions around availability, security and automation.

Server Virtualization includes:

- **DAS OIT Managed Basic Server Virtualization:** DAS OIT hosts the virtual server and manages the hardware/virtualization layer. DAS OIT is also responsible for managing the server's operating system (OS). This service includes 1 virtual CPU (vCPU), 1 GB of RAM and 50 GB of General Disk Storage used for the operating system.

Please explain how the State's Data Center Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

3.3.4. Hosted Services

3.3.4.1. Database as a Service:

Database as a Service provides an enterprise database solution that is easy to use and simple to update without incurring the cost of setting up and maintaining an enterprise database environment through which scaling, load balancing, failover and backup can all be managed. DAS OIT Database Specialists ensure that all aspects of handling data are taken care of which includes, but is not limited to, storage, backups, tuning and security.

Current Database Solutions being offered:

- SQL Server
- Oracle
- DB2

Oracle Exadata DBaaS:

- **Starter/Small Database:** 2 Cores, 6GB Ram, 200GB min Storage, *Up to 2 databases
Entry level database environment for small applications.
- **Medium Database:** 4 Cores, 8 GB Ram, 500GB Min Storage, *Up to 4 databases
Medium sized database environment for DB consolidation.
- **Large Database:** 6 Cores, 12GB Ram, 1TB Min Storage, *Up to 6 Databases

Optimal service for large, complex database and data warehouse environments.

*The maximum number of databases is dependent upon the database size and actual usage.

Based on the model the proposed service model for DAS OIT includes the following structure:

- **Small:** 2 Core = 1 billable unit per month.
- **Medium:** 4 Cores = 2 billable units per month.
- **Large:** 6 Cores = 3 billable units per month.

3.3.4.2. Database Support:

Database Support provides technical assistance for database implementation and usage. Services utilized may include any or all of the following service offerings: installation, upgrade and management of database software, database administration tools and packaged application database products, backup/recovery procedure implementation, monitoring, tuning and troubleshooting.

Please explain how the State's Hosted Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

3.3.5. IT Security Services

3.3.5.1. Secure Sockets Layer (SSL) Digital Certificate Provisioning:

SSL Digital Certificate Provisioning service provides SSL Certificate service across multiple enterprise service offerings. SSL certificates are used to provide communication security to various web sites and communications protocols over the internet (ex. Web Servers, Network Devices, Application Servers, Internet Information Server (IIS), Apache, F5 devices and Exchange servers). SSL Digital Certificate Provisioning supports the delegation of administration and reporting processes while leveraging a common portal.

In addition, please review the Security Supplement (Supplement S - State Information Security and Privacy Requirements and State Data Handling Requirements).

Please explain how the State's IT Security Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

3.3.6. IT Support Services

3.3.6.1. Enterprise End User Support:

Enterprise End User Support is a standardized, fully managed endpoint computing service. This Service uses enterprise tools and standards. This comprehensive service includes e-mail, network connectivity, device procurement, printer support, security policy maintenance, system monitoring, software updates and patching, software deployment to individuals and devices and inventory software and hardware. IT assets provided with the Enterprise End User Support include:

- Dedicated on-site technician
- Break/Fix
- Enterprise Image
- System Center Configuration Management (SCCM)
- Patch Management through SCCM
- Application packaging and deployment
- Asset management (hardware)
- Asset management (software)
- Application usage report provided upon request

3.3.6.2. Enterprise Virtual Desktop:

Enterprise Virtual Desktop service takes advantage of the Enterprise Private Cloud to store all electronic data via a virtual desktop. The service provides a platform with access to Microsoft Windows and State of Ohio business applications from any device, from any location, at any time.

The Enterprise Virtual Desktop service offers the following:

- **Hosted** - The unmanaged service provides an isolated and dedicated environment that is managed by DAS OIT. This hosted service includes a provisioning portal, a basic window image and a basic group policy for desktops but does not include management or deployment of specific software or desktop provisioning.
- **Managed** - The managed service provides an isolated and dedicated environment that is managed by DAS OIT including desktops and software deployment. The Managed service also includes all Hosted services, software packaging and updating, management of the operating system, deployments and updates.

Please explain how the State's IT Support Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

3.3.7. Messaging Services

3.3.7.1. Microsoft License Administration (Office 365):

The Office 365 service provides the ability to use email, Office 365 ProPlus, instant messaging, online meetings and web conferencing, and file storage all from the Cloud, allowing access to services virtually anytime and from anywhere and includes email archiving and eDiscovery services.

The Office 365 service provides licensing and support for email, Office 365 ProPlus (Outlook, Word, Excel, PowerPoint, Publisher, Skype for Business and OneNote), SharePoint, and OneDrive for Business. Microsoft Office Suite includes:

- Email in the Microsoft Cloud
- Office 365 ProPlus
- Skype for Business

- SharePoint Online
- OneDrive for Business

Please explain how the State’s Messaging Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

3.3.8. Network Services

Offeror’s solutions must work within the State’s LAN / WAN infrastructure.

3.3.8.1. Ohio One Network:

The State of Ohio’s One Network is a unified solution that brings together design, engineering, operations, service delivery, security, mobility, management, and network infrastructure to target and solve key government challenges by focusing on processes, procedures, consistency and accountability across all aspects of State, city and local government.

Ohio One Network can deliver an enterprise network access experience regardless of location or device and deliver a consistent, reliable network access method.

3.3.8.2. Secure Authentication:

The DAS OIT Secure Authentication service provides a managed two-factor User authentication solution. The authentication function requires the User to identify themselves with two unique factors, something they know and something they have, before they are granted access. Whether local or remote, this service ensures that only authorized individuals are permitted access to an environment.

3.3.8.3. Wireless as a Service:

Wireless as a Service is the IT Enterprise Wireless hosted network. This service is an all-inclusive enterprise level wireless LAN solution that offers guest, employee, voice and location-based services with 24/7 target availability.

Coverage is three tiered:

- Broad coverage – small number of Users with low throughput, i.e. public hot spot, warehouse.
- General data use – most common, general computing with robust data performance.
- High capacity use (Voice) – maximum capacity, high bandwidth Users, i.e. location and tracking service.

Please explain how the State’s Network Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

3.3.9. Telephony Services

3.3.9.1. Voice Services – VoIP

The State of Ohio hosted cloud VoIP service, also known as NGTS (Next Generation Telephony Service) provides core telephony, voice mail, e911, collaboration, video, audio, conferencing and auto attendant functions. Optional services include automatic call distributor (ACD), interactive voice response (IVR), multi-channel contact center solutions and session initiation protocol (SIP) trunking among a variety of other features. The service was the first business class phone system to offer closed captioning for the hearing impaired, and also includes features for those with vision and mobility impairments. The following voice services are offered in addition to the State's hosted VoIP service:

3.3.9.2. Toll-Free Services:

A service provided to incur telephone charges for incoming calls to an 8xx number.

3.3.9.3. Automatic Caller Navigation and Contact Center Services (ACD/Contact) Centers:

Contact Center Enterprise allows callers to fill in CRM forms with information prior to an agent responding. With IVR and Advanced Data Collection, callers will spend less time in Call Queues. However, during high demand times, callers can be put on Virtual Hold allowing callers to receive a call back when agents become available. Call recording with screen capture allows the User to monitor, record, store, and QA calls, helping insure a consistent service experience.

Service also includes multi-channel communications including chat, text, SMS and email to afford those trying to contact the State the ability to contact the State in a variety of ways.

3.3.9.4. Call Recording Services:

Call Recording Services for new VoIP profiles or modifying existing profiles.

3.3.9.5. Conferencing

This service offers a conferencing service via telephone lines. It provides voice conferencing capabilities within the network and participants can also join in from outside the network.

3.3.9.6. Fax2Mail:

Fax2Mail is a "hosted" fax solution that allows organizations to seamlessly integrate inbound and outbound fax with their existing desktop email and back-office environments. Fax2Mail is completely "cloud-based" (SaaS), providing an easy to implement, easy to manage solution requiring no expenditures on hardware or software. Fax2Mail solves all faxing requirements, including inbound and out-bound fax, both at the computer desktop and from/to back-office systems, ERP applications, and electronic workflows.

3.3.9.7. Session Initiation Protocol (SIP) Call Paths:

Session Initiation Protocol Call Paths is used to allocate bandwidth. SIP Call paths:

- Provide existing telephony infrastructure with NGTS services.
- Extends infrastructure into the NGTS cloud.
- Leverages existing investment.
- Bridges the gap.
- All of the United States are Local Calls.
- Share video and collaboration.

- Leverage Toll Free offering.
- Centralized trunk savings.

3.3.9.8. Site Survivability:

Provides reliable communications via multi-feature redundancy for centralized call processing.

3.3.9.9. VoIP related Professional Services and Training:

Training services can be requested for VoIP telephone Users.

Professional services are also available for planning and migration of large contact centers, and for integration of contact centers with cloud services including Salesforce.

Please explain how the State's Voice/VoIP Services will be incorporated into the proposed solution. If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed variances must be noted in Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements. The language within the supplement shall not be modified.

--

Appendix A – Request for Variance to State IT Policy, Standard or Service Requirements

If an offeror needs to request a variance from a State IT Policy, Standard or Service requirement outlined in this supplement, please provide a rationale and an overview for each request in the table below.

Section Reference	IT Policy, Standard or Service Requirement	Rationale for Proposed Variance from Requirement	Proposed Variance Overview
Example: Section 3.3.2 Application Services - Enterprise eSignature Service	Example: The offeror shall use the State's eSignature solution.	Example: An eSignature solution is already integrated into the proposed solution. Using the State's service would result in increased cost due to integration complexities, as well as additional testing and resource needs. It would also result in longer deliverable timeframe.	Example: The Offeror's eSignature solution provides the same capabilities as the State's required solution. The Offeror's solution includes a workflow component and an eSignature User interface.

Supplement S

State Information Security and Privacy Requirements

State Data Handling Requirements

Revision History:

Date:	Description of Change:	Version
10/01/2019	Updated the State Information Security and Privacy Requirements as well as the State Data Handling Requirements to align with current practices.	1.0

Table of Contents

	Page
State Information Security, Privacy and Data Handling Requirements Instructions.....	1
Overview and Scope	1
State Requirements Applying to All Solutions.....	1
1. State Information Security and Privacy Standards and Requirements.....	2
1.1. The Offeror's Responsibilities	2
1.2. The State's Responsibilities.....	3
1.3. Periodic Security and Privacy Audits	3
1.3.1. State Penetration and Controls Testing	4
1.3.2. System Security Plan	4
1.3.3. Risk Assessment.....	5
1.4. Security and Data Protection	5
1.5. Protection of State Data	6
1.6. Handling the State's Data	6
1.7. Contractor Access to State Networks Systems and Data.....	8
1.8. State Network Access (VPN)	10
1.9. Portable Devices and Media	10
2. State and Federal Data Privacy Requirements	10
2.1. Contractor Requirements	11
2.2. Federal Tax Information (FTI)	11
2.2.1. IRS 1075 Performance Requirements	11
2.3.2. IRS 1075 Criminal/Civil Sanctions	13
2.4.3. Disclosure	14
2.5. Background Investigations of Contractor Personnel.....	14
3. Contractor Responsibilities Related to Reporting of Concerns, Issues and Security/Privacy Issues	15
3.1. General.....	15
3.2. Actual or Attempted Access or Disclosure.....	16
3.3. Unapproved Disclosures and Intrusions: Contractor Responsibilities	17
3.4. Security Incident Reporting and Indemnification Requirements	18
4. Security Review Services.....	19
4.1. Hardware and Software Assets	19
4.2. Security Standards by Device and Access Type	19
4.3. Boundary Defenses.....	20

4.4.	Audit Log Reviews	20
4.5.	Application Software Security	21
4.7.	Account Access Privileges.....	23
4.8.	Additional Controls and Responsibilities	23
Appendix A – Compensating Controls to Security and Privacy Supplement.....		25

State Information Security, Privacy and Data Handling Requirements Instructions

When providing a response to this Supplement, please follow the instructions below and frame your response as it relates to your proposed solution e.g., cloud (Software as a Service, Platform as a Service, or Infrastructure as a Service), on-premises, or hybrid.

1. After each specific requirement the offeror must provide a response on how the requirement will be met or indicate if it is not applicable and why.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement shall not be modified.

2. In the event there is a security or privacy requirement outlined in this supplement that needs to be met by a compensating control, please identify it [in Appendix A – Compensating Controls to Security and Privacy Requirements](#). Please be sure to provide a rationale for the change.

Reference	Current Language	Contractor's Proposed Change	Rationale of Proposed Change
Example: Supplement 2 - Page 11	Example: Provide vulnerability management services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. As a minimum, the Contractor must provide vulnerability scan results to the State monthly .	Example: Provide vulnerability management services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. As a minimum, the Contractor must provide vulnerability scan results to the State weekly .	Per company policy vulnerability report are only provided to customers on a quarterly basis.

3. Upon completion, please submit the security supplement responses with the proposal documentation.

Overview and Scope

This supplement shall apply to the Contracts for all work, services, locations (e.g., cloud (Software as a Service, Platform as a Service, or Infrastructure as a Service), on-premises, or hybrid) along with the computing elements that the Contractor will perform, provide, occupy, or utilize in conjunction with the delivery of work to the State and any access to State resources in conjunction with the delivery of work.

The selected Contractor will accept the security and privacy requirements outlined in this supplement in their entirety as they apply to the services being provided to the State. The Contractor will be responsible for maintaining information security in environments under the Contractor's management and in accordance with State IT security policies and standards.

This scope shall specifically apply to:

- Major and minor projects, upgrades, updates, fixes, patches, and other software and systems inclusive of all State elements or elements under the Contractor's responsibility utilized by the State.
- Any systems development, integration, operations, and maintenance activities performed by the Contractor.
- Any authorized change orders, change requests, statements of work, extensions, or amendments to this contract.
- Contractor locations, equipment, and personnel that access State systems, networks or data directly or indirectly.
- Any Contractor personnel or sub-contracted personnel that have access to State confidential, personal, financial, infrastructure details or sensitive data.

The terms in this supplement are in addition to the Contract terms and conditions. In the event of a conflict for whatever reason, the highest standard contained in this contract shall prevail.

Please note that any proposed compensating controls to the security and privacy requirements outlined in this supplement are required to be identified in Appendix A – Compensating Controls to Security and Privacy Requirements. Contractors are asked not to make any changes to the language contained within this supplement.

State Requirements Applying to All Solutions

This section describes the responsibilities for both the selected Contractor and the State of Ohio as it pertains to State information security and privacy standards and requirements for all proposed solutions whether cloud, on-premises, or hybrid based. The Contractor will comply with State of Ohio IT security and privacy policies and standards as they apply to the services being provided to the State. A list of IT policy and standard links is provided in the State IT Policy and Standard Requirements and State IT Service Requirements supplement.

1. State Information Security and Privacy Standards and Requirements

The Contractor is responsible for maintaining the security of information in accordance with State security policies and standards. If the State is providing the network layer, the Contractor must be responsible for maintaining the security of the information in environment elements that are accessed, utilized, developed, or managed. In either scenario, the Contractor must implement information security policies, standards, and capabilities as set forth in statements of work and adhere to State policies and use procedures in a manner that does not diminish established State capabilities and standards.

1.1. The Offeror's Responsibilities

The offeror's responsibilities with respect to security services include the following, where applicable:

- 1.1.1. Support State IT security policies and standards, which includes the development, maintenance, updates, and implementation of security procedures with the State's review and approval, including physical access strategies and standards, User ID approval procedures, and a security incident action plan.
- 1.1.2. Support the implementation and compliance monitoring as per State IT security policies and standards.
- 1.1.3. If the Contractor identifies a potential issue with maintaining an "as provided" State infrastructure element in accordance with a more stringent State level security policy, the Contractor shall identify and communicate the nature of the issue to the State, and, if possible, outline potential remedies for consideration by the State.
- 1.1.4. Support intrusion detection and prevention, including prompt State notification of such events and reporting, monitoring, and assessing security events.
- 1.1.5. Provide vulnerability management services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. At a minimum, the Contractor shall provide vulnerability scan results to the State monthly.
- 1.1.6. Develop, maintain, update, and implement security procedures, with State review and approval, including physical access strategies and standards, ID approval procedures and a security incident response plan.
- 1.1.7. Manage and administer access to the systems, networks, system software, systems files, State data, and end users if applicable.
- 1.1.8. Install and maintain current versions of system software security, assign and reset passwords per established procedures, provide the State access to create User IDs, suspend and delete inactive User IDs, research system security problems, maintain network access authority, assist in processing State security requests, perform security reviews to confirm that adequate security procedures are in place on an ongoing basis, provide incident investigation support (jointly with the State), and provide environment and server security support and technical advice.
- 1.1.9. Develop, implement, and maintain a set of automated and manual processes to ensure that data access rules are not compromised.
- 1.1.10. Perform physical security functions (e.g., identification badge controls and alarm responses) at the facilities under the Contractor's control.

1.2 The State's Responsibilities

The State will:

- 1.2.1. Develop, maintain, and update the State IT security policies, including applicable State information risk policies, standards, and procedures.
- 1.2.2. Provide the Contractor with contact information for security and program personnel for incident reporting purposes.
- 1.2.3. Provide a State resource to serve as a single point of contact, with responsibility for account security audits.
- 1.2.4. Support intrusion detection, prevention, and vulnerability scanning pursuant to State IT security policies.
- 1.2.5. Conduct a Security and Data Protection Audit, if deemed necessary, as part of the testing process.
- 1.2.6. Provide audit findings material for the services based upon the security policies, standards and practices in effect as of the effective date and any subsequent updates.
- 1.2.7. Assist the Contractor in performing a baseline inventory of User IDs for the systems for which the Contractor has security responsibility.
- 1.2.8. Authorize user IDs and passwords for State personnel for the system's software, software tools and network infrastructure systems and devices under Contractor management.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement shall not be modified.

--

1.3. Periodic Security and Privacy Audits

The State will be responsible for conducting periodic security and privacy audits and will generally utilize members of the Office of Information Security and Privacy, the Office of Budget and Management – Office of Internal Audit, and the Auditor of State, depending on the focus area of the audit. Should an audit issue or finding be discovered, the following resolution path shall apply:

If a security or privacy issue exists in any of the IT resources furnished to the Contractor by the State (e.g., code, systems, computer hardware and software), the State will have responsibility to address or resolve the issue. The State may elect to work with the Contractor, under mutually agreeable terms for resolution services or the State may elect to address the issue independent of the Contractor. The Contractor is responsible for resolving any security or privacy issues that exist in any of the IT resources they provide to the State.

For in-scope environments and services, all new systems implemented or deployed by the Contractor must comply with State security and privacy policies and standards.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.3.1. State Penetration and Controls Testing

The State may, at any time in its sole discretion, elect to perform a Security and Data Protection Audit. This includes a thorough review of Contractor controls, security/privacy functions and procedures, data storage and encryption methods, backup/restoration processes, as well as security penetration testing and validation. The State may utilize a third-party Contractor to perform such activities to demonstrate that all security, privacy, and encryption requirements are met.

State acceptance testing will not proceed until the Contractor cures, according to the State’s written satisfaction, all findings, gaps, errors or omissions pertaining to the audit. Such testing will be scheduled with the Contractor at a mutually agreed upon time.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.3.2. System Security Plan

A completed System Security Plan must be provided by the Contractor to the State and the primary point of contact from the Office of Information Security and Privacy no later than the end of the project development phase of the System Development Life Cycle (SDLC). The plan must be updated annually or when major changes occur within the solution. The templates referenced below are the required format for submitting security plans to the State.



Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.3.3. Risk Assessment

A Risk Assessment report completed within the past 12 months must be provided to the State and the primary point of contact from the Office of Information Security and Privacy no later than the project development phase of the System Development Life Cycle (SDLC). A new risk assessment must be conducted every two years, or as a result of significant changes to infrastructure, a system or application environment, or following a significant security incident.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.4. Security and Data Protection

All solutions must classify data per State of Ohio IT-13 Data Classification policy and per the sensitivity and criticality, must operate at the appropriate baseline (low, moderate, high) as defined in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations" (current, published version), be consistent with Federal Information Security Management Act ("FISMA 2014") requirements, and offer a customizable and extendable capability based on open-standards APIs that enable integration with third party applications. The solution must provide the State's systems administrators with 24x7 visibility into the services through a real-time web-based "dashboard" capability that enables them to monitor, in real or near real time, the services' performance against the established service level agreements and promised operational parameters.

If the solution is cloud based, the Contractor must obtain an annual audit that meets the American Institute of Certified Public Accountants (AICPA) Statements on Standards for Attestation Engagements ("SSAE") No. 16,

Service Organization Control 1 Type 2 and Service Organization Control 2 Type 2. The audit must cover all operations pertaining to the Services covered by this Agreement. The audit will be at the sole expense of the Contractor and the results must be provided to the State within 30 days of its completion each year.

At no cost to the State, the Contractor must immediately remedy any issues, material weaknesses, or other items identified in each audit as they pertain to the Services.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

--

1.5. Data

1.5.1. "State Data" includes all data and information created by, created for, or related to the activities of the State and any information from, to, or related to all persons that conduct business or personal activities with the State, including, but not limited to Sensitive Data.

1.5.2. "Sensitive Data" is any type of data that presents a high or moderate degree of risk if released or disclosed without authorization. Sensitive Data includes but not limited to:

1.5.2.1. Certain types of personally identifiable information (PII) that is also sensitive, such as medical information, social security numbers, and financial account numbers.

1.5.2.2. Federal Tax Information (FTI) under IRS Special Publication 1075,

1.5.2.3. Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA)

1.5.2.4. Criminal Justice Information (CJI) under Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy.

1.5.2.5. The data may also be other types of information not associated with an individual such as security and infrastructure records, trade secrets, and business bank account information.

1.6. Protection and Handling the State's Data

To protect State Data as described in this contract, the Contractor must use due diligence to ensure computer and telecommunications systems and services involved in storing, using, or transmitting State Data are secure and to protect State Data from unauthorized disclosure, modification, use or destruction.

To accomplish this, the Contractor must adhere to the following requirements regarding State Data:

- 1.6.1. Maintain in confidence State Data it may obtain, maintain, process, or otherwise receive from or through the State in the course of the contract.
- 1.6.2. Use and permit its employees, officers, agents, and subcontractors to use any State Data received from the State solely for those purposes expressly contemplated by the contract.
- 1.6.3. Not sell, rent, lease, disclose, or permit its employees, officers, agents, and sub-contractors to sell, rent, lease, or disclose, any such State Data to any third party, except as permitted under this contract or required by applicable law, regulation, or court order.
- 1.6.4. Take all commercially reasonable steps to (a) protect the confidentiality of State Data received from the State and (b) establish and maintain physical, technical, and administrative safeguards to prevent unauthorized access by third parties to State Data received by the Contractor from the State.
- 1.6.5. Apply appropriate risk management techniques to balance the need for security measures against the sensitivity of the State Data.
- 1.6.6. Ensure that its internal security policies, plans, and procedures address the basic security elements of confidentiality, integrity, and availability of State Data.
- 1.6.7. Align with existing State Data security policies, standards and procedures designed to ensure the following:
 - 1.6.7.1. Security and confidentiality of State Data
 - 1.6.7.2. Protection against anticipated threats or hazards to the security or integrity of State Data
 - 1.6.7.3. Protection against the unauthorized access to, disclosure of, or use of State Data
- 1.6.8. Suggest and develop modifications to existing data security policies and procedures or draft new data security policies and procedures when gaps are identified.
- 1.6.9. Maintain appropriate access control and authorization policies, plans, and procedures to protect system assets and other information resources associated with State Data.
- 1.6.10. Give access to State Data only to those individual employees, officers, agents, and sub-contractors who reasonably require access to such information in connection with the performance of Contractor's obligations under this contract.
- 1.6.11. Maintain appropriate identification and authentication processes for information systems and services associated with State Data.
- 1.6.12. Any Sensitive Data at rest, transmitted over a network, or taken off-site via portable/removable media must be encrypted pursuant to the State's data encryption standard, Ohio IT Standard ITS-SEC-01, "Data Encryption and Cryptography," and Ohio Administrative Policy IT-14, "Data Encryption and Securing State Data."
- 1.6.13. Any data encryption requirement identified in this supplement means encryption that complies with National Institute of Standards and Technology's Federal Information Processing Standard 140-2 as demonstrated by a valid FIPS certificate number.

- 1.6.14. Maintain plans and policies that include methods to protect against security and integrity threats and vulnerabilities, as well as detect and respond to those threats and vulnerabilities.
- 1.6.15. Implement and manage security audit logging on information systems, including computers and network devices.
- 1.6.16. Cooperate with any attempt by the State to monitor Contractor's compliance with the foregoing obligations as reasonably requested by the State. The State will be responsible for all costs incurred by the Contractor for compliance with this provision of this subsection.
- 1.6.17. Upon request by the State, promptly destroy or return to the State, in a format designated by the State, all State Data received from or through the State.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.7. Contractor Access to State Network Systems and Data

The Contractor must maintain a robust boundary security capability that incorporates generally recognized system hardening techniques. This includes determining which ports and services are required to support access to systems that hold State Data, limiting access to only these ports, and disabling all others.

To do this, the Contractor must:

- 1.7.1. Use assets and techniques such as properly configured firewalls, a demilitarized zone for handling public traffic, host-to-host management, Internet protocol specification for source and destination, strong authentication, encryption, packet filtering, activity logging, and implementation of system security fixes and patches as they become available.
- 1.7.2. Use multifactor authentication to limit access to systems that contain Sensitive Data, such as Personally Identifiable Information.
- 1.7.3. Assume all State Data is both confidential and critical for State operations. The Contractor's security policies, plans, and procedures for the handling, storage, backup, access, and, if appropriate, destruction of State Data must be commensurate to this level of sensitivity unless the State instructs the Contractor otherwise in writing.
- 1.7.4. Employ appropriate intrusion and attack prevention and detection capabilities. Those capabilities must track unauthorized access and attempts to access State Data, as well as attacks on the Contractor's infrastructure associated with the State Data. Further, the Contractor must monitor and appropriately

address information from its system tools used to prevent and detect unauthorized access to and attacks on the infrastructure associated with the State Data.

- 1.7.5. Use appropriate measures to ensure that State Data is secure before transferring control of any systems or media on which State data is stored. The method of securing the State Data must be in alignment with the required data classification and risk assessment outcomes, and may include secure overwriting, destruction, or encryption of the State data before transfer of control in alignment with NIST SP 800-88. The transfer of any such system or media must be reasonably necessary for the performance of the Contractor's obligations under this contract.
- 1.7.6. Have a business continuity plan in place that the Contractor tests and updates no less than annually. The plan must address procedures for responses to emergencies and other business interruptions. Part of the plan must address backing up and storing data at a location sufficiently remote from the facilities at which the Contractor maintains State Data in case of loss of State Data at the primary site. The Contractor's backup solution must include plans to recover from an intentional deletion attempt by a remote attacker exploiting compromised administrator credentials.

The plan also must address the rapid restoration, relocation, or replacement of resources associated with the State Data in the case of a disaster or other business interruption. The Contractor's business continuity plan must address short- and long-term restoration, relocation, or replacement of resources that will ensure the smooth continuation of operations related to the Sensitive Data. Such resources may include, among others, communications, supplies, transportation, space, power and environmental controls, documentation, people, data, software, and hardware. The Contractor also must provide for reviewing, testing, and adjusting the plan on an annual basis.

- 1.7.7. Not allow State Data to be loaded onto portable computing devices or portable storage components or media unless necessary to perform its obligations under this contract. If necessary, for such performance, the Contractor may permit State Data to be loaded onto portable computing devices or portable storage components or media only if adequate security measures are in place to ensure the integrity and security of State Data. Those measures must include a policy on physical security and appropriate encryption for such devices to minimize the risk of theft and unauthorized access as well as a prohibition against viewing sensitive or confidential data in public or common areas.
- 1.7.8. Ensure that portable computing devices have anti-virus software, personal firewalls, and system password protection. In addition, State Data must be encrypted when stored on any portable computing or storage device or media or when transmitted across any data network.
- 1.7.9. Maintain an accurate inventory of all such devices and the individuals to whom they are assigned.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

--

1.8. State Network Access (VPN)

Any remote access to State systems and networks, Contractor or otherwise, must employ secure data transmission protocols, including transport layer security (TLS) and public key authentication, signing and/or encryption. In addition, any remote access solution must use Secure Multipurpose Internet Mail Extensions (S/MIME) to provide encryption and non-repudiation services through digital certificates and the provided public key infrastructure (PKI). Multifactor authentication must be employed for users with privileged network access by State provided solutions.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

1.9. Portable Devices and Media

The Contractor must have reporting requirements for lost or stolen portable computing devices authorized for use with State Data and must report any loss or theft of such devices to the State in writing as defined in Section 3 Contractor Responsibilities Related to Reporting of Concerns, Issues and Security/Privacy Issues. The Contractor must have a written policy that defines procedures for how the Contractor must detect, evaluate, and respond to adverse events that may indicate an incident or an attempt to attack or access State Data or the infrastructure associated with State Data.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

2. State and Federal Data Privacy Requirements

All systems and services must be designed and must function according to Fair Information Practice Principles (FIPPS), which are transparency, individual participation, purpose specification, data minimization, use limitation, data quality and integrity, security, accountability, and auditing.

To the extent that personally identifiable information (PII) in a system is “protected health information” under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, the FIPPS principles must be implemented in alignment with the HIPAA Privacy Rule. To the extent that there is PII in a system that is not “protected health information” under HIPAA, the FIPPS principles must still be implemented and, when applicable, aligned to other laws or regulations.

2.1 Contractor Requirements

The Contractor specifically agrees to comply with state and federal confidentiality and information disclosure laws, rules and regulations applicable to the work associated with this Contract including but not limited to:

- 2.1.1. United States Code 42 USC 1320d through 1320d-8 (HIPAA).
- 2.1.2. Code of Federal Regulations for Public Health and Public Welfare: 42 CFR 431.300, 431.302, 431.305, 431.306, 435.945, 45 CFR 164.502 (e) and 164.504 (e).
- 2.1.3. Ohio Revised Code (ORC) 1347.01, 1347.04 through 1347.99, 2305.24, 2305.251, 3701.243, 3701.028, 4123.27, 5101.26, 5101.27, 5160.39, 5168.13, and 5165.88.
- 2.1.4. Corresponding Ohio Administrative Code Rules and Updates.
- 2.1.5. Systems and services must support and comply with the State’s security operational support model, which is aligned to NIST SP 800-53 (current, published version).
- 2.1.6. IRS Publication 1075, Tax Information Security Guidelines for federal, state, and local agencies.
- 2.1.7. Criminal Justice Information Systems Policy.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

2.2. Federal Tax Information (FTI)

All computer systems receiving, processing, storing, or transmitting Federal Tax Information (FTI) must meet the requirements defined in IRS Publication 1075.

2.2.1. IRS 1075 Performance Requirements:

In the performance of this contract, the contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

- 2.2.1.1. All work involving FTI will be done under the supervision of the Contractor or the Contractor's employees.

- 2.2.1.2. The contractor and the contractor's employees with access to or who use FTI must meet the background check requirements defined in IRS Publication 1075.
- 2.2.1.3. Any federal tax return or return information made available in any format shall be used only for the purposes of performing this contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this contract. Disclosure to anyone other than an officer or employee of the Contractor is prohibited.
- 2.2.1.4. All federal tax returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material.
- 2.2.1.5. The Contractor certifies that the IRS data processed during the performance of this contract will be completely purged from all data storage components of its computer facility, and no output will be retained by the Contractor after the work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosure.
- 2.2.1.6. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the State or its designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts and will provide the State or its designee with a Statement containing the date of destruction, description of material destroyed, and the method used.
- 2.2.1.7. All computer systems receiving, processing, storing or transmitting FTI must meet the requirements defined in the IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operations, and technical IRS 1075 controls. All security features must be available and activated to protect against unauthorized use of and access to Federal Tax Information.
- 2.2.1.8 No work involving Federal Tax Information furnished under this contract will be subcontracted without prior written approval of the IRS.
- 2.2.1.9. The Contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

The agency will have the right to void the Contract if Contractor fails to provide the safeguards described above.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

--

2.2.2. IRS 1075 Criminal/Civil Sanctions

- 2.2.2.1. Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as 5 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRCs 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1.
- 2.2.2.2. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of the contract. Inspection by or disclosure to anyone without an official need-to-know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as 1 year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of the officer or employee (United States for Federal employees) in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC 7213A and 7431.
- 2.2.2.3. Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to Contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a Contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

2.2.3. Inspection

The IRS and the Agency, with 24 hour notice, shall have the right to send its inspectors into the offices and plants of the Contractor for inspection of the facilities and operations performing any work under this contract for compliance with requirements defined in IRS Publication 1075. The IRS' right of inspection shall include the use of manual, and/or automated scanning tools to perform compliance and vulnerability assessment of information technology (IT) assets that access, store, process or transmit FTI. On the basis of such inspection, corrective actions may be required in cases where the Contractor is found to be noncompliant with contract safeguards.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

2.3. Disclosure

Disclosure to Third Parties. This Contract must not be deemed to prohibit disclosures in the following cases:

2.3.1. Required by applicable law, regulation, court order or subpoena; provided that, if the Contractor or any of its representatives are ordered or requested to disclose any information provided by the State, whether Sensitive Data or otherwise, pursuant to court or administrative order, subpoena, summons, or other legal process or otherwise believes that disclosure is required by any law, ordinance, rule or regulation, Contractor must notify the State within 24 hours in order that the State may have the opportunity to seek a protective order or take other appropriate action. Contractor must also cooperate in the State's efforts to obtain a protective order or other reasonable assurance that confidential treatment will be accorded the information provided by the State. If, in the absence of a protective order, Contractor is compelled as a matter of law to disclose the information provided by the State, Contractor may disclose to the party compelling disclosure only the part of such information as is required by law to be disclosed (in which case, prior to such disclosure, Contractor must advise and consult with the State and its counsel as to the scope of such disclosure and the nature of wording of such disclosure) and Contractor must use commercially reasonable efforts to obtain confidential treatment for the information:

2.3.1.1. To State auditors or regulators.

2.3.1.2. To service providers and agents of either party as permitted by law, provided that such service providers and agents are subject to binding confidentiality obligations.

2.3.1.3. To the professional advisors of either party, provided that such advisors are obligated to maintain the confidentiality of the information they receive.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

2.4. Background Investigations of Contractor Personnel

Contractor agrees that (1) the State of Ohio will conduct background investigations on Contractor personnel who will perform Sensitive Services (as defined below), and (2) no ineligible personnel will perform Sensitive Services under this contract. The term “ineligible personnel” means any person who (a) has been convicted at any time of any criminal offense involving dishonesty, a breach of trust, money laundering, or who has entered into a pre-trial diversion or similar program in connection with a prosecution for such offense, (b) is named by the Office of Foreign Asset Control (OFAC) as a Specially Designated National, or (c) has been convicted of a felony.

“Sensitive Services” means those services that (i) require access to customer, consumer, or State employee information, (ii) relate to the State’s computer networks, information systems, databases or secure facilities under circumstances that would permit modifications to such systems, or (iii) involve unsupervised access to secure facilities.

Contractors who will have access to Federal Tax Information (FTI) or Criminal Justice Information (CJI) must complete a background investigation that is favorably adjudicated, prior to being permitted to access the information. In addition, existing Contractors with access to FTI or CJI that have not completed a background investigation within the last 5 years must complete a background investigation that is favorably adjudicated, prior to being permitted to access the information.

FTI or criminal justice background investigations will include:

- 2.4.1. FBI Fingerprinting (FD-258)
- 2.4.2. Local law enforcement agencies where the employee has lived, worked and/or attended school within the last five years
- 2.4.3. Citizenship/residency eligibility to legally work in the United States
- 2.4.4. New employees must complete USCIS Form I-9, which must be processed through the Federal E-Verify system
- 2.4.5. FTI training, with a 45 day wait period

In the event that the Contractor does not comply with the terms of this section, the State may, in its sole and absolute discretion, terminate this Contract immediately without further liability.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

3. Contractor Responsibilities Related to Reporting of Concerns, Issues, and Security/Privacy Issues

3.1. General

If, over the course of the Contract a security or privacy issue arises, whether detected by the State, a State auditor, or the Contractor, that was not existing within an in-scope environment or service prior to the commencement of any contracted service associated with this Contract, the Contractor must:

- 3.1.1. Notify the State of the issue or acknowledge receipt of the issue within two (2) hours.
- 3.1.2. Within forty-eight (48) hours from the initial detection or communication of the issue from the State, present a potential exposure or issue assessment document to the State account representative and the State Chief Information Security Officer with a high-level assessment as to resolution actions and a plan.
- 3.1.3. Within four (4) calendar days, and upon direction from the State, implement, to the extent commercially reasonable, measures to minimize the State's exposure to the security or privacy issue until such time as the issue is resolved.
- 3.1.4. Upon approval from the State, implement a permanent repair to the identified issue at the Contractor's cost.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

3.2. Actual or Attempted Access or Disclosure

If the Contractor determines that there is any actual, attempted or suspected theft of, accidental disclosure of, loss of, or inability to account for any Sensitive Data by the Contractor or any of its Subcontractors (collectively "Disclosure") and/or any unauthorized intrusions into Contractor's or any of its Subcontractor's facilities or secure systems (collectively "Intrusion"), Contractor must immediately:

- 3.2.1. Notify the State within two (2) hours of the Contractor becoming aware of the unauthorized disclosure or intrusion.
- 3.2.2. Investigate and determine if an intrusion and/or disclosure has occurred.
- 3.2.3. Fully cooperate with the State in estimating the effect of the disclosure or intrusion and fully cooperate to mitigate the consequences of the disclosure or intrusion.
- 3.2.4. Specify corrective action to be taken.
- 3.2.5. Take corrective action to prevent further disclosure and/or intrusion.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

--

3.3. Unapproved Disclosures and Intrusions: Contractor Responsibilities

The following are the responsibility of the Contractor to provide at its own cost:

- 3.3.1. The Contractor must, as soon as is practical, make a report to the State including details of the disclosure and/or intrusion and the corrective action the Contractor has taken to prevent further disclosure and/or intrusion. The Contractor must, in the case of a disclosure, cooperate fully with the State to notify the affected persons as to the facts and circumstances of the disclosure of the Sensitive Data. Additionally, the Contractor must cooperate fully with all government regulatory agencies and/or law enforcement agencies that have jurisdiction to investigate a disclosure and/or any known or suspected criminal activity.
- 3.3.2. If, over the course of delivering services to the State under this statement of work for in-scope environments, the Contractor becomes aware of an issue, or a potential issue that was not detected by security and privacy teams, the Contractor must notify the State within two (2) hours. This notification must not minimize the more stringent service level contracts pertaining to security scans and breaches contained herein, which due to the nature of an active breach must take precedence over this notification. The State may elect to work with the Contractor under mutually agreeable terms for those specific resolution services at that time or elect to address the issue independent of the Contractor.
- 3.3.3. If the Contractor identifies a potential issue with maintaining an “as provided” State infrastructure element in accordance with a more stringent State level security policy, the Contractor must identify and communicate the nature of the issue to the State, and, if possible, outline potential remedies.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

--

3.4. Security Incident Reporting and Indemnification Requirements

- 3.4.1. The Contractor must report any security incident of which it becomes aware. For the purposes of this document, "Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. It does not mean unsuccessful log-on attempts, denial of service attacks, unsuccessful network attacks such as pings, probes of firewalls, port scans, or any combination of those, as long as there is no unauthorized access, acquisition, use, or disclosure of Sensitive Data as a result.
- 3.4.2. In the case of an actual security incident that may have compromised Sensitive Data, the Contractor must notify the State in writing within two (2) hours of the Contractor becoming aware of the breach. The Contractor is required to provide the best available information from the investigation.
- 3.4.3. In the case of a suspected incident, the Contractor must notify the State in writing within twenty-four (24) hours of the Contractor becoming aware of the suspected incident. The Contractor is required to provide the best available information from the investigation.
- 3.4.4. The Contractor must fully cooperate with the State to mitigate the consequences of an incident/suspected incident at the Contractor's own Cost. This includes any use or disclosure of the Sensitive Data that is inconsistent with the terms of this Contract and of which the Contractor becomes aware, including but not limited to, any discovery of a use or disclosure that is not consistent with this contract by an employee, agent, or Subcontractor of the Contractor.
- 3.4.5. The Contractor must give the State full access to the details of the breach/suspected breach and assist the State in making any notifications to potentially affected people and organizations that the State deems are necessary or appropriate at the Contractor's own cost.
- 3.4.6. The Contractor must document and provide incident reports for all such incidents/suspected incidents to the State. The Contractor must provide updates to incident reports until the investigation is complete at the Contractor's own cost. At a minimum, the incident/suspected incident reports will include:
 - 3.4.6.1. Data elements involved, the extent of the Data involved in the incident, and the identification of affected individuals, if applicable.
 - 3.4.6.2. A description of the unauthorized persons known or reasonably believed to have improperly used or disclosed State Data, or to have been responsible for the incident.
 - 3.4.6.3. A description of where the State Data is believed to have been improperly transmitted, sent, or utilized, if applicable.
 - 3.4.6.4. A description of the probable causes of the incident.
 - 3.4.6.5. A description of the proposed plan for preventing similar future incidents, including ongoing risk remediation plan approval.
 - 3.4.6.6. Whether the Contractor believes any federal or state laws requiring notifications to individuals are triggered.
- 3.4.7. In addition to any other liability under this contract related to the Contractor's improper disclosure of State Data, and regardless of any limitation on liability of any kind in this Contract, the Contractor will be responsible for acquiring one year's identity theft protection service on behalf of any individual or entity

whose Sensitive Data is compromised while it is in the Contractor's possession. This service will be provided at Contractor's own cost. Such identity theft protection must provide coverage from all three major credit reporting agencies and provide immediate notice through phone or email of attempts to access the individual's credit history through those services.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

4. Security Review Services

As part of a regular Security Review process, the Contractor will include the following reporting and services to the State:

4.1. Hardware and Software Assets

The Contractor will support the State in defining and producing specific reports for both hardware and software assets. At a minimum this includes:

- 4.1.1. Deviations from the hardware baseline.
- 4.1.2. Inventory of information types by hardware device.
- 4.1.3. Software inventory compared against licenses (State purchased).
- 4.1.4. Software versions and then scans of versions against patches distributed and applied.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

4.2. Security Standards by Device and Access Type

The Contractor must:

4.2.1. Document security standards by device type and execute regular scans against these standards to produce exception reports.

4.2.2. Document and implement a process for any required remediation.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

4.3. Boundary Defenses

The Contractor must:

4.3.1. Work with the State to support the denial of communications to/from known malicious IP addresses.

4.3.2. Ensure that the system network architecture separates internal systems from DMZ and extranet systems.

4.3.3. Require the use of two-factor authentication for remote login.

4.3.4. Support the State's monitoring and management of devices remotely logging into the internal network.

4.3.5. Support the State in the configuration of firewall session tracking mechanisms for addresses that access the solution.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

4.4. Audit Log Reviews

The Contractor must:

4.4.1. Work with the State to review and validate audit log settings for hardware and software.

- 4.4.2. Ensure that all systems and environments have adequate space to store logs.
- 4.4.3. Work with the State to devise and implement profiles of common events from given systems to reduce false positives and rapidly identify active access.
- 4.4.4. Provide requirements to the State to configure operating systems to log access control events.
- 4.4.5. Design and execute bi-weekly reports to identify anomalies in system logs.
- 4.4.6. Ensure logs are written to write-only devices for all servers or a dedicated server managed by another group.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

4.5. Application Software Security

The Contractor must:

- 4.5.1. Perform configuration review of operating system, application, and database settings.
- 4.5.2. Ensure software development personnel receive training in writing secure code.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A – Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

4.6. System Administrator Access

The Contractor must:

- 4.6.1. Inventory all administrative passwords (application, database, and operating system level).

- 4.6.2. Implement policies to change default passwords in accordance with State policies, following any transfer or termination of personnel (State, existing Materials and Supplies Vendor, or Contractor).
- 4.6.3. Configure administrative accounts to require regular password changes.
- 4.6.4. Ensure user and service level accounts have cryptographically strong passwords.
- 4.6.5. Store passwords in a hashed or encrypted format.
- 4.6.6. Ensure administrative accounts are used only for administrative activities.
- 4.6.7. Implement focused auditing of administrative privileged functions.
- 4.6.8. Configure systems to log entry and alert when administrative accounts are modified.
- 4.6.9. Segregate administrator accounts based on defined roles.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

--

4.7. Account Access Privileges

The Contractor must, in alignment with policy requirements:

- 4.7.1. Review and disable accounts not associated with a business process.
- 4.7.2. Create a daily report that includes locked out accounts, disabled accounts, etc.
- 4.7.3. Implement a process for revoking system access.
- 4.7.4. Automatically log off users after a standard period of inactivity.
- 4.7.5. Monitor account usage to determine dormant accounts.
- 4.7.6. Monitor access attempts to deactivated accounts through audit logging.
- 4.7.7. Profile typical account usage and implement or maintain profiles to ensure that security profiles are implemented correctly and consistently.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

--

4.8. Additional Controls and Responsibilities

The Contractor must meet with the State no less frequently than annually to:

- 4.8.1. Review, update and conduct security training for personnel, based on roles.
- 4.8.2. Review the adequacy of physical and environmental controls.
- 4.8.3. Verify the encryption of Sensitive Data in transit.
- 4.8.4. Review access controls based on established roles and access profiles.
- 4.8.5. Update and review system administration documentation.
- 4.8.6. Update and review system maintenance policies.
- 4.8.7. Update and review system and integrity policies.
- 4.8.9. Review and implement updates to the System security plan.

4.8.10 Update risk assessment policies and procedures.

4.8.11 Update and implement incident response procedures.

Please explain how these requirements will be met within the context of the proposed solution (e.g., Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), On-Premises or Hybrid). If this section, or portions of this section, are not applicable, please explain and note as N/A. Please note that any proposed compensating controls and/or requirement modifications must be noted in Appendix A - Compensating Controls to Security and Privacy Requirements. The language within the supplement will not be modified.

--

Appendix A – Compensating Controls to Security and Privacy Supplement

In the event that there is a security or privacy requirement outlined in this supplement that needs to be met by a compensating control, please identify it below and provide a proposed language change as well as a rationale for the change.

Reference	Current Language	Contractor's Proposed Change	Rationale of Proposed Change
Example: Supplement 2 - Page 11	Example: Provide vulnerability management services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. As a minimum, the Contractor must provide vulnerability scan results to the State monthly .	Example: Provide vulnerability management services for the Contractor's internal secure network connection, including supporting remediation for identified vulnerabilities as agreed. As a minimum, the Contractor must provide vulnerability scan results to the State weekly .	Per company policy vulnerability report are only provided to customers on a quarterly basis.