STATE OF NORTH CAROLINA Department of Revenue	**REQUEST FOR PROPOSAL NO. RFP 45-RQ161211**
	Contract Name: Tax System Modernization
	Bid Opening Date: May 16, 2025
Refer ALL inquiries regarding this RFP to: Name: Christopher Drew, Department of Revenue (NCDOR) Director of Procurement & Contracts Email: Christopher.Drew@ncdor.gov	Issue Date: March 5, 2025
	Commodity Code: 93161703
	Purchasing Agency: Department of Revenue
	Requisition No.: RQ161211

OFFER

The Purchasing Agency solicits offers for Services and/or goods described in this solicitation. All offers and responses received shall be treated as Offers to contract as defined in 9 NCAC 06A.0102(12).

EXECUTION

In compliance with this Request for Proposal ("RFP"), and subject to all the conditions herein, the undersigned offers and agrees to furnish any or all Services or goods upon which prices are offered, at the price(s) offered herein, within the time specified herein.

Failure to execute/sign offer prior to submittal shall render offer invalid. Late offers are not acceptable.

OFFEROR			
STREET ADDRESS:		P.O. BOX:	ZIP:
CITY, STATE & ZIP:		TELEPHONE NUMBER:	TOLL FREE TEL. NO
NAME & TITLE OF PERSON SIGNING:		FAX NUMBER:	
AUTHORIZED SIGNATURE:	DATE:	E-MAIL:	

Offer valid for one hundred eighty (180) days from date of offer opening unless otherwise stated here: ____ days

ACCEPTANCE OF OFFER

If any or all parts of this offer are accepted, an authorized representative of Department of Revenue shall affix its signature hereto and any subsequent Request for Best and Final Offer, if issued. Acceptance shall create a contract having an order of precedence as follows: Best and Final Offers, if any, Special terms and conditions specific to this RFP, Specifications of the RFP, the Department of Information Technology Terms and Conditions, and the agreed portion of the awarded Vendor's Offer. A copy of this acceptance will be forwarded to the awarded Vendor(s).

FOR PURCHASING AGENCY USE ONLY

Offer accepted and contract awarded this date, , as indicated on attached certification,

by (Authorized representative of the NC Department of Revenue).

Table of Contents

1.0 AnTicipated Procurement Schedule....4
2.0 Purpose of RFP....4
2.1 Introduction....4
2.2 Agency Background....4
2.3 Summary of Problem Statement....8
2.4 Program Governance....8
2.5 Contract Term....10
2.6 Effective Date....10
2.7 Contract Type....10
3.0 RFP Requirements and Specifications....10
3.1 General Requirements and Specifications....10
3.2 Security Specifications....12
3.3 Enterprise Specifications....12
3.4 Business and Technical Specifications....13
3.5 Oral Presentation and Product Demonstration....33
3.6 Value Added Services....34
4.0 Cost of Vendor's Offer....34
4.1 Offer Costs....34
4.2 Payment Schedule....34
5.0 Evaluation....34
5.1 Source Selection....34
5.2 Evaluation Criteria....35
5.3 Best and Final Offers ("BAFO")....35
5.4 Possession and Review....35
6.0 Vendor Information and Instructions....36
6.1 General Conditions of Offer....36
6.2 General Instructions for Vendor....37
6.3 Instructions for Offer Submission....40
7.0 Other Requirements and Special Terms....42
7.1 Vendor Utilization Of Workers Outside of U.S....42
7.2 Financial Statements....42
7.3 Financial Resources Assessment, Quality Assurance, Performance and Reliability....42
7.4 Vendor's License or Support Agreements....43
7.5 Resellers....43
7.6 Disclosure of litigation....43
7.7 Criminal Conviction....44
7.8 Security and Background Checks....44
7.9 Assurances....44
7.10 Confidentiality of Offers....45
7.11 Project Management....45
7.12 Meetings....45
7.13 Recycling and Source Reduction....45

7.14 Special Terms and Conditions 46
7.15 Agency Terms and Conditions 46
8.0 List of Attachments & Exhibits 48
Attachment A: Definitions 50
Attachment B: Department of Information Technology Terms and Conditions 52
Attachment C: Description of Vendor 68
Attachment D: Cost Form 70
Attachment E: Vendor Certification Form 71
Attachment F: Location of Workers Utilized by Vendor 72
Attachment G: References 73
Attachment H: Financial Review Form 74
Attachment I: Functional Specifications Matrix 76
Attachment J: Technical Specifications Matrix 76
Attachment K: Key Personnel and Resumes 77
Attachment L: Staffing Plan 89
Attachment M: Tax Schedule Matrix 89
Attachment N: Forms Inventory 89
Attachment O: Systems Inventory 89
Attachment P: Interfaces Inventory 89
Attachment Q: Implementation Roles & Responsibilities 89
Attachment R: NCDOR IT Certification and Accreditation Policy 90
Attachment S: NCDOR Certification and Accreditation Process 92
Attachment T: Internal Revenue Service Publication 1075, Exhibit 7 Safeguarding Contract Language 105
Attachment U: Security Requirements for Vendor Staff and Contractors 109
Attachment V: NC Statutory References 111
Attachment W: Vendor Experience 112

1.0 ANTICIPATED PROCUREMENT SCHEDULE

The Agency will make every effort to adhere to the following schedule.

Table 1. Anticipated Procurement Schedule

Action	Responsibility	Date
RFP Issued	Agency	03/05/2025
Written Questions Deadline	Potential Vendors	03/28/2025 3 PM EST
Agency's Response to Written Questions/ RFP Addendum Issued	Agency	04/11/2025
Offer Opening Deadline	Vendor(s)	05/16/2025 3 PM EST
Oral Presentations and/or Product Demonstrations by Finalist(s)	Selected Vendor(s)	06/13/2025
Offer Evaluation	Agency	07/18/2025
Negotiations with Finalists	Agency designees and selected Vendor(s)	08/29/2025
Best and Final Offers Deadline from Finalists	Selected Vendors	9/05/2025
Contract Award	Agency	10/03/2025
Protest Deadline	Responding Vendors	15 days after award

2.0 PURPOSE OF RFP

2.1 INTRODUCTION

The purpose of this RFP is to solicit Offers for a modern Commercial-Off-the-Shelf ("COTS") integrated tax system ("ITS") and implementation services for the North Carolina Department of Revenue ("the Agency," "State", or "NCDOR").

The Agency is seeking from qualified Vendors the information necessary to select a partner to replace its aging Integrated Tax Administration System ("ITAS") and ancillary tax processing systems with a modern, secure ITS that meets the Agency's tax administration needs and requirements with minimal customization. The Agency is looking for an ITS that is customer centric, meets the diverse needs of various agency constituencies, is scalable, continuously upgraded, and adheres to the latest security protocols. The Agency seeks to partner with a Vendor that has demonstrated experience in supporting the modernization of an organization of similar size and complexity. The Agency prefers the proposed tax solution be implemented by the owner of the product rather than a third-party system integrator.

2.2 AGENCY BACKGROUND

The North Carolina Department of Revenue is a cabinet-level executive agency charged with administering tax laws and collecting taxes due to the State. The Secretary of Revenue is appointed by the Governor. The Agency's mission is to fund public services benefiting the people of North Carolina by administering the tax laws and collecting the taxes due in an impartial, consistent, secure, and efficient manner.

2.2.1 Current Business Landscape

The Agency developed a Business Capability Model ("BCM") to provide a high-level functional overview of its operations. The BCM captures current state functional capabilities by dividing the Agency's activities into eight (8) major capabilities which cover the building blocks of tax administration in North Carolina. It is expected that the proposed ITS will support these business capabilities, associated processes, requirements, and functionalities (see Attachment I – Functional Specifications Matrix).

The eight (8) major capabilities are defined below:

a) Process Registrations, Returns, and Payments – The ability to create taxpayer accounts and receive, process, and validate tax returns and payments.

b) Manage Taxpayer Relationships – The ability to maintain taxpayer information, provide taxpayer assistance, and manage taxpayer correspondence, as well as support online taxpayer self-service capabilities.

c) Conduct Investigations and Audits – The ability to support case management of tax audits, select accounts for audit, manage audit programs and results, and execute fraud programs.

d) Manage Collections – The ability to score, track, and enforce payment from delinquent and underpaid taxpayers, as well as manage accounts in bankruptcy and debt setoffs.

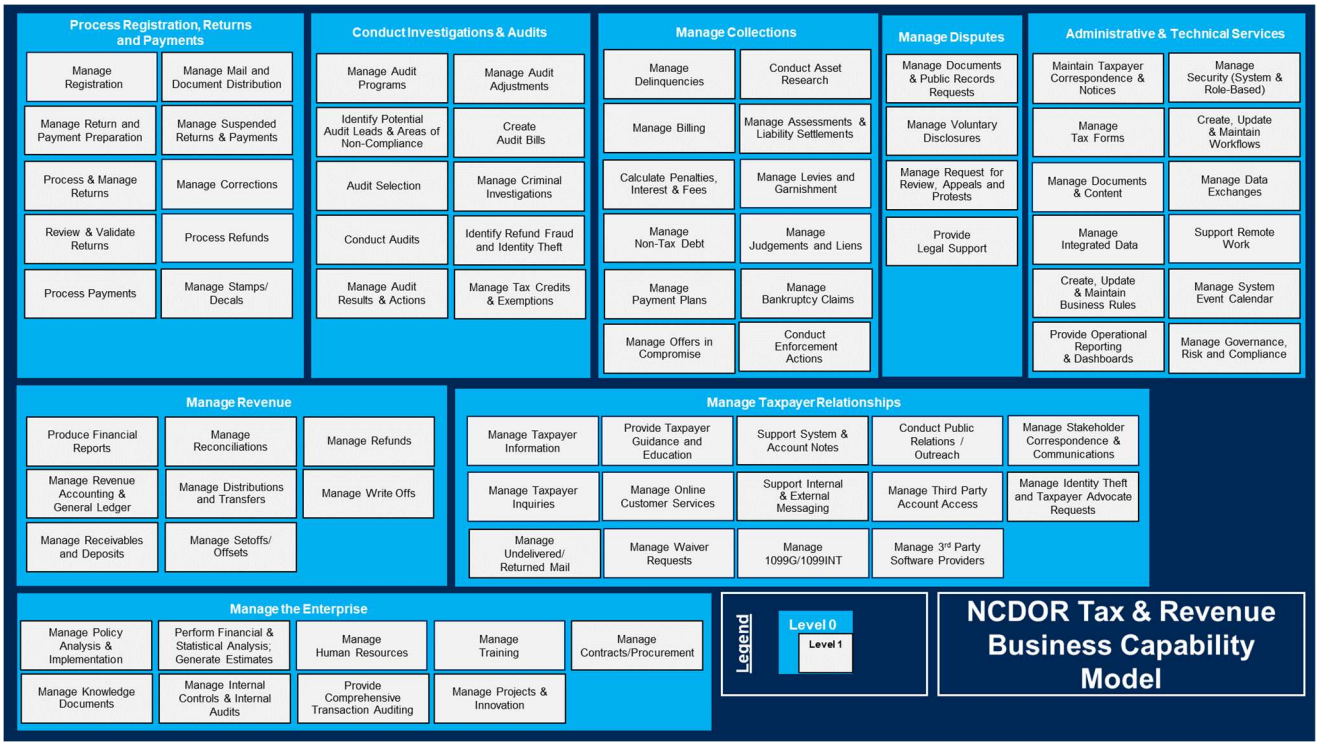
e) Manage Disputes – The ability to manage requests for review and protests, issue private letter rulings, comply with public records requests and process voluntary disclosures.

f) Manage Revenue – The ability to manage revenue accounting, produce financial reports, distribute funds, and post summary financial transactions to the State's general ledger.

g) Administrative & Technical Services – The ability to provide technical support for business capabilities, manage documents, maintain workflows and business rules, provide operational reporting and data analytics, and meet compliance requirements.

h) Manage the Enterprise – The ability to support human resource processes, train staff, buy goods and services, manage projects and innovation, conduct policy analysis, and maintain internal controls.

Figure 1. NCDOR Business Capability Model



2.2.2 Principal Business Activity

The principal sources of revenue for North Carolina State government are through taxes administered and collected by the Agency. ITAS houses the majority of the taxes collected by the Agency including Individual Income and Sales & Use taxes, which make up over 85% of net general fund collections. For fiscal year ending 2023, the Agency processed over $44 billion in gross collections. The Department of Revenue Certified Budget for FY2022-2023 was $179.6 million.

Table 2. Business Activity Statistics - Fiscal Year 2022-2023

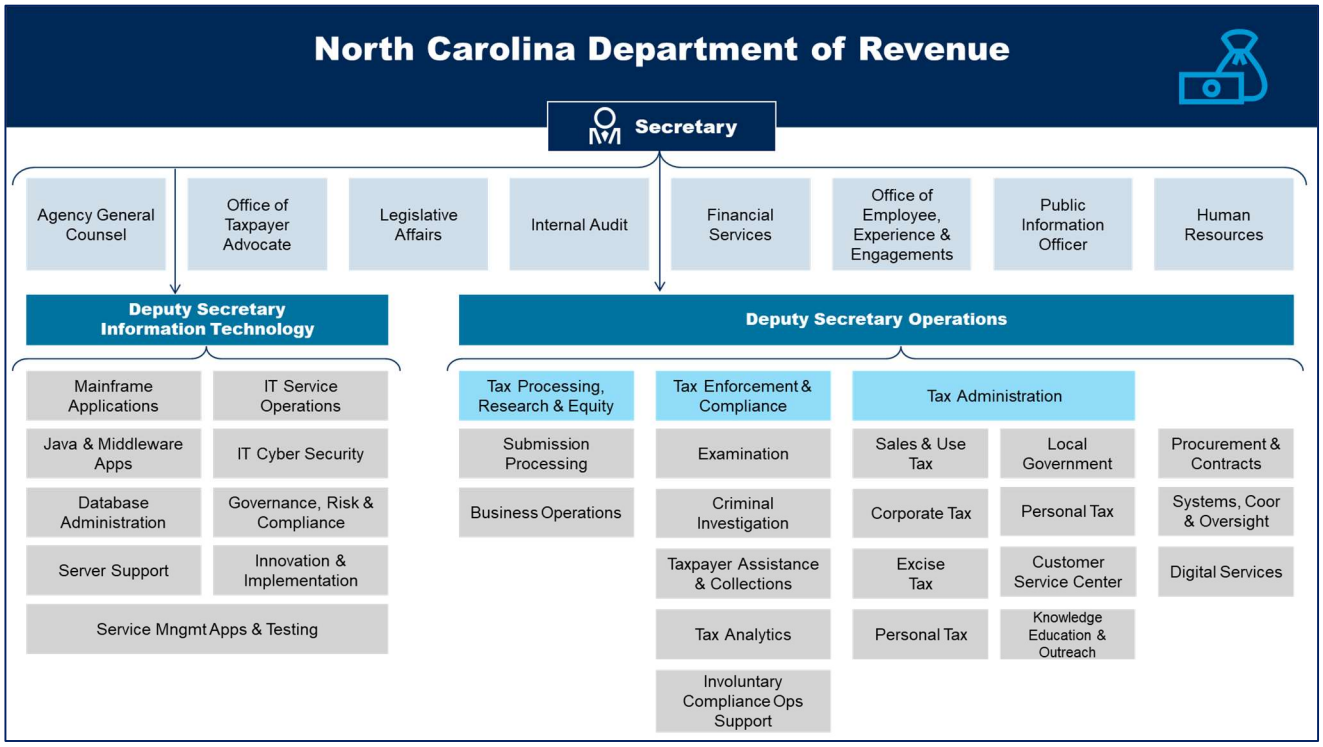
Activity	Volume
Gross Collections	$44.6 billion
Average Daily Deposit	$178.5 million
Pieces of Mail (Incoming)	2,789,629
Pieces of Mail (Outgoing)	4,752,256
Tax Returns Processed	12,525,216
Tax Payments Processed	9,516,295
Refunds Issued (all tax schedules)	3,086,698 with a value of $3.0 billion
Refunds Issued (Individual Income)	3,010,256 with a value of $1.9 billion
Refunds (Individual Income) Direct Deposited	2,313,252 with a value of $1.2 billion
Individual Income Returns Filed Electronically	5,066,429
Non-Individual Income Returns Filed Electronically	6,032,680

Returns Filed by Paper Return (All Tax Schedules)	1,426,107
Gross Electronic Funds Transfer (EFT) Collections	$38.8 billion
Distributions/Transfers to Local Governments/State Agencies	$5.5 billion

2.2.3 Organization & Staffing

The Agency staff consists of approximately 1,450 permanent positions, 100 seasonal positions, and 125 non-seasonal temporaries. In addition, there are various contractors working directly for the Agency or working for vendors that provide services to the Agency. Over 90% of staff access one or more of the legacy systems and applications included in the scope of this RFP. The Agency workforce consists of employees working in other states and throughout North Carolina. Currently, 90% of the staff are either full or part time teleworkers.

Figure 2. North Carolina Department of Revenue Organizational Chart



2.2.4 Current Technical Landscape

ITAS, the Agency's core tax administration system, has been operational since October 1994. While this 30-year-old legacy tax system functions as it was originally designed, its use of the COBOL language with a DB2 database on the mainframe makes it an unsuitable and restrictive platform for the type of transformational change the Agency intends to implement.

In addition, in 2010 the Agency initiated an effort to implement a new integrated tax system using a product called Public Sector Revenue Management ("PSRM"). Limited tax types were implemented on

this system. The intent is to also replace the PSRM system and consolidate tax processing into one tax administration system.

2.2.5 Overview of Key Systems

In addition to ITAS and PSRM, there are various other systems and applications that support tax administration and processing, some of which are integrated and some stand alone. A number of Access databases have also been created over the years to meet business needs not provided by the tax systems. It is anticipated that functionality provided by the Access databases will be provided by the new tax system and the databases can be retired. See Attachment O: Systems Inventory for more information on systems and applications and Attachment M: Tax Schedule Matrix for tax schedule information.

2.3 SUMMARY OF PROBLEM STATEMENT

The Agency's core tax administration systems are nearing the end of useful life and newer, more robust technologies are available to significantly improve the Agency's ability to meet its objectives and support the expansion of electronic and taxpayer self-services.

It is increasingly difficult for the Agency to provide efficient customer service, implement mandated legislative requirements, and make significant system improvements due to weaknesses in the aging systems and the challenges of maintaining multiple applications that have been separately developed over the last 25+ years. Maintaining multiple applications, along with the interfaces that connect them and the supporting infrastructure, requires significant technical and testing resources and hinders operations and innovation. Any failure in existing systems could lead to a significant business disruption with a potential loss of revenue for the State.

2.4 PROGRAM GOVERNANCE

The Agency will establish a Tax System Modernization Program Management Group and Governance structure to ensure the success of the Tax System Modernization Program ("Program"). The Agency Program Governance Structure below (Figure 3) shows the anticipated Governance Structure to facilitate decision-making throughout the duration of the Program. The final Governance Structure will be established prior to Program kick-off. The Vendor is expected to adapt to the Agency's approach to Governance and work closely with the Agency Program Executive Director and Program Leaders as well as the Executive Steering Committee and the Implementation Steering Committee.

The Program Management Group is led by the Agency Program Executive Director. The roles and objectives of the Agency Program Management Group are to:

a) Ensure consistency and standardization of processes, measurement, and communication across all aspects of the Program

b) Increase interaction of people, processes, and tools for effective collaboration, communication, accountability, and control

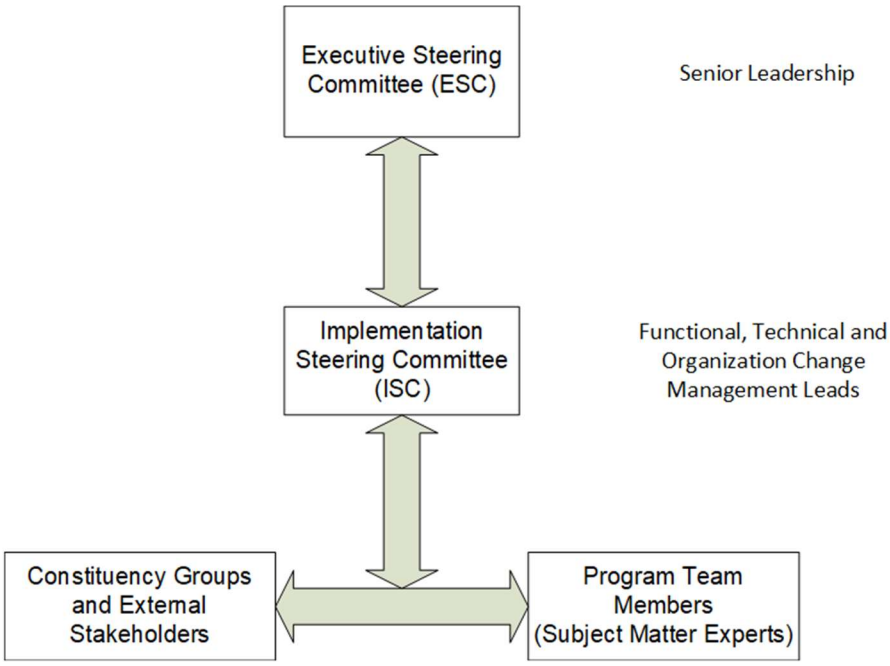
c) Serve as the communication channel between governance committees such as the Executive Steering Committee, the Implementation Steering Committee, and other constituency groups

d) Ensure comprehensive organizational change management

e) Resolve differences in approach, positions, opinions, and interpretations that can occur in the Program

f) Manage technical and business scope change across the project and program areas within the Tax System Modernization Program

Figure 3. Agency Program Governance Structure



2.4.1 Executive Steering Committee

The Executive Steering Committee ("ESC") will provide high-level oversight and act as a decision-making escalation point for the Program. The ESC is comprised of members from the Agency's executive tiers along with the Agency Program Executive Director.

The mission of the ESC is to:

a) Measure and monitor program activities to ensure alignment with program goals

b) Approve implementation plans and associated performance indicators

c) Serve as the escalation point for decisions, risks, and issue mitigation

d) Evaluate and approve change requests over a certain cost threshold and impact

e) Ensure accountability of all program areas

2.4.2 Implementation Steering Committee

The Implementation Steering Committee ("ISC") will provide guidance and subject matter expertise throughout the duration of the program. The ISC will be responsible for ensuring all deliverables meet the Agency's functional and technical needs.

The role and objectives of the ISC are to:

a) Ensure the System meets the needs of the Agency

b) Enforce integration of people, process, and tools for effective collaboration, communication, accountability, and control

c) Participate in organizational change management

d) Manage ongoing risks, action items, issues, decisions, and dependencies

e) Manage integration activities to ensure that current systems and functionality being retired are successfully decoupled, and the System is operational and tested before go-live

f) Resolve differences in approach, positions, opinions, and interpretations between the Agency and the Vendor

g) Maintain consistency and standards across all work streams and associated programs

2.4.3 Third-Party Independent Program Oversight

The Agency intends to have an independent third-party provide oversight services (Independent Verification and Validation ("IV&V")), including deliverable reviews, quality assurance ("QA"), and regular reporting on progress during the lifecycle of the Program. The Vendor will be expected to support IV&V reviews and have ongoing and recurring interactions with the third-party independent oversight service provider for the Program, throughout its duration, with Agency collaboration.

2.5 CONTRACT TERM

A contract awarded pursuant to this RFP shall have an effective date as provided in the Notice of Award. The base term shall be for an up to six (6) year period that includes the Implementation timeline and Maintenance, Support, and Upgrades following full implementation, and will expire upon the anniversary date of the effective date unless otherwise stated in the Notice of Award, or unless terminated earlier. The State retains the option to extend the Agreement for three (3) additional five (5)-year renewal options at its sole discretion.

2.6 EFFECTIVE DATE

This solicitation, including any Exhibits, or any resulting contract or amendment shall not become effective nor bind the State until the appropriate State purchasing authority/official, or Agency official has signed the document(s), contract or amendment; the effective award date has been completed on the document(s), by the State purchasing official, and that date has arrived or passed. The State shall not be responsible for reimbursing the Vendor for goods provided nor Services rendered prior to the appropriate signatures and the arrival of the effective date of the Agreement. No contract shall be binding on the State until an encumbrance of funds has been made for payment of the sums due under the Agreement.

2.7 CONTRACT TYPE

Definite Quantity Contract - This request is for a close-ended contract between the awarded Vendor and the State to furnish a pre-determined quantity of a good or service during a specified period of time.

The State reserves the right to make partial, progressive, or multiple awards where it is advantageous to award separately by items; where more than one supplier is needed to provide the contemplated specifications as to quantity, quality, delivery, service, geographical areas; or where other factors are deemed to be necessary or proper to the purchase in question.

3.0 RFP REQUIREMENTS AND SPECIFICATIONS

3.1 GENERAL REQUIREMENTS AND SPECIFICATIONS

3.1.1 REQUIREMENTS

Requirement means, as used herein, a function, feature, or performance that the System must provide. If the offer cannot meet the requirements, the offer will not be evaluated.

3.1.2 SPECIFICATIONS

Specification means, as used herein, a detailed description that documents the function and performance of a system or system component.

The apparent silence of the specifications as to any detail, or the apparent omission of detailed description concerning any point, shall be regarded as meaning that only the best commercial practice is to prevail and that only processes, configurations, materials and workmanship of the first quality may be used. Upon any notice of noncompliance provided by the State, Vendor shall supply proof of compliance with the specifications. Vendor must provide written notice of its intent to deliver alternate or substitute Services, products, goods or other Deliverables. Alternate or substitute Services, products, goods or Deliverables may be accepted or rejected in the sole discretion of the State; and any such alternates or substitutes must be accompanied by Vendor's certification and evidence satisfactory to the State that the function, characteristics, performance and endurance will be equal or superior to the original Deliverables specified.

3.1.3 SITE AND SYSTEM PREPARATION

Vendors shall provide to the Purchasing State Agency complete site requirement specifications for the Deliverables, if any. These specifications shall ensure that the Deliverables to be installed or implemented shall operate properly and efficiently within the site and system environment. Any alterations or modification in site preparation, which are directly attributable to incomplete or erroneous specifications provided by the Vendor, and which would involve additional expenses to the State, shall be made at the expense of the Vendor.

3.1.4 EQUIVALENT ITEMS

Whenever a material, article or piece of equipment is identified in the specification(s) by reference to a manufacturer or Vendor's name, trade name, catalog number or similar identifier, it is intended to establish a standard for determining substantial conformity during evaluation, unless otherwise specifically stated as a brand specific requirement (no substitute items will be allowed). Any material, article or piece of equipment of other manufacturers or Vendors shall perform to the standard of the item named. Equivalent offers must be accompanied by sufficient descriptive literature and/or specifications to provide for detailed comparison.

3.1.5 ENTERPRISE LICENSING

In offering the best value to the State, Vendors are encouraged to leverage the State's existing resources and license agreements, which can be viewed here:

https://it.nc.gov/resources/statewide-it-procurement/statewide-it-contracts

a) Identify components or products that are needed for your solution that may not be available with the State's existing license agreement.

b) Identify and explain any components that are missing from the State's existing license agreement.

c) If the Vendor can provide a more cost-effective licensing agreement, please explain in detail the agreement and how it would benefit the State.

3.1.6 ENTERPRISE, SERVICES, AND STANDARDS

Vendors should refer to the Vendor Resources Page for information on North Carolina Department of Information Technology regarding architecture, security, strategy, data, digital, identity and access management and other general information on doing business with state IT process.

The Vendor Resources Page can be found at the following link: https://it.nc.gov/vendor-engagement-resources. This site provides vendors with statewide information and links referenced throughout the RFP document. Agencies may request additional information.

3.2 SECURITY SPECIFICATIONS

A. SOLUTIONS HOSTED ON STATE INFRASTRUCTURE

The Agency Tax System Modernization Program will be required to receive and securely manage data that is classified as Federal Tax Information (FTI) as defined in the North Carolina Department of Revenue Security Policy Manual located at the following website: https://www.ncdor.gov/documents/files/ncdor-security-policy-manual/open.

To comply with the Internal Revenue Service (IRS) Publication 1075 safeguards requirements, the Agency is required to perform security and risk assessments on its information systems using IRS Publication 1075 controls at least annually.

3.2.1 SOLUTIONS NOT HOSTED ON STATE INFRASTRUCTURE

RESERVED

3.3 ENTERPRISE SPECIFICATIONS

3.3.1 ARCHITECTURE DIAGRAMS

Vendors are required to supply high level Network Architecture and Technology Stack diagrams as part of their proposal. The State utilizes architectural diagrams to better understand the design and technologies of a proposed solution. Details on these diagrams can be found at the following link:

https://it.nc.gov/resources/statewide-it-procurement/vendor-engagement-resources#Tab-Architecture-1192

The provision of these two diagrams is a requirement at offer submission. If they are not supplied at that time, the Vendor's offer will be considered non-responsive and will not be evaluated.

Vendor will be required to submit additional architectural diagrams using templates supplied by the Agency after contract award. This will be communicated to the Vendor by the Agency as needed during the Program.

3.3.2 SOLUTION ROADMAP

A Solution Roadmap defines the vision and strategic elements of the solution. The Solution Roadmap is a plan of action for how a Solution will evolve over time.

Describe the solution roadmap for your product.

a) The minimum content should include:

   i) Vision for the solution
   ii) High-level functionality expected for each solution release into production environment
   iii) High-level timeline
   iv) Description of how customer feedback is collected and incorporated into solution enhancements

b) In addition to the elements above, describe release strategies for functionality, roadmap for technical architecture, and how scalability of solution is planned.

c) The Agency prefers all proposed solution components and modules be developed and currently available. Describe any components or modules that are under development and not currently in production or available as part of the proposed solution.

3.3.3 IDENTITY AND ACCESS MANAGEMENT

The proposed solution must externalize identity and access management.

Describe how the proposed solution will meet IRS Publication 1075 (Rev. 11-2021) 4.1 Access Controls AC-1 through AC-23 to validate and secure all components of the application including the internal-facing ITS user interface and public-facing taxpayer portal.

3.3.4 ACCESSIBILITY

a) Describe how the proposed solution complies with industry and federal accessibility standards including the following standards:

   i) W3C Web Accessibility Initiative - Web Content Accessibility Guidelines (WCAG) 2.1: https://www.w3.org/TR/WCAG21/

   ii) Section 508: https://www.section508.gov/

   iii) Voluntary Product Accessibility Template (VPAT®): https://www.itic.org/policy/accessibility/vpat

b) Describe how the proposed solution is digitally accessible and compliant with the accessibility standards above, or, if not fully accessible, describe a proposed roadmap with a timeline for remediation for compliance by April 24, 2026.

3.4 BUSINESS AND TECHNICAL SPECIFICATIONS

3.4.1 CORPORATE PROFILE

3.4.1.1 Company Overview

a) Describe the Vendor's professional track record, including company history, organizational structure, number of employees, and number of years in business.

b) Describe any specific restructuring, mergers and/or downsizing within Vendor's organization that has occurred during the past three (3) years or is anticipated in the next three (3) years, noting potential impacts to the products and services proposed in response to this RFP, and any information relating to company bankruptcies or reorganizations due to financial hardship.

c) Describe any system implementation projects that have been delayed, stopped or cancelled, and whether any contract was terminated for convenience or cause as applicable.

3.4.1.2 Competitive Differentiators

Describe the attributes that distinguish the Vendor's organization as the best partner for NCDOR. Describe any special or unique characteristics of the organization which would make it especially qualified to perform the work required in this RFP.

3.4.1.3 Product Differentiators

Describe any features of the core solution that differentiate the proposed product and make it the best solution to meet NCDOR's business needs, including any features or capabilities that are not explicitly described in the specifications of this RFP.

3.4.2 EXPERIENCE

Describe the Vendor's relevant experience as the primary Contractor by completing Attachment W: Vendor Experience.

3.4.3 PROGRAM ORGANIZATION

3.4.3.1 Program Organizational Chart

Describe, preferably in chart form, the structure of Vendor's proposed implementation team including any subcontractors and the relationship between Vendor's Program team and the Agency's Program team. Describe the roles and responsibilities for each of the Vendor's and the Agency's Program team members, identifying each position title that corresponds to the position titles and job descriptions in Attachment L: Staffing Plan.

Any proposed organization and roles/responsibilities will be subject to Agency approval.

3.4.3.2 Key Personnel

Certain Program team members have been deemed 'Key Personnel'. For each member of the Vendor's proposed Program team that occupies a Key Personnel position, describe the person's background and experience by completing the Key Personnel Resume Template in Attachment K: Key Personnel Positions & Resumes.

3.4.3.3 Staffing Plan

Describe your proposed approach to staffing the implementation team in Attachment L: Staffing Plan, including:

a) Total number of staff assigned to the Program

b) Program team member roles

c) Staffing proposed for production support during the Program and post-implementation support once implementation is completed

3.4.4 QUALITY ASSURANCE

Describe the quality assurance processes to be utilized throughout the software development lifecycle and while implementing the Program.

3.4.5 IMPLEMENTATION SERVICES & APPROACH

The Modernization Program will move forward in phases from Initiation, through all phases of implementation to Production Support.

The Agency prefers to have the ITS solution implemented in five (5) releases by tax grouping as shown below in Table 4. Attachment M: Tax Schedule Matrix provides additional information.

Table 4. Anticipated Implementation Releases by Tax Grouping

Release 1	Release 2	Release 3	Release 4	Release 5
Tobacco Alcohol Installment Paper Sports Wagering Severance Conveyance Motor Carrier/IFTA	Individual Income Partnership Withholding Estates and Trusts	Sales, Use, and Taxes Administered like Sales & Use	Corporate & Franchise Insurance Privilege	Freight Car Lines Unauthorized Substance Motor Fuels Property Information Reporting Other

Describe an implementation plan based on your experience. It is acceptable if your plan differs from what is described above; however, the Agency seeks plans which cover all the functionality and in-scope taxes set forth in this RFP. Describe how your Cost Proposal aligns with your proposed implementation plan. Further information on the tax schedules referenced in Table 4 can be found in Attachment M: Tax Schedule Matrix.

After each major release, the Agency prefers a warranty period of twelve (12) months for monitoring and incident response support for the ITS system release. The Agency also prefers twelve (12) months of operations and maintenance support for the entire system after full implementation. See Section 3.4.7 - Production Support Services.

3.4.5.1 Implementation Approach & Project Management

Describe the proposed approach to plan, manage, and control the successful completion of all tasks and deliverables associated with the scope and specifications in the RFP, including:

a) A description of the implementation methodology to be used in executing the Modernization Program scope.

b) Project management processes to be used during the implementation.

c) The Vendor's recommended implementation phasing.

d) A list of key deliverables required for successful execution of the Program, including the criteria for deliverable approval.

e) A high-level schedule from the execution of the Contract through final warranty period of implementation phases, to include activities and milestones based on the Vendor's implementation methodology, prior experience, and details provided in this RFP. This indicative project plan should be at a level of detail sufficient to provide the Agency with a clear picture of how the Vendor might execute this initiative.

f) Utilization of a project management tool and repository to support requirement and specification traceability; schedule and task management; and storage of all work products, meeting minutes, document deliverables, issues, risks, decisions, and other project documents.

g) A description of project reporting, cadence of status meetings, and a method for the recording, distributing, accessing, and storing of key meeting minutes throughout the Program, including meeting agendas for all Vendor-led meetings.

h) An approach and methodology for Program communications management, including the methods and activities needed to ensure timely and appropriate communication amongst the Program team.

i) An approach to risk analysis, risk prioritization, risk mitigation, and risk tracking/control, including tools and techniques that should be used for risk management and escalation.

j) An approach and methodology for issue management to ensure that issues are identified, evaluated, assigned for resolution, monitored, resolved, documented, and communicated, including tools and techniques that should be used for issue management and escalation.

k) A description of the process for making Program decisions and acting upon those decisions per the Program Governance structure outlined in Section 2.4.

l) An approach and methodology for change control to address changes to the project scope, cost, and schedule, including tools for tracking and approval of change requests.

Attachment Q: Implementation Roles & Responsibilities provides additional information on technical services roles and responsibilities for implementing the System.

3.4.5.2 Training and Knowledge Transfer

The Agency seeks a Vendor who will provide a comprehensive initial and ongoing training program over the course of the ITS implementation so that all the Agency staff are properly trained in the components of the ITS that are required for their specific role(s).

Describe your approach to training and knowledge transfer, including:

a) An overall training and knowledge transfer strategy to include onsite and virtual training for technical and non-technical staff. The Agency will provide training facilities for all onsite training.

b) An approach to training needs analysis conducted to identify necessary skills by role and any special training delivery considerations.

c) A description of training methods to be utilized, including train-the-trainer, onsite instructor-led training and web-based or computer-based training ("CBT") approaches.

d) A plan for development of the curriculum and materials required for role-based training delivery and knowledge transfer, including instructor materials, presentations, hands-on exercises, CBT modules, job aids, user guides, training data, etc.

e) A knowledge transfer plan to ensure that the Agency technical personnel have the necessary skills to operate, support, and maintain the ITS during the post-implementation period including use of the Vendor's development methodology and tools. The plan should specify how knowledge achievement milestones are tracked.

f) An evaluation mechanism to allow training and knowledge transfer participants to provide feedback so that the Vendor can improve curriculum and materials.

3.4.5.3 Organizational Change Management

Describe the approach to the organizational change management ("OCM") process. The response should include the following:

a) Methodology to provide OCM services aligned with the scope, key strategic themes/drivers, and requirements and specifications in the RFP.

b) An approach and methodology for communications management, including the methods and activities needed to ensure timely and appropriate communication to Program stakeholders.

c) An approach to supporting the Agency in stakeholder engagement, including ongoing communications, planning, and execution. The goals are to minimize disruption, optimize adoption, and enable realization of targeted benefits.

d) An approach to supporting the Agency in OCM Change Impact Assessments in parallel with each implementation phase to help identify process or policy changes, people or cultural impacts, and any associated role or organizational changes required to enable the Agency to adopt the ITS solution successfully and fully.

3.4.5.4 Business Process Analysis

Describe the process to be used to validate the Functional Specifications contained in Attachment I: Functional Specifications Matrix and identify any changes to minimize customization and increase use of configuration functionality, include all special adaptation efforts that may be required to meet the Agency's future State business needs. The Vendor is expected to perform a specifications and future business process validation to identify any functional gaps before configuring the new ITS to enable the processes.

3.4.5.5 Design, Configuration and Customization

The Agency desires that the ITS be configurable outside of the core code to allow for ongoing changes, such as periodic tax rate and form changes.

a) Describe the approach and method by which the Agency's specifications for the ITS will be validated and implemented utilizing configuration and/or customization. Further, explain the method of configuration (e.g., via scripting, XML, code tables, etc.), as well as all development languages and/or platforms utilized for customization. The Agency prefers for the customization of the ITS to be kept to a minimum to limit the effect on system upgrades and maintenance, and that appropriate procedures and controls are enforced.

b) Describe the process for review, analysis and documentation of statutory requirements, business specifications, and business rules to support design and configuration of the system.

c) Describe documentation created resulting from design sessions and any associated review and approval processes, including how gaps are identified, tracked, and resolved.

d) Describe the process for identifying, documenting and designing all reports, queries, and extracts required to support each phase of the Program.

e) Describe how business rules are written in business terms to enable operational area understanding, and where appropriate, to enable the authorized business users to make updates.

f) Describe how the business rules engine applies change control to provide management of business rule changes to the various environments.

g) Describe the process when a configuration or business rule changes including:

   i) Can changes to the configuration or business rule be back dated after in production to an earlier effective date.

   ii) What happens when back dating occurs? Are processes and accounts recalculated automatically?

   iii) Can configuration or business rule values be deleted or deactivated?

   iv) What happens when deletion or deactivation occurs? Are processes or accounts recalculated with the prior business rule value?

   v) Do business rules have effective start and end dates? If so, how do the dates impact processing and calculations?

   vi) What types of dates can the business rules validate against (e.g., system date, assessment date, period dates, etc.)?

3.4.5.6 Testing

a) Describe the process for testing all application components work as designed and configured, and that those components work together in an integrated process to perform their specified functions, including interfaces/integrations to legacy applications or other Third-Party external applications, and:

   i) Approach for creating unit, integration (end-to-end), performance, stress, security, and regression test plans that are fully documented and repeatable

   ii) Approach for performing quality assurance testing (unit, integration, performance, stress, security, and regression, where applicable) prior to handing over to the Agency for User Acceptance Testing ("UAT")

   iii) Validation with a specification and design traceability matrix and demonstrations that verify the system functionality meets the business needs as documented in system design documents

iv) Approach for providing assistance and support to the Agency in preparing user acceptance test cases and during user acceptance testing

v) Use of testing tools to store and track test scripts and cases, expected results, actual results, defects and resolution

vi) Use of tools for automated performance, stress, or regression testing

vii) Use of tools for generating test application data in bulk (e.g., entities, accounts, periods, names, addresses, etc.)

b) The Agency prefers that UAT not overlap with performance or security testing or that such overlap be minimized. Describe how the different types of testing will be scheduled and planned to minimize any overlap.

3.4.5.7 Data Conversion and Migration

Data conversion will include data from several systems including ITAS and PSRM, RSI Portfolio Warehouse, and ancillary systems such as Modernized E-File system which processes multiple tax schedules, among other systems identified in Attachment O: Systems Inventory. The data conversion process steps are to be reviewed and approved by NCDOR prior to conversion execution. The Vendor will be expected to provide as many iterations of data conversion as necessary to resolve all errors and/or determine an NCDOR approved plan for resolving all data conversion errors. Once the Vendor is selected, a detailed data flow will be provided.

a) Describe the process for documenting the data requirements for data conversion, migration strategy and methodology, and how data conversion will align with proposed phases of implementation. The data conversion approach should address factors such as:

i) Data conversion requirements definition (i.e., number of years and data elements)

ii) Processes to identify data requiring cleansing and data cleansing activities

iii) Data governance

iv) Data mapping, timing, risks, staging, and operational impacts

v) Data conversion and matching of entities, accounts, financials, etc. that may be stored in legacy applications and proposed ITS across phases of the Program

vi) Conversion documentation such as record layouts for import files, mapping of source to target, and exceptions

vii) Testing and validation of conversion results and tax system functions as expected with converted data

viii) Performance testing of conversion process (mock conversions) and estimated implementation timeline

ix) Mock data conversions and their alignment to testing activities

x) Data conversion signoff and cutover processes

xi) Error handling and impact to existing interfaces

xii) Identification of potential and average number of data conversions (test conversions) required to ensure end-to-end data integrity and reliability.

xiii) Identification of any risks associated with data conversion

b) Describe any tools, scripts, and automated conversion programs used for planning, evaluating, validating or executing data conversion, and performing root cause analysis for error handling.

c) Describe the methodology used to identify gaps in the data and how to minimize the data gap through automated processes and appropriate algorithms to prevent human intervention.

d) Describe techniques and methodology used to ensure no data identified in the conversion plan is left behind and all the data has been converted to the final destination and/or to an environment that requires further analysis due to exception handling and control processes.

e) Describe how data conversion and validation efforts will be coordinated with configuration and setup (i.e. prior year forms/returns, rates and applicable business rules). This description should explicitly include whether converted data will be subject to defined validation routines when loaded to the proposed solution.

f) Describe the roles and responsibilities for Vendor staff and Agency staff in support of conversion activities to include but not limited to extracting, mapping, converting, cleansing, and validating data to be converted. Identify the resource skill set needed (i.e., background, accountability, authority, and responsibility) for data conversion. Include any associated assumptions.

3.4.5.8 Production Cut-Over

a) Describe the approach, planning and execution of activities and tasks needed for successful production cut-over to the new ITS solution. The approach should include the following:

   i) Turning over all system components into the production environment in a systematic fashion, including ensuring that workflows, custom programs, compiled modules (where required), job streams, other components of the production environment, and all documentation are ready and organized for the production turnover.

   ii) A plan for interfacing between the ITS solution and legacy solutions and databases, if necessary, until all phases are complete.

3.4.6 TECHNICAL SERVICES

The Agency is seeking a solution based on modern technologies, including the ability to be scalable from both a platform and architecture perspective. The ITS will support multiple user interface touchpoints while ensuring compliance with security standards and ease of use for all Agency constituencies. In addition to responding to Attachment J: Technical Specifications Matrix, describe how the proposed ITS solution and implementation approach addresses the following technical capabilities.

3.4.6.1 Hosting

Describe the approach for providing hosting and management services necessary to implement and maintain the ITS as described in this RFP, beginning with the initial implementation of any ITS instance and continuing throughout the implementation and post-implementation. Managed hosting includes management of all components, for all environments, provided for the ITS, which will be located on the Agency's MS Azure cloud subscription.

Describe:

a) Estimated bandwidth requirements.

b) Managed hosting services (e.g., software and hardware installation, updating, patch application, monitoring, tuning, disaster recovery and backup support, emergency and planned network, system, application maintenance, etc.).

c) A detailed description outlining the shared responsibilities of Vendor and Agency for securing, maintaining, and operating every aspect of the cloud environment, including the application, hardware, infrastructure, endpoints, data, configurations, settings, operating system (OS), network controls and access rights.

3.4.6.2 Role-Based User Security

Describe how the ITS provides configurable features that can limit or restrict access to system screens and actions based on the user's constructed role within the solution, including how a role-based security profile is attached to the user's login credentials.

3.4.6.3 Data Warehouse

The Agency currently uses RSI Portfolio Warehouse to identify non-filers, refund fraud, and other tax compliance issues. Additionally, the data warehouse is used as a data repository for IRS data extracts along with data from Agency tax systems, other State agencies/sources, and numerous Access databases and spreadsheets. The current data warehouse contains data management, audit identification and selection, tax calculation, case management, and correspondence generation capabilities. Not all of the Agency's data is currently housed in the data warehouse; data is contained in multiple systems.

a) Describe how the proposed solution could integrate with the current data warehouse for predictive and descriptive modeling, data mining, forecasting, simulation and experimental design. Also describe the typical data refresh cycle.

b) For any new data warehouse included in the proposed solution, describe the data warehouse capabilities, implementation approach and proposed tools to meet the Agency's ad hoc, analytic, data modelling, research, dashboard, tax modeling, business intelligence ("BI") and/or reporting needs. Also describe how the ITS data warehouse would incorporate and improve audit programs and fraud detection.

   Describe the following in the data warehouse design:

   i) Data sources and key structures.

   ii) Labeling and tracking of Federal Tax Information ("FTI"), including FTI viewed or printed.

   iii) The tools, routines, configuration, integration, and setup to support the initial loading and ongoing refresh of and synchronization assurance.

   iv) Compliance analytics, scoring, discovery, audit selection, and fraud detection functions to be established.

   v) Reporting tools, views, queries, and dashboards.

   vi) Backup, restore, and recovery methods and tools.

3.4.6.4 Interfaces and Third-Party Integrations

The Agency expects the ITS will require the development of inbound and outbound interfaces with systems, both inside and outside of the Agency. A list of interfaces is included in Attachment P: Interfaces Inventory.

a) Describe the approach to verifying, designing, documenting, developing, and testing interfaces and integration points that are required for the implementation of the proposed ITS solution, including how interfaces will be identified and associated with each release.

b) Describe proposed solution capabilities to interoperate with other solutions. Identify the standards supported, integrations platforms, adaptors, application programming interfaces ("APIs"), and the like.

c) Propose a decommissioning strategy in alignment with the interface and integration approach and provide for the expected use of "throw-away" interfaces, in the event that legacy systems remain operational concurrently, until deemed ready to be decommissioned.

3.4.6.5 Document Management

Describe how the proposed ITS would integrate with the Agency's existing data capture imaging and payment processing systems (See Attachment O: Systems Inventory), including, but not limited to, the following functionality:

a) Associate and/or map documents, images, and data elements to the correct taxpayer entity, account, period and, if applicable, the relevant collection or audit case.

b) Maintain a history of associated imaged documents and other artifacts created within the ITS, the functionality to search for imaged artifacts, as well as adoption and adherence to the Agency's document retention policies.

Imaged artifacts include, but are not limited to, inbound correspondence, returns, forms, payments, applications and registrations.

3.4.6.6 Environment Setup

Describe the process to set up and verify the installation of all requisite system components and environments. The Agency seeks to understand the requirements to initialize the installation of base system components, requisite third-party software, infrastructure components, middleware, etc. The various environments would include:

a) Sandbox (core solution patches and upgrades)

b) Development

c) System Test

d) User Acceptance Test

e) Pre-Production Staging

f) Production

g) Data Conversion

h) Training

3.4.6.7 System Documentation

Describe the types of documentation provided as part of the Program and how the documentation is maintained throughout the Program as additional phases are implemented.

Examples of desired documentation include but not limited to:

a) Operations Documentation: Overview of the application, system structure, major processes, required interfaces, and report and correspondence documentation. This includes any required periodic maintenance tasks. The operations documentation will also

describe the overall batch or background process schedule, including dependencies, sequencing, and timing and all batch and run time parameters.

b) Technical Documentation – System documentation that documents the application software and its architecture (e.g. implementation view of the application architecture, data flow diagram). This includes all programs and executables.

C) Customization/Configuration Documentation – Documentation including customization/configuration parameters used at the Agency, as well as the full range of alternative values possible (and the effect of each value). The documentation must reference all parameters and note and explain where dependencies occur and where environmental conditions dictate specific usage and settings.

d) User Online Help Documentation – Documentation accessible from within the application by all system users with information supporting system navigation, searches, transactions, error conditions, and update actions.

3.4.6.8 Technology Change Management

Describe the approach to, and controls over, technology change management activities including services required to appropriately manage and document (e.g., impact analysis, version control, library management, turnover management, build management, parallel development) changes to the application and any of the constituent components. Technology Change Management also includes services required to appropriately manage and document changes to the underlying application development environment components.

3.4.7 PRODUCTION SUPPORT SERVICES

Production support services include maintenance and operations (“M&O”), as well as warranty services to be provided by the Vendor during and post-implementation. The Agency is seeking a vendor who will provide production support from the first implementation through the remainder of the Program and for a period of at least twelve (12) months after the final release ‘go-live’. Production support services related to defect discovery, triage, and defect remediation should be complementary to (and not overlap with) services to be provided as part of the first year of onsite support after full implementation.

a) Describe the scope and approach to production support delivery, including functional, technical, operational, and application support.

b) Describe in detail the services under any tiered Production Support offerings, including:

   i) Product delivery including but not limited to planning and implementation of hot fixes, patches, or major solution enhancements

   ii) Functional and technical support including but not limited to defect identification, triage, and remediation, system modifications and enhancements, data fixes.

   iii) Operational support including but not limited to batch job creation, maintenance, execution, and monitoring, help phone line for Level 1 (Agency business staff), Level 2 (Agency technical staff), and Level 3 (Microsoft/3rd Party technical staff) support.

   iv) Application support including but not limited to legislative/business changes, annual tax type changes, supplemental user training and testing support.

c) If applicable, describe any use of proprietary or third-party defect tracking and resolution management software, as well as how those tools provide the capability to interface with the Agency’s ServiceNow ticket management system.

d) Describe options for vendor supported system monitoring (24 hour) and response to events starting with Phase I and continuing during and after the Program end.

e) Describe how custom code is managed, maintained and supported during upgrades and releases and on an ongoing basis.

f) Describe the proposed Service Level Agreement ("SLA") as part of the ongoing support and maintenance services. A final SLA will be mutually agreed upon between the Agency and the Vendor and shall apply for the duration of the Contract, including any extensions or renewals. Terms of the SLA should include, but not be limited to:

   i) Standard service hours

   ii) Non-standard and holiday service hours

   iii) Definition of defect or Error classification levels (e.g. Defect Severity 1, Defect Severity 2, etc.)

   iv) Proposed resolution timing for each defect or error classification

   v) Expectations regarding system response time, system uptime, downtime, and scheduled maintenance windows

   vi) Warranty extension criteria

g) Describe the services provided under the Vendor's proposed Warranty coverage.

   Include in the description the timing of when the Warranty coverage begins and the criteria that determines the start of the Warranty period such as the Agency's acceptance of the relevant aspect of the system in a production environment. The description should include a timeline of effective Warranty periods during implementation (i.e. following the go-live of each phase) as well as post-implementation Warranty coverage for the entire System once fully implemented (i.e., all phases).

3.4.7.1 Application Management

a) Describe how the proposed solution monitors and reports the metrics on system performance.

b) Describe how the proposed solution manages user administration.

c) Describe the audit capabilities of proposed solution related to management of the application.

3.4.7.2 Database Administration

The proposed tax solution is expected to be built around a common logical data dictionary, data model and a centralized database infrastructure that is separate from the transactional database. This consistency will allow the Agency to use a common set of tools for reporting and analysis.

a) Describe services related to on-going maintenance and support for the ITS database(s) to support broader data and analytic initiatives.

b) Vendor is expected to provide replication of application data from Production to an environment of the Agency's choosing. Describe how the Vendor has accommodated this capability for other clients or how it will fulfill the business need in this instance.

3.4.7.3 Disaster Recovery and Business Continuity

a) Describe in detail the Vendor's plans to mitigate against any disaster that would affect the ability to provide the Agency with the proposed ITS. Provide a detailed plan of the

proposed solution's security infrastructure including facility and information technology security. Provide plans of action for the following security incidents, as applicable to the RFP:

i) Interruption of service including denial of service attacks

ii) Vulnerability incidents

iii) Data loss or compromise

iv) Insider attacks

b) Describe the proposed solution's Disaster Recovery and Business Continuity Plan, including but not limited to:

i) Redundancy, Data Backup, and Disaster Recovery

ii) Data Export/Import

iii) Data Ownership and Access

iv) Testing

v) Recovery time objectives ("RTO") and data recovery point objectives ("RPO")

3.4.8 KEY FUNCTIONALITY

Vendors are asked to complete the Attachment I: Functional Specifications Matrix containing the Agency's business specifications as part of the Vendor's comprehensive proposal response.

In addition to completing and submitting Attachment I: Functional Specifications Matrix, Vendors are asked to describe how the proposed ITS and implementation approach addresses the following specific functional capabilities.

3.4.8.1 Reporting, Analytics, Queries and Extracts

a) Describe system capabilities to support the following:

i) Analytics driven workforce and key performance indicator reporting capabilities providing meaningful measurement of organizational performance.

ii) Executive dashboard reporting to include charts and graphs.

iii) Detailed reporting on tax revenue and tax-related operations (e.g., returns, refunds, audits, collections, refund interest, fraud, billings, tax credits, etc.).

iv) Operational/Standard Reporting – operational reports that are run and distributed on a regular basis and used to manage business operations.

v) Ad-hoc Reporting and Queries– special purpose reports and queries run on demand with the ability to copy logic and designs from other reports to create new ones quickly.

vi) Advanced Analytics Reporting – complex reports consisting of calculations against data sets, and reports that show trends and "what if" results.

vii) Reports forecasting revenue, reporting on past periods and conducting trend analysis to provide both historical and real-time insight into business operations.

b) Describe the architecture and technologies used to provide reporting for:

i) Operational reports

ii) Ad hoc reports

iii) Scheduled reports

iv) Reporting from both the Data Warehouse and the transactional database

Include any options to utilize Third Party reporting tools (e.g., Excel, Crystal, Cognos, Tableau, Power BI, etc.)

c) Describe the process for gathering reporting requirements for each implementation phase and any limitations to number of reports developed as part of this RFP response.

d) Describe the proposed solution's use of Business Intelligence ("BI") tools to perform advanced analytics. Include how Vendors proposed ITS integrates with commercial BI tools or has an analytical tool built-in to provide the functionality and meet the needs of the end-user as described in Attachment J: Technical Specifications.

e) Describe capabilities provided for operational staff who may not have technical knowledge to create reports (e.g., capabilities not requiring knowledge of SQL or similar programming) and any tools available for use. Include the interface available to users to save user-created reports, custom designed reports and queries for future use and ability to share extract criteria. End users may need an understanding of logical data element names and relationships in addition to actual table and field names.

f) Describe the analytical and statistical reporting features of the proposed solution including trend analysis, variance analysis, regression analysis, projections, what-if analysis, random sampling, and charting.

g) Describe how your solution handles the creation and maintenance of reports, including the ability to query and report against any data field defined by the Agency. Provide detail regarding the ability to create real-time and batch reports, the output types that are available for reports, and any limitations to data that can be included in reports.

h) Describe reporting capabilities to support creating and maintaining standard report distribution for pre-defined reports.

i) Describe how reports are managed and cataloged such as use of a report library or repository along with report metadata (e.g., description, purpose, version, owner and use statistics).

j) Describe any processes, best practices or restrictions associated with developing and running reports and queries to ensure no negative impact on application performance.

k) Describe capabilities provided for the Agency economists to perform economic forecasting, determine fiscal impacts of tax law changes and dynamic scoring (i.e. secondary effect of tax changes on the economy), identify recent and long-term trends, and use microsimulation data.

l) Describe capabilities available for creating an individual income tax microsimulation file that matches State income tax data with IRS Individual Master File/Individual Transaction File (IMF/IRTF) data at the taxpayer level.

m) Describe how the proposed solution produces microsimulation data that conforms to IRS Publication 1075 tax modeling methodology/standards.

n) Describe how the proposed solution ensures microsimulation data conforms with federal and state regulations to protect taxpayer confidentiality, such as removing personally identifiable information, and blurring the data (e.g., replacing actual values with average values for a group of similar taxpayers).

o) Describe how the proposed solution removes outlier values from the microsimulation data and takes stratified samples based on user-defined business rules.

p) Consumer Use Tax is reported on three different forms: Individual Income Tax Form, Boat and Aircraft Form and a separate Consumer Use Tax Form. Describe how the proposed solution can aggregate data and generate reports based on consumer use tax reported on multiple tax type forms.

3.4.8.2 Taxpayer Profile and Account Management

a) Describe the proposed solution's ability to extend the solution to add new data elements in the future for an entity, account, case, etc.

b) Describe the proposed solution's search capabilities. Explain whether the proposed solution has a maximum number of items that will be returned when an Agency user performs a search. If so, describe the maximum volume, how the maximum volume message is displayed to the user, and whether additional results can be viewed without refining the search criteria.

c) Describe how the proposed solution establishes taxpayer accounts and records activity on that account, including account creation, the posting of returns and payments, adjustments, display of document detail, and recording and display of account history.

d) Describe how the proposed solution manages the relationship between multiple identification numbers (e.g., a unique account identification number, federal employer identification number, Secretary of State number, streamlined sales tax identification number, or social security number) of a single entity.

e) Describe how the proposed solution accounts for duplicate social security numbers ("SSNs"), Federal Employer Identification Numbers ("FEINs"), and Individual Taxpayer Identification Numbers ("ITINs"), including how Agency users are alerted to potential account duplicates, e.g., workflow items for review or an indicator.

f) Describe how the proposed solution creates taxpayer accounts based on limited data and updates taxpayer account information as return, payment, or other data is received.

g) Describe the data elements required by the proposed solution to establish a relationship between a taxpayer entity and a third-party entity (e.g., employer, tax representative or payroll service provider)

h) Describe whether the proposed solution allows legacy account identification numbers to be used or if new account identification numbers will be created in the new solution for converted accounts.

i) Describe how the proposed solution manages joint liabilities, including spouses, responsible officers, and other situations where individuals are jointly liable for a tax debt.

j) Describe how the proposed solution allows for suspending system actions (e.g., outbound correspondence, billing, penalty and interest accrual) based on user intervention (e.g., bankruptcy, audit, investigation), natural disaster, temporary policy, or legislative change.

k) Describe how the proposed solution stores and validates addresses and phone numbers. Include U.S. addresses and phone numbers, international addresses and phone numbers, how the system distinguishes between international and US information, and any field size limitations.

l) Describe how the proposed solution selects the correct address for refunds, bills, and other outbound correspondence when multiple taxpayer addresses exist on the account.

m) Describe how the proposed solution standardizes addresses for the US Postal Service.

n) Describe the proposed solution's address verification functionality, including the data source and the frequency and method of updates. Include how business rules may be leveraged to determine the most current address.

o) Describe the proposed solution's ability to leverage other external interfaces to update addresses and phone numbers. Include how business rules may be leveraged to determine the most current address.

p) Describe how the proposed solution updates the data classification of each data element upon receiving the same data from a non-FTI source.

3.4.8.3 Submissions Processing

a) Define the process for reviewing the forms and associated business rules and processing requirements for each implementation phase and any limitations to the number of forms developed as part of this RFP response. See Attachment N: Forms Inventory.

b) Once a form has been defined or configured in the system and returns have been processed, there may be a need to make a change to the form definition or configuration. Describe how the change would be implemented in the proposed solution including any impact on previously processed returns.

c) Describe how the proposed solution supports data exchanges with the Sales and Use Streamline Governing Board. Include functionality such as verifying account numbers, processing registrations and adding, updating and closing accounts.

d) Describe how the proposed solution allows an employee to create and record manual deposits and how revenue accounting is updated. Manual deposits could include deposits for cash, foreign checks, or rejected checks from Image Cash Letter that are unable to be sent via electronic methods.

e) Currently an interface exists between the legacy tax system and the data capture system. Images from the data capture system are automatically retrieved from the image repository and displayed as suspended transactions (work list items) are selected. The image and suspended transaction are displayed side by side. Describe any similar functionality associated with the proposed solution.

f) Describe how the proposed solution reconciles payments (item count and amount) from payment sources including the third-party payment processor.

g) Describe how the proposed solution processes bank deposit errors (e.g., check encoding errors or checks paid twice).

h) Describe how the proposed solution could manage and track incomplete payment transactions that cannot be posted to a tax account. For example, payments are received without enough information to determine the correct tax entity. Include actions such as:

   i) Depositing funds

   ii) Tracking collections that cannot be allocated

   iii) Corresponding with the entity sending the payment for additional information

   iv) Creating a voucher with correct taxpayer information to include original payment

   v) Receipt date and check amount

   vi) Accounting for the payment for reporting purposes

i) Describe how the proposed solution can programmatically apply payments received by check that are split between two tax types but should be applied to just one.

j) Describe how the proposed solution processes payments prior to configuration and deployment of the associated return in production. For example, a payment is received by check for Individual Income tax year 2023 in January 2024. The check must be processed and deposited, but the 2023 tax period may not be defined in the system at that time.

k) Describe how the proposed solution processes a return that is for a filing period which is outside the range of the return configuration's effective dates. For example, an entity submits an out of business notification and final tax return for a tax period where the version of the return's configuration is not yet defined in the solution.

l) Describe how payments or returns are processed for tax accounts or tax periods that were not converted from the legacy systems.

m) Currently, when forms and payments are processed, business rules are applied and some transactions suspend and require manual intervention prior to posting to the tax account. Describe how the proposed solution provides similar functionality. Include any capabilities to make corrections and reprocess transactions in bulk without having to manually make corrections to each transaction.

n) Describe how the proposed solution processes different types of payments (checks, debits, credit cards) rejected by the bank due to a variety of reasons (e.g., insufficient funds, bad account number, closed bank account). Include how the taxpayer account and revenue accounting are updated.

o) Some of the Agency source systems currently assign an intelligent Document Locator Number ("DLN") that is uploaded to the tax systems. The DLN is maintained in the source system to enable a cross-reference between the two systems (e.g., data capture system). Describe the format of DLNs generated by the proposed solution. Include how DLNs generated by external source systems will be differentiated and unique from DLN generated by the proposed solution.

p) On a semi-annual basis, a file is created from the legacy tax processing system containing partial demographic information for specific tax types. For example, the Individual Income tax file contains the following information for existing accounts:

   i) Primary and Secondary SSN,

   ii) Part of last name,

   iii) Part of address, and

   iv) Zip code

   As part of an account verification process, the Data Capture system uses the file to match against demographic data from scanned returns and payments to determine if the taxpayer and account exist. If a match exists, the partial demographic information from the file (i.e., 9-digit SSN, First 4 characters of last name, etc.) is included in the data capture extract. If a match does not exist, full taxpayer demographic information from the return or payment is included in the data capture extract.

   Describe how the proposed solution will integrate with the Agency's data capture system and if a similar account verification process may be needed.

3.4.8.4 Financial Transactions

a) Describe how the proposed solution manages the merging of two accounts. Examples include when two individuals are separately assessed as individual tax entities but later file a joint tax return, and payments have been made in each separate account.

b) Describe how the proposed solution handles multiple tax types on one form. Specifically, how the financials are displayed, how revenue accounting tracks receipts and liabilities by tax type, and how information is displayed on correspondence.

c) Describe how the proposed solution identifies, tracks, and accounts for internal and external offsets of taxpayer refunds.

d) Corporate and Franchise taxes are included on one tax form. Current processing includes duplicating the shared profile information and separating applicable form line items to the two different tax accounts, allowing the Corporate account to use the DLN assigned by the source system and assigning a unique DLN to Franchise tax. Each account (Corporate and Franchise) functions as a separate account within the system. Describe how the proposed solution would process one tax return that includes two different tax types and must account for payments separately.

e) The Agency assesses a Collection Assistance Fee ("CAF") which applies when a liability is not paid and an installment agreement has not been approved within sixty (60) days of the Notice of Collection, or an installment agreement defaults. Describe how the proposed solution can identify tax periods that should be assessed the fee.

3.4.8.5 Collections

a) Describe how the proposed solution manages taxpayer accounts that are in Bankruptcy. Include how accounts are identified in the system, users are alerted of bankruptcy status and creation of associated workflow items.

b) Describe how the proposed solution tracks and displays collections activity at the entity, tax account, and tax period levels.

c) Describe how the proposed solution tracks and reports collection statistics at multiple levels such as the division, work unit, and employee level. Include capabilities to create dashboards and scorecards for monitoring key performance metrics.

d) Describe how the proposed solution identifies accounts that might need a certificate of tax liability ("CTL") to be docketed or released. A CTL may be filed to collect a tax owed by a taxpayer and places a judgment on any real or personal property held by a taxpayer, which must be satisfied or resolved to get a clear title to the property.

e) Describe how the proposed solution supports automating generation of CTLs and creation of a central lien repository for all CTLs issued by the ITS that can be published externally for searching.

f) Describe how the proposed solution can automate the matching of assets and data to support programmatic issuance of wage and bank garnishments. For example, match asset information and data from NC-3, W-2, bank information, 1099Misc, and other data sources to taxpayers that have collectible debt and automatically issue a wage or bank garnishment. Include any functionality related to creation and maintenance of relationships between entities for related asset matches.

g) Describe how the proposed solution performs a liability settlement where the liability cannot be reinstated (programmatically or manually) on tax periods that have been deemed uncollectible by statute. For example, liabilities over 10 years old or liabilities where an Offer in Compromise is accepted.

h) Describe how the proposed solution allows users to download cases and work in an "offline" mode. For example, work from a laptop not connected to the Agency's network.

i) Describe how the proposed solution allows a single liability to be shared among multiple taxpayers, such as responsible officers.

j) Describe how the proposed solution allows addition and removal of various types of suppressions to an entity, account, filing period, or case with reason for suppression (e.g., Active Military Combat Zone and Natural Disaster) which can limit or suspend activities such as penalty and interest accrual, billing refunds, enforced collections, correspondence and other actions from occurring.

k) Describe how the proposed solution routes and prioritizes collections workflow items. Examples include but are not limited to total balance owed, previous collection activity, asset matching, time in a particular status, time in a workflow state, existence of delinquent or non-filed returns, existence of specific workflow item types such as bankruptcy or Offer in Compromise, existence of payment plans, and any combination of the above.

3.4.8.6 Audit and Examinations

a) Describe how the proposed solution supports the identification of fraudulent returns, fraudulent preparers, and tax protestors during return processing. Include analytics capabilities available to identify non-compliance, fraud, identity theft and non-filers and how compliance issues can be prioritized for review.

b) Describe how the proposed solution supports the end-to-end audit process, including the selection of potential audit candidates for any tax type, comparison of third-party information and audit results.

c) Describe how the user will access a taxpayer's audit history notes and activities across tax types.

d) Describe how the proposed solution tracks auditors' case inventory level, assessment dollars, and the audit hours utilized while completing an audit. Explain whether the proposed solution will also be able to track additional adjustments made to audits (e.g., reversals and secondary audit).

e) Describe how the proposed solution supports an automated Individual Income tax or business tax non-filer program, including but not limited to:

   i) Using data from various sources to identify non-filed returns

   ii) Creating a case for each non-filed return

   iii) Calculating an estimated liability

   iv) Issuing a notice to the taxpayer regarding the estimated liability

   v) Allowing throttling of notices

   vi) Allowing adjustments to the estimated liability

   vii) Issuing a revised assessment

f) Once data is archived/purged from the proposed solution, describe the process used for re-establishing the tax period and financial transactions to process an audit or additional adjustments.

3.4.8.7 Revenue Accounting

a) Describe how the proposed solution supports the timely receipt and allocation or distribution of collections to hundreds of jurisdictions for a variety of tax types, such as the distribution of sales taxes to local governments and special districts. In addition, describe how receipts and disbursements are compiled and reconciled as well as how receipts are processed and managed when no return has been filed to indicate proper distribution of the money.

b) Describe controls within the proposed solution that exist to prevent duplicate distributions or transfers of the same funds to internal or external entities.

c) Describe how the proposed solution reconciles refund checks written, returned, cancelled, and paid.

3.4.8.8 Correspondence

a) Describe process controls that exist to manage the generation of correspondence (e.g., stagger the release dates of a high volume of correspondence to keep call center volumes manageable). In addition, define the criteria and parameters that can be used to segment correspondence for volume control.

b) Describe how notice, bill and correspondence templates are created, maintained and version control applied. Include how templates can be designed to include account financials and return line item details.

c) Describe functionality within the proposed solution that works to reduce undeliverable mail and automate returned mail processing.

d) Describe capabilities within the proposed solution to issue courtesy copies of correspondence to third parties other than the primary recipient (e.g. power of attorney (“POA”), accountant, or attorney).

e) Describe the process for gathering notice and correspondence requirements for each implementation phase and any limitations to number of notices and correspondence developed as part of this RFP response.

3.4.8.9 Workflow and Case Management

a) Describe how the proposed solution programmatically routes and assigns work list items and cases. Include in the response the type of work list items and cases that can be defined.

b) Describe how the business rules for workflow and work list items are created and maintained.

3.4.8.10 Notes and Reason Codes

a) Describe information captured and displayed when a note is created or updated. (e.g., user identifier (“ID”), username, date, time and other audit trail information).

b) Describe how notes are corrected, whether entered in error or requiring revision.

c) Describe any limitations on notes, including the maximum number of characters in a note and the maximum number of notes that can be added to an entity, account, filing period, case, or other areas where notes may be captured.

d) Describe proposed solution functionality supporting programmatic or manual selection of reason codes and associated explanations for printing on notices and correspondence generated for external recipients. Describe any limitations the proposed solution has

related to reason codes. Specifically, the maximum characters that can be included in reason codes and maximum number of reason codes that can be created and maintained.

e) Describe how the proposed solution handles data classification for notes (e.g., FTI) including whether the ability exists to redact any information designated as FTI when printing notes.

3.4.8.11 Electronic Submissions and Taxpayer e-Services Portal

a) Describe how the proposed solution supports a web-based taxpayer self-service portal that includes, but is not limited to the following functionality:

   i) Allow taxpayers, authorized tax professionals, and bulk filers to submit, update, and review their information such as licenses, returns, correspondence and communication, payments, and refunds based on established business rules and validation procedures.

   ii) Create and manage account information and access based on established business rules and validation procedures.

   iii) View account balances and payments due.

   iv) Manage and coordinate payments required via all payment channels.

   v) Track real-time progress of license, returns, payment status, and cases.

   vi) Establish payment plans based on established business rules and validation procedures.

   vii) Provide historical review of tax information and payments.

   viii) Submit questions to the Agency and receive secure responses.

   ix) Issue reminders and notifications on payments due and compliance activities.

b) Describe the proposed solution's ability to accept W-2 and 1099 forms via bulk method in the format prescribed by the Social Security Administration ("SSA") and IRS, including the proposed solution's validation process for electronically submitted W-2s and 1099s to reduce the chance of fraudulent document submissions.

c) The Agency participates in the Federal/State Modernized eFile ("MeF") program. Describe how the proposed solution will support processes to receive, validate, store, and process State returns e-filed in conjunction with Federal returns.

   i) Individual Income

   ii) Corporate/Franchise

   iii) Partnership

   iv) Estates and Trusts

d) Describe the level of automation associated with the proposed solution's assurance testing process for MeF. Include in the response answers to the following questions:

   a) Are transmitters able to submit test cases directly in the test environment?

   b) If so, is the proposed solution able to associate the submission to the transmitter and test case automatically?

   c) Is there a process to provide results to transmitters automatically as to whether their submission is accepted or rejected and whether it passes the criteria for the test case?

e) Describe how the proposed solution stores and maintains MeF transmitter supported forms and limitations for purposes of testing (e.g., determining cases and forms required for approval) and production (e.g., forms that can be accepted from the provider, such as amended forms).

f) Describe the proposed solution's functionality related to Letter of Intent submissions by software providers that support MeF and creation of substitute tax forms. Describe whether the solution provides the ability for the provider to submit the document electronically in a format that the data is captured and can be used as part of the approval process.

g) The Agency will participate in the IRS Direct File Program for filing season 2025 (Tax Year 2024). Describe how the proposed solution supports integration with the IRS Direct File Program for a state filing option and how the State returns will be processed in the new system.

3.4.8.12 Unauthorized Substance

The Agency administers the Unauthorized Substance ("USUB") Tax that has some unique processing needs. Many times, agents work in areas with limited internet connections and need to issue assessments in the middle of the night at a remote location using up-to-date system data. With the current system, the users have a copy of an application on their laptop which "syncs" to the main system daily. Describe how the proposed solution can provide similar or the same functionality to meet business needs. Include how the proposed solution could support the following capabilities:

a) Provide 24/7 access to system data on laptops in the field for research

b) Manually add cases or accounts (accounts can be individual or joint)

c) Provide account numbers via a workflow process

d) Manually enter possession date and time, location, type of substance and quantity, reporting officer name and contact info, USUB agent information

e) Generate an assessment on-demand for the full amount to each of the taxpayers on the account from laptops with tables to calculate the correct tax based on quantity, substance type, and tax rate

f) Sync or transfer case information captured offline to the main system daily without any duplicate entry

g) Track each event as a case or account

h) Allow multiple possession dates and substances on one account

i) Enter fees on the account that are variable in amount and type (e.g., towing and printing)

j) Interface to state's surplus property system for tracking items being sold for USUB debt

k) Apply penalties 48 hours from the date/time of possession

l) Track distribution for each case/account

m) Provide a generic account, not a taxpayer entity, for processing tax stamps purchases to which the money can be posted and tracked

3.5 ORAL PRESENTATION AND PRODUCT DEMONSTRATION

Preliminary scores from the initial evaluation of Offers will be used to select Vendors to provide up to four (4) days of oral presentations and solution demonstrations. Presentations will take place in Raleigh, North

Carolina. Exact dates and location of the presentations will be made available at least two (2) weeks in advance.

The purpose of oral presentation and product demonstration is to clarify and expand upon information provided in the written proposals. Vendors are prohibited from altering the basic substance of their Offers.

Should the Vendor be invited to Oral Presentations and Demonstrations, Key Personnel are expected to be present. The Agency may request to interview certain Key Personnel as part of the Oral Presentations and Demonstration phase of the evaluation.

3.6 VALUE ADDED SERVICES

Vendors are invited to propose value-added services and/or features that may be deemed beneficial to the ongoing improvement of the Agency's tax and revenue administration efforts, both near-term and long-term, but are not contemplated in the scope of services and requirements detailed in this RFP.

Vendors should provide costs for any proposed value-added services and/or features in Attachment D: Cost Form, but these costs will not be included in the Total Cost Summary. Costs for value-added services and/or features will not be scored in the evaluation but are informational purposes for the Agency.

4.0 COST OF VENDOR'S OFFER

4.1 OFFER COSTS

The Vendor must list, itemize, and describe any applicable offer costs in Attachment D: Cost Form.

4.2 PAYMENT SCHEDULE

The Vendor shall propose its itemized payment schedule based on the content of its offer. All payments must be based upon acceptance of one or more Deliverables and subject to the Retainage Provisions of subsection 7.3(a).

5.0 EVALUATION

5.1 SOURCE SELECTION

A trade-off/ranking method of source selection will be utilized in this procurement to allow the State to award this RFP to the Vendor providing the Best Value and recognizing that Best Value may result in award other than the lowest price or highest technically qualified offer. By using this method, the overall ranking may be adjusted up or down when considered with or traded-off against other non-price factors.

a) Evaluation Process Explanation. State Agency employees will review all offers. All offers will be initially classified as being responsive or non-responsive. If an offer is found non-responsive, it will not be considered further. All responsive offers will be evaluated based on stated evaluation criteria. All offers will be compared with other Vendors' offers. Any references in an answer to another location in the RFP materials or Offer shall have specific page numbers and sections stated in the reference.

b) To be eligible for consideration, Vendor's offer must substantially conform to the intent of all specifications. Compliance with the intent of all specifications will be determined by the State. Offers that do not meet the full intent of all specifications listed in this RFP may be deemed deficient. Further, a serious deficiency in the offer to any one (1) factor may be grounds for rejection regardless of overall score.

c) The evaluation committee may request clarifications, an interview with or presentation from any or all Vendors as allowed by 9 NCAC 06B.0307. However, the State may refuse to accept, in full or partially, the response to a clarification request given by any Vendor. Vendors are cautioned that

the evaluators are not required to request clarifications; therefore, all offers should be complete and reflect the most favorable terms. Vendors should be prepared to send qualified personnel to Raleigh, North Carolina, to discuss technical and contractual aspects of the offer.

d) Vendors are advised that the State is not obligated to ask for or accept after the closing date for receipt of offer, data that is essential for a complete and thorough evaluation of the offer.

5.2 EVALUATION CRITERIA

Evaluation shall include best value, as the term is defined in N.C.G.S. § 143-135.9(a)(1), compliance with information technology project management policies as defined by N.C.G.S. §143B-1340, compliance with information technology security standards and policies, substantial conformity with the specifications, and other conditions set forth in the solicitation. The following Evaluation Criteria are listed in Order of Importance.

a) How well the Vendor's offer conforms with specifications, including in Section 3.4, Attachment I: Functional Specification Matrix, Attachment J: Technical Specification Matrix, and Section 3.5 Oral Presentations and Product Demos.

b) How each Vendor's offer compares with other Vendor's offers.

c) Vendor experience and references as described in Attachment W: Vendor Experience and Attachment G: References.

d) How well the Vendor's offer conforms with Terms and Conditions in Section 7.14 Special Terms and Conditions and Section 7.15 Agency Terms and Conditions.

e) Illustration(s) and/or explanations of adherence to Section 3.3 Enterprise Specifications and Section 3.4.6 Technical Services.

f) Vendor's schedule and timeline for completing the work.

g) Total cost of ownership.

5.3 BEST AND FINAL OFFERS ("BAFO")

The State may establish a competitive range based upon evaluations of offers and request BAFOs from the Vendor(s) within this range; e.g. "Finalist Vendor(s)". If negotiations or subsequent offers are solicited, the Vendor(s) shall provide BAFO(s) in response. Failure to deliver a BAFO when requested shall disqualify the non-responsive Vendor from further consideration. The State will evaluate BAFO(s), oral presentations, and product demonstrations as part of the Vendors' respective offers to determine the final rankings.

5.4 POSSESSION AND REVIEW

During the evaluation period and prior to award, possession of the bids and accompanying information is limited to personnel of the issuing agency, the contracted procurement support vendor, and to the committee responsible for participating in the evaluation. Vendors who attempt to gain this privileged information, or to influence the evaluation process (i.e. assist in evaluation) will be in violation of purchasing rules and their offer will not be further evaluated or considered.

After award of contract the complete bid file will be available to any interested persons with the exception of trade secrets, test information or similar proprietary information as provided by statute and rule. Any proprietary or confidential information, which conforms to exclusions from public records as provided by N.C.G.S. §132-1.2 must be clearly marked as such in the offer when submitted.

6.0 VENDOR INFORMATION AND INSTRUCTIONS

6.1 GENERAL CONDITIONS OF OFFER

6.1.1 VENDOR RESPONSIBILITY

It shall be the Vendor's responsibility to read this entire document, review all enclosures and attachments, and comply with all specifications, requirements and the State's intent as specified herein. If a Vendor discovers an inconsistency, error or omission in this solicitation, the Vendor should request a clarification from the State's contact person.

The Vendor will be responsible for investigating and recommending the most effective and efficient solution. Consideration shall be given to the stability of the proposed configuration and the future direction of technology, confirming to the best of its ability that the recommended approach is not short lived. Several approaches may exist for hardware configurations, other products and any software. The Vendor must provide a justification for their proposed hardware, product and software solution(s) along with costs thereof. Vendors are encouraged to present explanations of benefits and merits of their proposed solutions together with any accompanying Services, maintenance, warranties, value added Services or other criteria identified herein.

6.1.2 RIGHTS RESERVED

While the State has every intention to award a contract as a result of this RFP, issuance of the RFP in no way constitutes a commitment by the State of North Carolina, or the procuring Agency, to award a contract. Upon determining that any of the following would be in its best interests, the State may:

a) waive any formality;

b) amend the solicitation;

c) cancel or terminate this RFP;

d) reject any or all offers received in response to this RFP;

e) waive any undesirable, inconsequential, or inconsistent provisions of this RFP;

f) if the response to this solicitation demonstrates a lack of competition, negotiate directly with one or more Vendors;

g) not award, or if awarded, terminate any contract if the State determines adequate State funds are not available; or

h) if all offers are found non-responsive, determine whether Waiver of Competition criteria may be satisfied, and if so, negotiate with one or more known sources of supply.

6.1.3 SOLICITATION AMENDMENTS OR REVISIONS

Any and all amendments or revisions to this document shall be made by written addendum from the Agency Procurement Office. If either a unit price or extended price is obviously in error and the other is obviously correct, the incorrect price will be disregarded.

6.1.4 ORAL EXPLANATIONS

The State will not be bound by oral explanations or instructions given at any time during the bidding process or after award. Vendor contact regarding this RFP with anyone other than the State's procurement contact person may be grounds for rejection of said Vendor's offer. Agency staff contact without the direction of the State's procurement contact person regarding this RFP with any Vendor may be grounds for cancellation of this RFP.

6.1.5 E-PROCUREMENT

This is an E-Procurement solicitation. See ATTACHMENT B, paragraph #38 of the attached North Carolina Department of Information Technology Terms and Conditions.

The Terms and Conditions made part of this solicitation contain language necessary for the implementation of North Carolina's statewide E-Procurement initiative. It is the Vendor's responsibility to read these terms and conditions carefully and to consider them in preparing the offer. By signature, the Vendor acknowledges acceptance of all terms and conditions including those related to E-Procurement.

a) General information on the E-Procurement service can be found at http://eprocurement.nc.gov/

b) Within two days after notification of award of a contract, the Vendor must register in NC E-Procurement @ Your Service at the following website: http://eprocurement.nc.gov/Vendor.html

c) As of the RFP submittal date, the Vendor must be current on all E-Procurement fees. If the Vendor is not current on all E-Procurement fees, the State may disqualify the Vendor from participation in this RFP.

6.1.6 ELECTRONIC VENDOR PORTAL (EVP)

The State has implemented the electronic Vendor Portal (eVP) that allow the public to retrieve award notices and information on the Internet at https://evp.nc.gov. Results may be found by searching by Solicitation Number or agency name. This information may not be available for several weeks dependent upon the complexity of the acquisition and the length of time to complete the evaluation process.

6.1.7 PROTEST PROCEDURES

Protests of awards exceeding $25,000 in value must be submitted to the issuing Agency at the address given on the first page of this document. Protests must be received in the purchasing agency's office within fifteen (15) calendar days from the date of this RFP award and provide specific reasons and any supporting documentation for the protest. **All protests are governed by Title 9, Department of Information Technology (formerly Office of Information Technology Services), Subchapter 06B Sections .1101 - .1121.**

6.2 GENERAL INSTRUCTIONS FOR VENDOR

6.2.1 QUESTIONS CONCERNING THE RFP

All inquiries regarding the solicitation specifications or requirements are to be addressed to the contact person listed on Page 1 of this solicitation via the Ariba Sourcing Tool's message board.

All general inquiries regarding the solicitation are to be addressed to the contact person listed on Page 1 of this solicitation. Vendor contact regarding this Solicitation with anyone other than the contact person listed on Page 1 of this Solicitation may be grounds for rejection of said Vendor's offer.

Written questions concerning this Solicitation will be received until **March 28, 2025** at **3:00 PM Eastern Standard Time**.

Written questions must be submitted via the Ariba Sourcing Tool's Message Board by the date and time specified above. Please enter "Questions RFP Tax System Modernization" as the subject for the message. Questions should be submitted in the following format:

REFERENCE	VENDOR QUESTION
RFP Section, Page Number	

The Agency will prepare responses to all written questions submitted by the stated deadline and post an addendum to the RFP on the North Carolina electronic Vendor Portal (eVP). The Offeror is cautioned that contacting anyone other than the individual noted on the Page 1 of this RFP may be grounds for rejection of said Offeror's response.

Questions received prior to the submission deadline date, the State's response, and any additional terms deemed necessary by the State will be posted in the Sourcing Tool in the form of an addendum and shall become an Addendum to this RFP. No information, instruction, or advice provided orally or informally by any State personnel, whether made in response to a question or otherwise in connection with this RFP, shall be considered authoritative or binding. Vendors shall rely only on written material contained in an Addendum to this RFP.

Questions or issues related to using the Sourcing Tool itself can be directed to the North Carolina eProcurement Help Desk at 888-211-7440, Option 2. Help Desk representatives are available Monday through Friday from 7:30 AM ET to 5:00 PM Eastern Standard Time

6.2.2 ADDENDUM TO RFP

If a pre-offer conference is held or written questions are received prior to the submission date, an addendum comprising questions submitted and responses to such questions, or any additional terms deemed necessary by the State shall become an Addendum to this RFP and provided via the State's Ariba Sourcing Tool. Vendors' questions posed orally at any pre-offer conference must be reduced to writing by the Vendor and provided to the Purchasing Officer as directed by said Officer. Oral answers are not binding on the State.

Critical updated information may be included in these Addenda. It is important that all Vendors bidding on this RFP periodically check the State's Sourcing Tool for all Addenda that may be issued prior to the offer opening date.

6.2.3 COSTS RELATED TO OFFER SUBMISSION

Costs for developing and delivering responses to this RFP and any subsequent presentations of the offer as requested by the State are entirely the responsibility of the Vendor. The State is not liable for any expense incurred by the Vendors in the preparation and presentation of their offers.

All materials submitted in response to this RFP become the property of the State and are to be appended to any formal documentation, which would further define or expand any contractual relationship between the State and the Vendor resulting from this RFP process.

6.2.4 VENDOR ERRATA AND EXCEPTIONS

Any errata or exceptions to the State's requirements and specifications may be presented on a separate page labeled "Exceptions to Requirements and Specifications". Include references to the corresponding requirements and specifications of the Solicitation. Any deviations shall be explained in detail. **The Vendor shall not construe this paragraph as inviting deviation or implying that any deviation will be acceptable. Offers of alternative or non-equivalent goods or services may be rejected if not found substantially conforming; and if offered, must be supported by independent documentary verification that the offer substantially conforms to the specified goods or services specification.** If a vendor materially deviates from RFP requirements or specifications, its offer may be determined to be non-responsive by the State.

Offers conditioned upon acceptance of Vendor Errata or Exceptions may be determined to be non-responsive by the State.

6.2.5 ALTERNATE OFFERS

The Vendor may submit alternate offers for various levels of service(s) or products meeting specifications. Alternate offers must specifically identify the RFP specifications and advantage(s) addressed by the alternate offer. Any alternate offers must be clearly marked with the legend as shown herein. Each offer must be for a specific set of Services or products and offer at specific pricing. If a Vendor chooses to respond with various service or product offerings, each must be an offer with a different price and a separate RFP offer. Vendors may also provide multiple offers for software or systems coupled with support and maintenance options, provided, however, all offers must satisfy the specifications.

Alternate offers must be submitted in a separate document and clearly marked "Alternate Offer for 'name of Vendor'" and numbered sequentially with the first offer if separate offers are submitted.

6.2.6 MODIFICATIONS TO OFFER

An offer may not be unilaterally modified by the Vendor.

6.2.7 BASIS FOR REJECTION

Pursuant to 9 NCAC 06B.0401, the State reserves the right to reject any and all offers, in whole or in part; by deeming the offer unsatisfactory as to quality or quantity, delivery, price or service offered; non-compliance with the specifications or intent of this solicitation; lack of competitiveness; error(s) in specifications or indications that revision would be advantageous to the State; cancellation or other changes in the intended project, or other determination that the proposed specification is no longer needed; limitation or lack of available funds; circumstances that prevent determination of the best offer; or any other determination that rejection would be in the best interest of the State.

6.2.8 NON-RESPONSIVE OFFERS

Vendor offers will be deemed non-responsive by the State and will be rejected without further consideration or evaluation if statements such as the following are included:

) "This offer does not constitute a binding offer",
a) "This offer will be valid only if this offer is selected as a finalist or in the competitive range",
b) "The Vendor does not commit or bind itself to any terms and conditions by this submission",
c) "This document and all associated documents are non-binding and shall be used for discussion purposes only",
d) "This offer will not be binding on either party until incorporated in a definitive agreement signed by authorized representatives of both parties", or
e) A statement of similar intent

6.2.9 VENDOR REGISTRATION WITH THE SECRETARY OF STATE

Vendors do not have to be registered with the NC Secretary of State to submit an offer; however, in order to receive an award/contract with the State, they must be registered. Registration can be completed at the following website: https://www.sosnc.gov/Guides/launching_a_business

6.2.10 VENDOR REGISTRATION AND SOLICITATION NOTIFICATION SYSTEM

The NC electronic Vendor Portal (eVP) allows Vendors to electronically register with the State to receive electronic notification of current procurement opportunities for goods and Services available at the following website: https://evp.nc.gov.

This RFP is available electronically on the electronic Vendor Portal ("eVP") at the following website: https://evp.nc.gov.

6.3 INSTRUCTIONS FOR OFFER SUBMISSION

6.3.1 GENERAL INSTRUCTIONS FOR OFFER

Vendors are strongly encouraged to adhere to the following general instructions in order to bring clarity and order to the offer and subsequent evaluation process:

a) Organize the offer in the exact order in which the specifications are presented in the RFP. The Execution page of this RFP must be placed at the front of the Proposal. Each page should be numbered. The offer should contain a table of contents, which cross-references the RFP specification and the specific page of the response in the Vendor's offer.

b) Provide complete and comprehensive responses with a corresponding emphasis on being concise and clear. Elaborate offers in the form of brochures or other presentations beyond that necessary to present a complete and effective offer are not desired.

c) Clearly state your understanding of the problem(s) presented by this RFP including your proposed solution's ability to meet the specifications, including capabilities, features, and limitations, as described herein, and provide a cost offer.

d) Supply all relevant and material information relating to the Vendor's organization, personnel, and experience that substantiates its qualifications and capabilities to perform the Services and/or provide the goods described in this RFP. If relevant and material information is not provided, the offer may be rejected from consideration and evaluation.

e) Furnish all information requested; and if response spaces are provided in this document, the Vendor shall furnish said information in the spaces provided. Further, if required elsewhere in this RFP, each Vendor must submit with its offer sketches, descriptive literature and/or complete specifications covering the products offered. References to literature submitted with a previous offer will not satisfy this provision. Proposals that do not comply with these instructions may be rejected.

f) Any offer that does not adhere to these instructions may be deemed non-responsive and rejected on that basis.

g) **Only information that is received in response to this RFP will be evaluated.** Reference to information previously submitted or Internet Website Addresses (URLs) will not suffice as a response to this solicitation.

6.3.2 OFFER ORGANIZATION

Within each section of its offer, Vendor should address the items in the order in which they appear in this RFP. Forms, attachments or exhibits, if any provided in the RFP, must be completed and included in the appropriate section of the offer. All discussion of offered costs, rates, or expenses must be presented in Section 4.0. Cost of Vendor's Offer.

The offer should be organized and indexed in the following format and should contain, at a minimum, all listed items below.

Signed Execution Page AND all pages of this solicitation document in ONE (1) PDF. This includes:

a) Attachments A and B

b) Completed Description of Vendor Submitting Offer Form (Attachment C)

c) Completed Cost Form (Attachment D)

d) Completed and Signed Vendor Certification Form (Attachment E)

e) Completed Location of Workers Utilized by Vendor Form (Attachment F)

f) Completed References (Attachment G)

g) Completed Financial Review Form (Attachment H)

h) Response to Functional Specifications (Attachment I)

i) Response to Technical Specifications (Attachment J)

j) Completed Key Personnel & Resumes (Attachment K)

k) Completed Staffing Plan (Attachment L)

l) Completed Vendor Experience (Attachment W)

m) Architecture Diagrams

n) Errata and Exceptions if any

o) Vendor's License and Maintenance Agreements if any

p) Vendor may attach other supporting materials that it feels may improve the quality of its response. These materials should be included as items in a separate appendix.

6.3.3 OFFER SUBMITTAL

Due Date: **May 16, 2025**

Time: **3 PM Eastern Standard Time**

IMPORTANT NOTE: It is the Vendor's sole responsibility to upload their offer to the Ariba Sourcing Module by the specified time and date of opening. Vendor shall bear the risk for late electronic submission due to unintended or unanticipated delay, including but not limited to internet issues, network issues, local power outages, or application issues. Vendor must include all the pages of this solicitation in their response.

Sealed offers, subject to the conditions made a part hereof, will be received until 3:00pm Eastern Time on the day of opening and then opened, for furnishing and delivering the commodity as described herein. Offers must be submitted via the Ariba Sourcing Module with the Execution page signed and dated by an official authorized to bind the Vendor's firm. Failure to return a signed offer shall result in disqualification.

Attempts to submit a proposal via facsimile (FAX) machine, telephone, email, email attachments, or in any hardcopy format in response to this Bid SHALL NOT be accepted and will automatically be deemed Non-Responsive.

a) Submit **one (1) signed, original electronic offer** through the Ariba Sourcing Module.
b) The Ariba Sourcing Module document number is: Doc1288967193
c) All File names should start with the Vendor name first, in order to easily determine all the files to be included as part of the vendor's response. For example, files should be named as follows: Vendor Name-your file name.
d) File contents **SHALL NOT** be password protected, the file formats must be in .PDF, .JPEG, .DOC or .XLS format, and shall be capable of being copied to other sources. Inability by the State to open the Vendor's files may result in the Vendor's offer(s) being rejected as Non-Responsive.

e) If the vendor's proposal contains any confidential information (as defined in Attachment B, Section 2, Paragraph #17), then the vendor must provide one (1) signed, original electronic offer and one (1) redacted electronic copy.

For Vendor training on how to use the Ariba Sourcing Tool to view solicitations, submit questions, develop responses, upload documents, and submit offers to the State, Vendors should go to the following site: https://eprocurement.nc.gov/training/vendor-training

Questions or issues related to using the Ariba Sourcing Tool itself can be directed to the North Carolina eProcurement Help Desk at 888-211-7440, Option 2. Help Desk representatives are available Monday through Friday from 7:30 AM EST to 5:00 PM EST

7.0 OTHER REQUIREMENTS AND SPECIAL TERMS

7.1 VENDOR UTILIZATION OF WORKERS OUTSIDE OF U.S.

In accordance with N.C.G.S. §143B-1361(b), the Vendor must detail the manner in which it intends to utilize resources or workers in the RFP response. The State of North Carolina will evaluate the additional risks, costs, and other factors associated with such utilization prior to making an award for any such Vendor's offer.

Complete ATTACHMENT F - Location of Workers Utilized by Vendor and submit with your offer.

7.2 FINANCIAL STATEMENTS

The Vendor shall provide evidence of financial stability by returning with its offer 1) completed Financial Review Form (Attachment H), and 2) copies of Financial Statements as further described hereinbelow. As used herein, Financial Statements shall exclude tax returns and compiled statements.

a) For a publicly traded company, Financial Statements for the past three (3) fiscal years, including at a minimum, income statements, balance sheets, and statement of changes in financial position or cash flows. If three (3) years of financial statements are not available, this information shall be provided to the fullest extent possible, but not less than one year. If less than 3 years, the Vendor must explain the reason why they are not available.

b) For a privately held company, when certified audited financial statements are not prepared: a written statement from the company's certified public accountant stating the financial condition, debt-to-asset ratio for the past three (3) years and any pending actions that may affect the company's financial condition.

c) The State may, in its sole discretion, accept evidence of financial stability other than Financial Statements for the purpose of evaluating Vendors' responses to this RFP. The State reserves the right to determine whether the substitute information meets the requirements for Financial Information sufficiently to allow the State to evaluate the sufficiency of financial resources and the ability of the business to sustain performance of this RFP award. Scope Statements issued may require the submission of Financial Statements and specify the number of years to be provided, the information to be provided, and the most recent date required.

7.3 FINANCIAL RESOURCES ASSESSMENT, QUALITY ASSURANCE, PERFORMANCE AND RELIABILITY

a) Contract Performance Security. The State reserves the right to require performance guaranties pursuant to N.C.G.S. §143B-1340(f) and 09 NCAC 06B.1207 from the Vendor without expense to the State.

The Agency uses a “pay for performance” model in which only stand-alone Deliverables that are complete, of high quality, and fully usable by the Agency will be paid for. As such, the Project billing milestones are constructed to align with tangible deliverables rather than based on dates, labor time, travel, or material reimbursements.

All billable items or Deliverables are “not to exceed” the specified amounts in Attachment D Cost Form.

The Agency shall hold back twenty percent (20%) of each payment for Vendor-delivered and accepted billing milestones by Phase as a contingency fee that will not be paid until completion of each Phase and the relevant release has been implemented into the production environment (“Retainage”).

Commercially available equipment and licenses not proprietary to the Vendor are not subject to Retainage (e.g., Microsoft SQL Server).

Non-production deliverables such as design documents are not subject to Retainage.

In the event the Project is terminated for cause prior to the implementation of a Phase, the Retainage will not be paid. In the event the Project is terminated for convenience prior to the implementation of a Phase, the Retainage withheld to that point will be paid to the Vendor.

The Agency, within its sole discretion, reserves the option to release some amount of the Retainage at any time if Vendor’s performance and quality exceeds expectation.

b) Project Assurance, Performance and Reliability Evaluation – Pursuant to N.C.G.S. §143B-1340, the State CIO may require quality assurance reviews of Projects as necessary.

7.4 VENDOR’S LICENSE OR SUPPORT AGREEMENTS

Vendor should present its license or support agreements for review and evaluation. Terms offered for licensing and support of Vendors’ proprietary assets will be considered.

The terms and conditions of the Vendor’s standard services, license, maintenance or other agreement(s) applicable to Services, Software and other Products acquired under this RFP may apply to the extent such terms and conditions do not materially change the terms and conditions of this RFP. In the event of any conflict between the terms and conditions of this RFP and the Vendor’s standard agreement(s), the terms and conditions of this RFP relating to audit and records, jurisdiction, choice of law, the State’s electronic procurement application of law or administrative rules, the remedy for intellectual property infringement and the exclusive remedies and limitation of liability in the NCDIT Terms and Conditions herein shall apply in all cases and supersede any provisions contained in the Vendor’s relevant standard agreement or any other agreement. The State shall not be obligated under any standard license and/or maintenance or other Vendor agreement(s) to indemnify or hold harmless the Vendor, its licensors, successors or assigns, nor arbitrate any dispute, nor pay late fees, penalties, legal fees or other similar costs.

7.5 RESELLERS

Reserved.

7.6 DISCLOSURE OF LITIGATION

The Vendor’s failure to fully and timely comply with the terms of this section, including providing reasonable assurances satisfactory to the State, may constitute a material breach of the Agreement.

a) The Vendor shall notify the State in its offer, if it, or any of its subcontractors, or their officers, directors, or key personnel who may provide Services under any contract awarded pursuant to this solicitation, have ever been convicted of a felony, or any crime involving moral turpitude, including, but not limited to fraud, misappropriation or deception. The Vendor shall promptly notify the State of

any criminal litigation, investigations or proceeding involving the Vendor or any subcontractor, or any of the foregoing entities' then current officers or directors during the term of the Agreement or any Scope Statement awarded to the Vendor.

b) The Vendor shall notify the State in its offer, and promptly thereafter as otherwise applicable, of any civil litigation, arbitration, proceeding, or judgments against it or its subcontractors during the three (3) years preceding its offer, or which may occur during the term of any awarded to the Vendor pursuant to this solicitation, that involve (1) Services or related goods similar to those provided pursuant to any contract and that involve a claim that may affect the viability or financial stability of the Vendor, or (2) a claim or written allegation of fraud by the Vendor or any subcontractor hereunder, arising out of their business activities, or (3) a claim or written allegation that the Vendor or any subcontractor hereunder violated any federal, state or local statute, regulation or ordinance. Multiple lawsuits and or judgments against the Vendor or subcontractor shall be disclosed to the State to the extent they affect the financial solvency and integrity of the Vendor or subcontractor.

c) All notices under subsection A and B herein shall be provided in writing to the State within thirty (30) calendar days after the Vendor learns about any such criminal or civil matters; unless such matters are governed by the NCDIT Terms and Conditions annexed to the solicitation. Details of settlements which are prevented from disclosure by the terms of the settlement shall be annotated as such. Vendor may rely on good faith certifications of its subcontractors addressing the foregoing, which certifications shall be available for inspection at the option of the State.

7.7 CRIMINAL CONVICTION

In the event the Vendor, an officer of the Vendor, or an owner of a 25% or greater share of the Vendor, is convicted of a criminal offense incident to the application for or performance of a State, public or private Contract or subcontract; or convicted of a criminal offense including but not limited to any of the following: embezzlement, theft, forgery, bribery, falsification or destruction of records, receiving stolen property, attempting to influence a public employee to breach the ethical conduct standards for State of North Carolina employees; convicted under State or federal antitrust statutes; or convicted of any other criminal offense which in the sole discretion of the State, reflects upon the Vendor's business integrity and such vendor shall be prohibited from entering into a contract for goods or Services with any department, institution or agency of the State.

7.8 SECURITY AND BACKGROUND CHECKS

The Agency reserves the right to conduct a security background check or otherwise approve any employee or agent provided by the Vendor, and to refuse access to or require replacement of any such personnel for cause, including, but not limited to, technical or training qualifications, quality of work or change in security status or non-compliance with the Agency's security or other similar requirements.

All State and Vendor personnel (including subcontractors) that have access to Agency Data as defined by the North Carolina Department of Revenue Security Policy Manual (located at http:www.ncdor.gov/documents/files/ncdor-security-policy-manual/open) must have a security background check performed by the Agency. The State reserves the right to check tax compliance.

7.9 ASSURANCES

In the event that criminal or civil investigation, litigation, arbitration or other proceedings disclosed to the State pursuant to this Section, or of which the State otherwise becomes aware, during the term of the Agreement, causes the State to be reasonably concerned about:

a) the ability of the Vendor or its subcontractor to continue to perform the Agreement in accordance with its terms and conditions, or

b) whether the Vendor or its subcontractor in performing Services is engaged in conduct which is similar in nature to conduct alleged in such investigation, litigation, arbitration or other proceedings, which conduct would constitute a breach of the Agreement or violation of law, regulation or public policy, then the Vendor shall be required to provide the State all reasonable assurances requested by the State to demonstrate that: the Vendor or its subcontractors hereunder will be able to continue to perform the Agreement in accordance with its terms and conditions, and the Vendor or its subcontractors will not engage in conduct in performing Services under the Agreement which is similar in nature to the conduct alleged in any such litigation, arbitration or other proceedings.

7.10 CONFIDENTIALITY OF OFFERS

All offers and any other RFP responses shall be made public as required by the NC Public Records Act and GS 143B-1350. Vendors may mark portions of offers as confidential or proprietary, after determining that such information is excepted from the NC Public Records Act, provided that such marking is clear and unambiguous and preferably at the top and bottom of each page containing confidential information. Standard restrictive legends appearing on every page of an offer are not sufficient and shall not be binding upon the State.

Certain State information is not public under the NC Public Records Act and other laws. Any such information which the State designates as confidential and makes available to the Vendor in order to respond to the RFP or carry out the Agreement, or which becomes available to the Vendor in carrying out the Agreement, shall be protected by the Vendor from unauthorized use and disclosure. The Vendor shall not be required under the provisions of this section to keep confidential, (1) information generally available to the public, (2) information released by the State generally, or to the Vendor without restriction, (3) information independently developed or acquired by the Vendor or its personnel without reliance in any way on otherwise protected information of the State. Notwithstanding the foregoing restrictions, the Vendor and its personnel may use and disclose any information which it is otherwise required by law to disclose, but in each case only after the State has been so notified, and has had the opportunity, if possible, to obtain reasonable protection for such information in connection with such disclosure.

7.11 PROJECT MANAGEMENT

All project management and coordination on behalf of the Agency shall be through a single point of contact designated as the Agency Project Manager. The Vendor shall designate a Vendor Project Manager who will provide a single point of contact for management and coordination of the Vendor's work. All work performed pursuant to the Agreement shall be coordinated between the Agency Project Manager and the Vendor Project Manager.

7.12 MEETINGS

The Vendor is required to meet with Agency personnel, or designated representatives, to resolve technical or contractual problems that may occur during the term of the Agreement. Meetings will occur as problems arise and will be coordinated by Agency. The Vendor will be given reasonable and sufficient notice of meeting dates, times, and locations or meeting vehicle (e.g. MS Teams, Webex, etc.).

7.13 RECYCLING AND SOURCE REDUCTION

It is the policy of this State to encourage and promote the purchase of products with recycled content to the extent economically practicable, and to purchase items which are reusable, refillable, repairable, more durable, and less toxic to the extent that the purchase or use is practicable and cost-effective. We also encourage and promote using minimal packaging and the use of recycled/recyclable products in the packaging of goods purchased. However, no sacrifice in quality of packaging will be acceptable. The Vendor remains responsible for providing packaging that will protect the commodity and contain it for its intended use. Vendors are strongly urged to bring to the attention of the purchasers at the NCDIT Statewide IT

Procurement Office those products or packaging they offer which have recycled content and that are recyclable.

7.14 SPECIAL TERMS AND CONDITIONS

7.14.1 Key Personnel

Key Personnel roles are considered essential to the work being performed as defined in this RFP and may not be filled by a subcontractor. Vendor must ensure Key Personnel have and maintain any relevant current license(s) and/or certification(s) prior to assignment on this Program.

Vendors must be committed to minimizing staff turnover throughout the duration of the Contract.

The substitution of Key Personnel is subject to the requirements of Attachment B: Department of Information Technology Terms and Conditions, Section 3, Paragraph 3, Personnel. Vendor will inform the Agency as soon as it is aware a change is required. Any proposed replacements for Key Personnel must have qualifications that meet or exceed those they replace. The Agency must have the opportunity to interview a potential replacement. If possible, replacements will be expected to work alongside the individual he/she is replacing for a minimum transition period of one (1) month, unless a different transition period is agreed upon with the Agency, at no incremental cost to the Agency.

The Vendor will remove and replace personnel, if requested by the Agency, within the agreed upon time but not to exceed one (1) month once the request for removal has been submitted.

7.15 AGENCY TERMS AND CONDITIONS

7.15.1 Staffing Plan

The Vendor will be asked to provide a list of its staff (including subcontractors), staff qualifications, and work experience at the beginning of each implementation phase and at the beginning of production support (Program Personnel List). The Program Personnel List must be updated and shared with the Agency whenever there are personnel changes.

7.15.2 Production Support Services

The Agency shall identify and notify the Vendor of any changes in applicable statutes, regulations, or policies that may directly or indirectly relate to Vendor's performance of the Production Support Services. The Vendor and the Agency shall work together to identify any impact of such changes upon the Agency's use, or Vendor's delivery, of the Production Support Services.

Vendor shall bear all costs and expenses associated with the identification, diagnosis, and remediation of core defects. This includes, but is not limited to, labor, materials, and any third-party services required to resolve the defect. For the purposes of this requirement, "core defects" shall be defined as any defects, errors, or malfunctions in the Vendor's products or services that significantly impair the functionality, performance, or usability of the product or service as intended and specified in the agreed-upon requirements and specifications.

7.15.3 Hosting

NCDOR will provide the Azure environment (subscription) for the ITS. NCDOR will provide all security components including, but not limited to, firewalls, logging, end point protection, and vulnerability patching. The Vendor will be given administrative access to the subscription and will be responsible for implementing all systems and services in that subscription to provide the ITS. The Vendor will work with NCDOR to determine exactly what controls, as prescribed by IRS publication 1075, are the responsibility of the Vendor, the controls that are the responsibility of NCDOR, and what controls, if any, are a shared responsibility.

Any costs associated with the Azure subscription to host the ITS and related security tools will be charged back to the Vendor. The Vendor should ensure that the Offer cost will be sufficient to cover the costs of the Azure ITS subscription.
The intent of this billing arrangement is to allow the Vendor complete flexibility to host the ITS while insulating NCDOR from unpredicted or variable costs. The Vendor can then control both performance and hosting costs for the ITS.

Example:

- NCDOR pays the Vendor for the ITS contract.
- The Vendor implements the ITS in the provided Azure subscription. NCDOR will apply all security tools that are required.
- Microsoft will bill the NCDOR for the cost of the subscription. This cost will be charged back to the Vendor.

Monthly payment terms are Net 30 days after receipt of correct invoice from NCDOR for the Azure subscription. Upon contract award, NCDOR will provide Vendor with the necessary information for payment remittance.

7.15.4 Data Ownership and Access

Data, database instances, and derived data products created, collected, manipulated, or directly purchased as part of an RFP is expected to become the property of the Agency. The Agency is considered the custodian of the data and will determine the use, access, distribution, and other conditions based on appropriate State statutes and regulations.

Licensed and/or copyrighted data will be governed by the terms and conditions identified in the negotiated vendor agreement.

Taxpayer user accounts and public jurisdiction data must not be accessed, except:

a) In the course of data center operations,

b) In response to service or technical issues,

c) As required by the express terms of the Contract, including as necessary to perform the services hereunder or

d) At Agency's written request.

7.15.5 Tax Laws and Statutes

The proposed solution must be designed and implemented so that all technical and business functionalities and capabilities comply with all applicable federal laws, and NC general statutes (that include but are not limited to those outlined in Attachment V: NC Statutory References). In the event of a conflict between Vendor and the Agency's interpretation of the relevant legal statutes, the Agency's interpretation and administration will prevail for purposes of system design.

7.15.6 IRS Publication 1075

The proposed solution must be designed and implemented to meet the safeguarding guidelines of Internal Revenue Service ("IRS") Publication 1075, including any amendments or revisions. In the event of a conflict between Vendor and Agency's interpretation of IRS Publication 1075, Agency's interpretation will prevail for purposes of system design.

7.15.7 Streamlined Sales Tax

North Carolina has adopted the Sales and Use tax simplification and uniformity measures outlined in the Streamlined Sales and Use Tax Agreement. The proposed solution must comply with guidelines set out by the Streamlined Sales Tax Governing Board (https://streamlinedssalestax.org) for administering Sales and Use tax obligations of remote sellers.

7.15.8 International Fuel Tax Agreement (IFTA)

The proposed solution must support guidelines of the International Fuel Tax Agreement ("IFTA") as outlined in the IFTA Audit Manual and IFTA Procedures Manual for the administration of motor fuel use taxation as maintained by the International Fuel Tax Association Inc. (https://iftach.org).

7.15.9 Certification and Accreditation (C&A)

The selected vendor will be the Technical Owner (as defined in Attachment S) of the proposed solution for purposes of the Agency's Certification and Accreditation Process ("C&A Process") and must comply with the C&A Process described in Attachment S: NCDOR Certification and Accreditation Process. The vendor must also adhere to the policy described in Attachment R: NCDOR IT Division Certification & Accreditation Policy.

7.15.10 IT Security Requirements

The Agency stores, processes and transmits data of many different classifications with differing regulatory authorities and requirements. As a result, the Agency secures all data, other than data classified as "public" by the Agency Chief Data Officer, using the standards set forth in IRS Publication 1075. This standard is based on NIST 800-53 moderate level controls and is augmented by additional requirements from the US Department of Treasury.

For any system that will store, process or transmit Agency data, it must be compliant with all parts of the most current version of IRS Publication 1075. To ensure the system is compliant with these requirements, the Agency IT Division uses a Certification & Accreditation (C&A) process. This process, once successfully completed, results in the system being provided an Authorization to Operate (ATO) by the Agency Chief Information Officer (CIO).

The Vendor must work closely with the Agency Architects, Agency Chief Information Security Officer ("CISO") and Agency Governance, Risk, and Compliance Manager, or their delegates, to successfully complete the C&A process.

See Attachment R: NCDOR IT Division Certification & Accreditation Policy and Attachment S: NCDOR Certification and Accreditation Process.

7.15.11 Internal Revenue Service Publication 1075, Exhibit 7 Contracting Language

Vendor will be required to comply with the data safeguarding requirements in Exhibit 7 Safeguarding Language for Contracts, attached as Attachment T: Internal Revenue Service Publication 1075, Exhibit 7 Safeguarding Contract Language.

Prior to accessing any Agency Data, Vendor will be required to complete any applicable security requirements outlined in Attachment U: Security Requirements for Vendor Staff and Contractors. The Agency will work with the vendor to determine the appropriate security requirements based on the level of access the Vendor will require to perform services under this contract.

8.0 LIST OF ATTACHMENTS & EXHIBITS

- Attachment A: Definitions (No Response Required)
- Attachment B: Department of Information Technology Terms and Conditions
- Attachment C: Description of Vendor

- Attachment D: Cost Form
- Attachment E: Vendor Certification Form
- Attachment F: Location of Workers Utilized by Vendor
- Attachment G: References
- Attachment H: Financial Review Form
- Attachment I: Functional Specifications Matrix
- Attachment J: Technical Specifications Matrix
- Attachment K: Key Personnel & Resumes
- Attachment L: Staffing Plan
- Attachment M: Tax Schedule Matrix (No Response Required)
- Attachment N: Forms Inventory (No Response Required)
- Attachment O: Systems Inventory (No Response Required)
- Attachment P: Interfaces Inventory (No Response Required)
- Attachment Q: Implementation Roles & Responsibilities (No Response Required)
- Attachment R: NCDOR IT Division Certification & Accreditation Policy (No Response Required)
- Attachment S: NCDOR Certification and Accreditation Process (No Response Required)
- Attachment T: Internal Revenue Service Publication 1075, Exhibit 7 Safeguarding Contract Language (No Response Required)
- Attachment U: Security Requirements for Vendor Staff and Contractors (No Response Required)
- Attachment V: NC Statutory References (No Response Required)
- Attachment W: Vendor Experience

ATTACHMENT A: DEFINITIONS

1) **24x7:** A statement of availability of systems, communications, and/or supporting resources every hour (24) of each day (7 days weekly) throughout every year for periods specified herein. Where reasonable downtime is accepted, it will be stated herein. Otherwise, 24x7 implies NO loss of availability of systems, communications, and/or supporting resources.
2) **Budget Code:** Five-digit number assigned by the NC Office of State Budget and Management (OSBM) for budgetary reporting. Budget code identifies major fund types and the responsible entity for reporting.
3) **Cybersecurity Incident (GS 143B-1320):** An occurrence that:
    a. Actually, or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or
    b. Constitutes a violation or imminent threat of violation of law, security policies, privacy policies, security procedures, or acceptable use policies.
4) **Deliverables**: Deliverables, as used herein, shall comprise all Hardware, Vendor Services, professional Services, Software and provided modifications to any Software, and incidental materials, including any goods, Software or Services access license, data, reports and documentation provided or created during the performance or provision of Services hereunder. Deliverables include “Work Product” and means any expression of Licensor’s findings, analyses, conclusions, opinions, recommendations, ideas, techniques, know-how, designs, programs, enhancements, and other technical information; but not source and object code or software.
5) **Distribution:** Funds disbursed to local governments, municipalities, and/or local law enforcement entities per statute.
6) **Goods**: Includes intangibles such as computer software; provided, however that this definition does not modify the definition of “goods” in the context of N.C.G.S. §25-2-105 (UCC definition of goods).
7) **ITAS**: Integrated Tax Administration System. NCDOR legacy mainframe system for processing the majority of tax schedules.
8) **ITS**: Integrated Tax System. Modernized tax system offered in response to this Request for Proposal.
9) **GRC**: Governance Risk and Compliance. Group within Information Technology that comprises Integrated Risk Management, Business Continuity Management and Privacy Management with a primary focus on ensuring IT systems are in compliance with IRS Publication 1075.
10) **Major Change:** Substantial transformation with high risk that significantly impacts the organization and requires extensive assessment, planning and stakeholder engagement.
11) **NCDIT:** The NC Department of Information Technology.
12) **NCDOR:** The NC Department of Revenue.
13) **Open Market Contract:** A contract for the purchase of goods or Services not covered by a term, technical, or convenience contract.
14) **Reasonable, Necessary or Proper**: as used herein shall be interpreted solely by the State of North Carolina.
15) **Request for Proposal (RFP):** The RFP is a formal, written solicitation document typically used for seeking competition and obtaining offers for more complex services or a combination of goods and services. The RFP is used when the value is over $10,000. This document contains specifications of the RFP, instructions to bidders and the standard IT Terms and Conditions for Goods and Related Services. User should add Supplemental Terms and Conditions for Software and Services, when applicable.

16) **Security Breach G.S. §75-61**: An incident of unauthorized access to an acquisition of unencrypted and unredacted records or data containing personal information where illegal use of the personal information has occurred or is reasonably likely to occur or that creates a material risk of harm to a consumer. Any incident of unauthorized access to and acquisition of encrypted records or data containing personal information along with the confidential process or key shall constitute a security breach. Good faith acquisition of personal information by an employee or agent of the business for a legitimate purpose is not a security breach, provided that the personal information is not used for a purpose other than a lawful purpose of the business and is not subject to further unauthorized disclosure.

17) **Significant Security Incident (GS 143B-1320):** A cybersecurity incident that is likely to result in demonstrable harm to the State's security interests, economy, critical infrastructure, or to the public confidence, civil liberties, or public health and safety of the residents of North Carolina. A significant cybersecurity incident is determined by the following factors:

    a. Incidents that meet thresholds identified by the Department jointly with the Department of Public Safety that involve information:

        i. That is not releasable to the public and that is restricted or highly restricted according to Statewide Data Classification and Handling Policy; or

        ii. That involves the exfiltration, modification, deletion, or unauthorized access, or lack of availability to information or systems within certain parameters to include (i) a specific threshold of number of records or users affected as defined in G.S. 75-65 or (ii) any additional data types with required security controls.

    b. Incidents that involve information that is not recoverable or cannot be recovered within defined timelines required to meet operational commitments defined jointly by the State agency and the Department or can be recovered only through additional measures and has a high or medium functional impact to the mission of an agency.

18) **SSP: System Security Plan:** Also referred to as a Safeguard Security Report by the IRS, this document is the primary source for agencies to report to the IRS Office of Safeguards on processes, procedures and security controls in place to protect Federal Tax Information in compliance with IRC 6103(p)(4). Agencies executing data exchange agreements involving access to FTI and subject to safeguarding requirements must have an approved SSR prior to having access to FTI. Section 2.E.4 of IRS Publication 1075 outlines SSR Reporting Requirements for 6103(p)(4)(E).

19) **Transfer:** Funds disbursed to other state entities per statute.

20) **Unidentified money:** Money received in which the taxpayer and/or the tax type to which the payment should be applied is unknown.

21) **Vendor:** Company, firm, corporation, partnership, individual, etc., submitting an offer in response to a solicitation.

ATTACHMENT B: DEPARTMENT OF INFORMATION TECHNOLOGY TERMS AND CONDITIONS

Section 1. General Terms and Conditions Applicable to All Purchases

1) **DEFINITIONS:** As used herein;

   Agreement means the contract awarded pursuant to this RFP.

   Deliverable/Product Warranties shall mean and include the warranties provided for products or deliverables licensed to the State in Section 2, Paragraph 2 of these Terms and Conditions unless superseded by a Vendor's Warranties pursuant to Vendor's License or Support Agreements.

   Purchasing State Agency or Agency shall mean the Agency purchasing the goods or Services.

   Services shall mean the duties and obligations undertaken by the Vendor under, and to fulfill, the specifications, requirements, terms and conditions of the Agreement.

   State shall mean the State of North Carolina, the Department of Information Technology (NCDIT), or the Purchasing State Agency in its capacity as the Contracting Agency, as appropriate.

2) **STANDARDS:** Any Deliverables shall meet all applicable State and federal requirements, such as State or Federal Regulation, and NC State Chief Information Officer's (CIO) policy or regulation. Vendor will provide and maintain a quality assurance system or program that includes any Deliverables and will tender or provide to the State only those Deliverables that have been inspected and found to conform to the RFP specifications. All Deliverables are subject to operation, certification, testing and inspection, and any accessibility specifications.

3) **WARRANTIES:** Unless otherwise expressly provided, any goods Deliverables provided by the Vendor shall be warranted for a period of 90 days after acceptance.

4) **SUBCONTRACTING:** The Vendor may subcontract the performance of required Services with Resources under the Agreement only with the prior written consent of the State contracting authority. Vendor shall provide the State with complete copies of any agreements made by and between Vendor and all subcontractors. The selected Vendor remains solely responsible for the performance of its subcontractors. Subcontractors, if any, shall adhere to the same standards required of the selected Vendor and the Agreement. Any contracts made by the Vendor with a subcontractor shall include an affirmative statement that the State is an intended third party beneficiary of the Agreement; that the subcontractor has no agreement with the State; and that the State shall be indemnified by the Vendor for any claim presented by the subcontractor. Notwithstanding any other term herein, Vendor shall timely exercise its contractual remedies against any non-performing subcontractor and, when appropriate, substitute another subcontractor.

5) **TRAVEL EXPENSES: All travel expenses should be included in the Vendor's proposed costs. Separately stated travel expenses will not be reimbursed**. In the event that the Vendor, upon specific request in writing by the State, is deemed eligible to be reimbursed for travel expenses arising under the performance of the Agreement, reimbursement will be at the out-of-state rates set forth in N.C.G.S. §138-6; as amended from time to time. Vendor agrees to use the lowest available airfare not requiring a weekend stay and to use the lowest available rate for rental vehicles. All Vendor incurred travel expenses shall be billed on a monthly basis, shall be supported by receipt and shall be paid by the State within thirty (30) days after invoice approval. Travel expenses exceeding the foregoing rates shall not be paid by the State. The State will reimburse travel allowances only for days on which the Vendor is required to be in North Carolina performing Services under the Agreement.

6) **GOVERNMENTAL RESTRICTIONS:** In the event any restrictions are imposed by governmental requirements that necessitate alteration of the material, quality, workmanship, or performance of the Deliverables offered prior to delivery thereof, the Vendor shall provide written notification of the necessary alteration(s) to the Agency Contract Administrator. The State reserves the right to accept any such alterations, including any price adjustments occasioned thereby, or to cancel the Agreement. The State

may advise Vendor of any restrictions or changes in specifications required by North Carolina legislation, rule or regulatory authority that require compliance by the State. In such event, Vendor shall use its best efforts to comply with the required restrictions or changes. If compliance cannot be achieved by the date specified by the State, the State may terminate the Agreement and compensate Vendor for sums then due under the Agreement.

7) **PROHIBITION AGAINST CONTINGENT FEES AND GRATUITIES:** Vendor warrants that it has not paid, and agrees not to pay, any bonus, commission, fee, or gratuity to any employee or official of the State for the purpose of obtaining any Contract or award issued by the State. Vendor further warrants that no commission or other payment has been or will be received from or paid to any third party contingent on the award of any Contract by the State, except as shall have been expressly communicated to the State Purchasing Agent in writing prior to acceptance of the Agreement or award in question. Each individual signing below warrants that he or she is duly authorized by their respective Party to sign the Agreement and bind the Party to the terms and conditions of this RFP. Vendor and their authorized signatory further warrant that no officer or employee of the State has any direct or indirect financial or personal beneficial interest, in the subject matter of the Agreement; obligation or Contract for future award of compensation as an inducement or consideration for making the Agreement. Subsequent discovery by the State of non-compliance with these provisions shall constitute sufficient cause for immediate termination of all outstanding contracts. Violations of this provision may result in debarment of the Vendor(s) as permitted by 9 NCAC 06B..1206, or other provision of law.

8) **AVAILABILITY OF FUNDS:** Any and all payments to Vendor are expressly contingent upon and subject to the appropriation, allocation and availability of funds to the Agency for the purposes set forth in the Agreement. If the Agreement or any Purchase Order issued hereunder is funded in whole or in part by federal funds, the Agency's performance and payment shall be subject to and contingent upon the continuing availability of said federal funds for the purposes of the Agreement or Purchase Order. If the term of the Agreement extends into fiscal years subsequent to that in which it is approved, such continuation of the Agreement is expressly contingent upon the appropriation, allocation and availability of funds by the N.C. Legislature for the purposes set forth in this RFP. If funds to effect payment are not available, the Agency will provide written notification to Vendor. If the Agreement is terminated under this paragraph, Vendor agrees to take back any affected Deliverables and software not yet delivered under the Agreement, terminate any Services supplied to the Agency under the Agreement, and relieve the Agency of any further obligation thereof. The State shall remit payment for Deliverables and Services accepted prior to the date of the aforesaid notice in conformance with the payment terms.

9) **ACCEPTANCE PROCESS:**
   a) The State shall have the obligation to notify Vendor, in writing within thirty (30) calendar days following provision, performance (under a provided milestone or otherwise as agreed) or delivery of any Services or other Deliverables described in the Agreement that are not acceptable.
   b) Acceptance testing is required for all Vendor supplied software and software or platform services unless provided otherwise in the solicitation documents or a Statement of Work. The State may define such processes and procedures as may be necessary or proper, in its opinion and discretion, to ensure compliance with the State's specifications, and Vendor's Product Warranties and technical representations. The State shall have the obligation to notify Vendor, in writing and within thirty (30) days prior to production cutover of an individual Phase if it is not acceptable.
   c) Acceptance of Services or other Deliverables including software or platform services may be controlled by an amendment hereto, or additional terms as agreed by the Parties consistent with IT Project management under GS §143B-1340.
   d) The notice of non-acceptance shall specify in reasonable detail the reason(s) a Service or given Deliverable is unacceptable. Acceptance by the State shall not be unreasonably withheld; but may be conditioned or delayed as required for installation and/or testing of Deliverables. Final acceptance is expressly conditioned upon completion of any applicable inspection and testing procedures. Should a Service or Deliverable fail to meet any specifications or acceptance criteria, the State may exercise any and all rights hereunder. Services or Deliverables discovered to be defective or failing to conform

to the specifications may be rejected upon initial inspection or at any later time if the defects or errors contained in the Services or Deliverables or non-compliance with the specifications were not reasonably ascertainable upon initial inspection. If the Vendor fails to promptly cure or correct the defect or replace or re-perform the Services or Deliverables, the State reserves the right to cancel the Purchase Order, contract with a different Vendor, and to invoice the original Vendor for any differential in price over the original Contract price.

10) **PAYMENT TERMS:** The total License Fee and the Support Service or Maintenance Fee (If applicable and provided the State subscribes or purchases such Services) for the first year shall be invoiced upon delivery of the Software. The Support Service or Maintenance Fee for subsequent contract years, if any will be invoiced annually sixty days prior to the anniversary date beginning each subsequent year. Increases in pricing for Support Services or Maintenance shall not exceed five percent (5%) per year following the first Contract Year. Payment terms are Net 30 days after receipt of correct invoice (with completed timesheets for Vendor personnel) and acceptance of one or more of the Deliverables, under milestones or otherwise as may be provided in Paragraph 9 (Acceptance), or elsewhere in this solicitation, unless a period of more than thirty (30) days is required by the Agency. Monthly Payment terms for Deliverables are Net 30 days after receipt of correct invoice (with completed timesheets for Vendor personnel) and acceptance of one or more of the Deliverables, under milestones or otherwise as may be provided in Paragraph 9 (Acceptance), or elsewhere in this solicitation, unless a period of more than thirty (30) days is required by the Agency. The Purchasing State Agency is responsible for all payments under the Agreement. No additional charges to the Agency will be permitted based upon, or arising from, the Agency's use of a Business Procurement Card. The State may exercise any and all rights of Set Off as permitted in Chapter 105A-1 *et. seq*. of the N.C. General Statutes and applicable Administrative Rules. Upon Vendor's written request of not less than thirty (30) days and approval by the State or Agency, the Agency may:
    a) Forward the Vendor's payment check(s) directly to any person or entity designated by the Vendor, or
    b) Include any person or entity designated in writing by Vendor as a joint payee on the Vendor's payment check(s), however
    c) In no event shall such approval and action obligate the State to anyone other than the Vendor and the Vendor shall remain responsible for fulfillment of all Contract obligations.
11) **EQUAL EMPLOYMENT OPPORTUNITY:** Vendor shall comply with all Federal and State requirements concerning fair employment and employment of the disabled, and concerning the treatment of all employees without regard to discrimination by reason of race, color, religion, sex, national origin or physical disability.
12) **ADVERTISING/PRESS RELEASE:** The Vendor absolutely shall not publicly disseminate any information concerning the Agreement without prior written approval from the State or its Agent. For the purpose of this provision of the Agreement, the Agent is the Purchasing Agency Contract Administrator unless otherwise named in the solicitation documents.
13) **LATE DELIVERY:** Vendor shall advise the Agency contact person or office immediately upon determining that any Deliverable will not, or may not, be delivered or performed at the time or place specified. Together with such notice, Vendor shall state the projected delivery time and date. In the event the delay projected by Vendor is unsatisfactory, the Agency shall so advise Vendor and may proceed to procure the particular substitute Services or other Deliverables.
14) **ACCESS TO PERSONS AND RECORDS:** Pursuant to N.C.G.S. §147-64.7, the Agency, the State Auditor, appropriate federal officials, and their respective authorized employees or agents are authorized to examine all books, records, and accounts of the Vendor insofar as they relate to transactions with any department, board, officer, commission, institution, or other agency of the State of North Carolina pursuant to the performance of the Agreement or to costs charged to the Agreement. The Vendor shall retain any such books, records, and accounts for a minimum of three (3) years after the completion of the Agreement. Additional audit or reporting requirements may be required by any Agency, if in the Agency's opinion, such requirement is imposed by federal or state law or regulation. The Joint Legislative Commission on Governmental Operations and the legislative employees whose primary responsibility is to provide

professional or administrative services to the Commission may audit the records of the Vendor during and after the term of this Agreement to verify accounts and data affecting fees or performance in accordance with Chapter 120, Article 13.

15) **ASSIGNMENT:** Vendor may not assign the Agreement or its obligations hereunder except as permitted by 09 NCAC 06B.1003 and this Paragraph. Vendor shall provide reasonable notice of not less than thirty (30) days prior to any consolidation, acquisition, or merger. Any assignee shall affirm the Agreement attorning and agreeing to the terms and conditions agreed, and that Vendor shall affirm that the assignee is fully capable of performing all obligations of Vendor under the Agreement. An assignment may be made, if at all, in writing by the Vendor, Assignee and the State setting forth the foregoing obligation of Vendor and Assignee.

16) **INSURANCE COVERAGE:** During the term of the Agreement, the Vendor at its sole cost and expense shall provide commercial insurance of such type and with such terms and limits as may be reasonably associated with the Agreement. As a minimum, the Vendor shall provide and maintain the following coverage and limits:
   a) **Worker's Compensation** - The Vendor shall provide and maintain Worker's Compensation Insurance, as required by the laws of North Carolina, as well as employer's liability coverage with minimum limits of $100,000.00, covering all of Vendor's employees who are engaged in any work under the Agreement. If any work is sublet, the Vendor shall require the subcontractor to provide the same coverage for any of his employees engaged in any work under the Agreement; and
   b) **Commercial General Liability** - General Liability Coverage on a Comprehensive Broad Form on an occurrence basis in the minimum amount of $2,000,000.00 Combined Single Limit (Defense cost shall be in excess of the limit of liability); and
   c) **Automobile** - Automobile Liability Insurance, to include liability coverage, covering all owned, hired and non-owned vehicles, used in connection with the Agreement. The minimum combined single limit shall be $500,000.00 bodily injury and property damage; $500,000.00 uninsured/under insured motorist; and $5,000.00 medical payment; and
   d) Providing and maintaining adequate insurance coverage described herein is a material obligation of the Vendor and is of the essence of the Agreement. All such insurance shall meet all laws of the State of North Carolina. Such insurance coverage shall be obtained from companies that are authorized to provide such coverage and that are authorized by the Commissioner of Insurance to do business in North Carolina. The Vendor shall at all times comply with the terms of such insurance policies, and all requirements of the insurer under any such insurance policies, except as they may conflict with existing North Carolina laws or the Agreement. The limits of coverage under each insurance policy maintained by the Vendor shall not be interpreted as limiting the Vendor's liability and obligations under the Agreement.

17) **DISPUTE RESOLUTION:** The parties agree that it is in their mutual interest to resolve disputes informally. A claim by the Vendor shall be submitted in writing to the Agency Contract Administrator for decision. A claim by the State shall be submitted in writing to the Vendor's Contract Administrator for decision. The Parties shall negotiate in good faith and use all reasonable efforts to resolve such dispute(s). During the time the Parties are attempting to resolve any dispute, each shall proceed diligently to perform their respective duties and responsibilities under the Agreement. If a dispute cannot be resolved between the Parties within thirty (30) days after delivery of notice, either Party may elect to exercise any other remedies available under the Agreement, or at law. This term shall not constitute an agreement by either party to mediate or arbitrate any dispute.

18) **CONFIDENTIALITY:** In accordance with N.C.G.S. §§ 143B-1350(e) and 143B-1375, and 09 NCAC 06B.0103 and 06B.1001, the State may maintain the confidentiality of certain types of information described in N.C.G.S. §132-1 *et seq*. Such information may include trade secrets defined by N.C.G.S. §66-152 and other information exempted from the Public Records Act pursuant to N.C.G.S. §132-1.2. Vendor may designate appropriate portions of its response as confidential, consistent with and to the extent permitted under the Statutes and Rules set forth above, by marking the top and bottom of pages containing confidential information with a legend in boldface type "**CONFIDENTIAL**". By so marking any

page, the Vendor warrants that it has formed a good faith opinion, having received such necessary or proper review by counsel and other knowledgeable advisors that the portions marked confidential meet the requirements of the Rules and Statutes set forth above. ***However, under no circumstances shall price information be designated as confidential.*** The State may serve as custodian of Vendor's confidential information and not as an arbiter of claims against Vendor's assertion of confidentiality. If an action is brought pursuant to N.C.G.S. §132-9 to compel the State to disclose information marked confidential, the Vendor agrees that it will intervene in the action through its counsel and participate in defending the State, including any public official(s) or public employee(s). The Vendor agrees that it shall hold the State and any official(s) and individual(s) harmless from any and all damages, costs, and attorneys' fees awarded against the State in the action. The State agrees to promptly notify the Vendor in writing of any action seeking to compel the disclosure of Vendor's confidential information. The State shall have the right, at its option and expense, to participate in the defense of the action through its counsel. The State shall have no liability to Vendor with respect to the disclosure of Vendor's confidential information ordered by a court of competent jurisdiction pursuant to N.C.G.S. §132-9 or other applicable law.

a) Care of Information: Vendor agrees to use commercial best efforts to safeguard and protect any data, documents, files, and other materials received from the State or the Agency during performance of any contractual obligation from loss, destruction or erasure. Vendor agrees to abide by all facilities and security requirements and policies of the agency where work is to be performed. Any Vendor personnel shall abide by such facilities and security requirements and shall agree to be bound by the terms and conditions of the Agreement.
b) Vendor warrants that all its employees and any approved third party Vendors or subcontractors are subject to a non-disclosure and confidentiality agreement enforceable in North Carolina. Vendor will, upon request of the State, verify and produce true copies of any such agreements. Production of such agreements by Vendor may be made subject to applicable confidentiality, non-disclosure or privacy laws; provided that Vendor produces satisfactory evidence supporting exclusion of such agreements from disclosure under the N.C. Public Records laws in N.C.G.S. §132-1 *et seq*. The State may, in its sole discretion, provide a non-disclosure and confidentiality agreement satisfactory to the State for Vendor's execution. The State may exercise its rights under this subparagraph as necessary or proper, in its discretion, to comply with applicable security regulations or statutes including, but not limited to 26 USC 6103 and IRS Publication 1075, (Tax Information Security Guidelines for Federal, State, and Local Agencies), HIPAA, 42 USC 1320(d) (Health Insurance Portability and Accountability Act), any implementing regulations in the Code of Federal Regulations, and any future regulations imposed upon the Department of Information Technology or the N.C. Department of Revenue pursuant to future statutory or regulatory requirements.
c) Nondisclosure: Vendor agrees and specifically warrants that it, its officers, directors, principals and employees, and any subcontractors, shall hold all information received during performance of the Agreement in the strictest confidence and shall not disclose the same to any third party without the express written approval of the State.
d) The Vendor shall protect the confidentiality of all information, data, instruments, studies, reports, records and other materials provided to it by the Agency or maintained or created in accordance with this Agreement. No such information, data, instruments, studies, reports, records and other materials in the possession of Vendor shall be disclosed in any form without the prior written consent of the State Agency. The Vendor will have written policies governing access to and duplication and dissemination of all such information, data, instruments, studies, reports, records and other materials.
e) All project materials, including software, data, and documentation created during the performance or provision of Services hereunder that are not licensed to the State or are not proprietary to the Vendor are the property of the State of North Carolina and must be kept confidential or returned to the State, or destroyed. Proprietary Vendor materials shall be identified to the State by Vendor prior to use or provision of Services hereunder and shall remain the property of the Vendor. Derivative works of any

Vendor proprietary materials prepared or created during the performance of provision of Services hereunder shall be subject to a perpetual, royalty free, nonexclusive license to the State.

19) **DEFAULT:** In the event Services or other Deliverable furnished or performed by the Vendor during performance of any Contract term fail to conform to any material requirement(s) of the Contract specifications, notice of the failure is provided by the State and if the failure is not cured within ten (10) days, or Vendor fails to meet the requirements of Paragraph 9) herein, the State may cancel the contract. Default may be cause for debarment as provided in 09 NCAC 06B.1206. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the Contract.
    a) If Vendor fails to deliver or provide correct Services or other Deliverables within the time required by the Agreement, the State shall provide written notice of said failure to Vendor, and by such notice require performance assurance measures pursuant to N.C.G.S. 143B-1340(f). Vendor is responsible for the delays resulting from its failure to deliver or provide services or other Deliverables.
    b) Should the State fail to perform any of its obligations upon which Vendor's performance is conditioned, Vendor shall not be in default for any delay, cost increase or other consequences resulting from the State's failure. Vendor will use reasonable efforts to mitigate delays, costs or expenses arising from assumptions in the Vendor's offer documents that prove erroneous or are otherwise invalid. Any deadline that is affected by any such failure in assumptions or performance by the State shall be extended by an amount of time reasonably necessary to compensate for the effect of such failure.
    c) Vendor shall provide a plan to cure any delay or default if requested by the State. The plan shall state the nature of the delay or default, the time required for cure, any mitigating factors causing or tending to cause the delay or default, and such other information as the Vendor may deem necessary or proper to provide.
    d) If the prescribed acceptance testing stated in the Solicitation Documents or performed pursuant to Paragraph 9) of the NCDIT Terms and Conditions is not completed successfully, the State may request substitute Software, cancel the portion of the Contract that relates to the unaccepted Software, or continue the acceptance testing with or without the assistance of Vendor. These options shall remain in effect until such time as the testing is successful or the expiration of any time specified for completion of the testing. If the testing is not completed after exercise of any of the State's options, the State may cancel any portion of the contract related to the failed Software and take action to procure substitute software. If the failed software (or the substituted software) is an integral and critical part of the proper completion of the work for which the Deliverables identified in the solicitation documents or statement of work were acquired, the State may terminate the entire contract.

20) **WAIVER OF DEFAULT:** Waiver by either party of any default or breach by the other Party shall not be deemed a waiver of any subsequent default or breach and shall not be construed to be a modification or novation of the terms of the Agreement, unless so stated in writing and signed by authorized representatives of the Agency and the Vendor, and made as an amendment to the Agreement pursuant to Paragraph 40) herein below.

21) **TERMINATION:** Any notice or termination made under the Agreement shall be transmitted via US Mail, Certified Return Receipt Requested. The period of notice for termination shall begin on the day the return receipt is signed and dated.
    a) The parties may mutually terminate the Agreement by written agreement at any time.
    b) The State may terminate the Agreement, in whole or in part, pursuant to Paragraph 19), or pursuant to the Special Terms and Conditions in the Solicitation Documents, if any, or for any of the following:
        i) Termination for Cause: In the event any goods, software, or service furnished by the Vendor during performance of any Contract term fails to conform to any material requirement of the Contract, and the failure is not cured within the specified time after providing written notice thereof to Vendor, the State may cancel and procure the articles or Services from other sources; holding Vendor liable for any excess costs occasioned thereby, subject only to the limitations provided in Paragraphs 22) and 23) herein. The rights and remedies of the State provided above shall not be exclusive and are in addition to any other rights and remedies provided by law or under the

Contract. Vendor shall not be relieved of liability to the State for damages sustained by the State arising from Vendor's breach of the Agreement; and the State may, in its discretion, withhold any payment due as a setoff until such time as the damages are finally determined or as agreed by the parties. Voluntary or involuntary Bankruptcy or receivership by Vendor shall be cause for termination.

ii) Termination For Convenience Without Cause: The State may terminate service and indefinite quantity contracts, in whole or in part by giving thirty (30) days prior notice in writing to the Vendor. Vendor shall be entitled to sums due as compensation for Deliverables provided and Services performed in conformance with the Contract. In the event the Contract is terminated for the convenience of the State the Agency will pay for all work performed and products delivered in conformance with the Contract up to the date of termination.

iii) Consistent failure to participate in problem resolution meetings, two (2) consecutive missed or rescheduled meetings, or failure to make a good faith effort to resolve problems, may result in termination of the Agreement.

22) LIMITATION OF VENDOR'S LIABILITY:

a) Where Deliverables are under the State's exclusive management and control, the Vendor shall not be liable for direct damages caused by the State's failure to fulfill any State responsibilities of assuring the proper use, management and supervision of the Deliverables and programs, audit controls, operating methods, office procedures, or for establishing all proper checkpoints necessary for the State's intended use of the Deliverables. Vendor shall not be responsible for any damages that arise from (i) misuse or modification of Vendor's Software by or on behalf of the State, (ii) the State's failure to use corrections or enhancements made available by Vendor, (iii) the quality or integrity of data from other automated or manual systems with which the Vendor's Software interfaces, (iv) errors in or changes to third party software or hardware implemented by the State or a third party (including the vendors of such software or hardware) that is not a subcontractor of Vendor or that is not supported by the Deliverables, or (vi) the operation or use of the Vendor's Software not in accordance with the operating procedures developed for the Vendor's Software or otherwise in a manner not contemplated by this Agreement.

b) The Vendor's liability for damages to the State arising under the contract shall be limited to two (2) times the value of the Contract.

c) The foregoing limitation of liability shall not apply to claims covered by other specific provisions including but not limited to Service Level Agreement or Deliverable/Product Warranties pursuant to Section II, 2) of these Terms and Conditions, or to claims for injury to persons or damage to tangible personal property, gross negligence or willful or wanton conduct. This limitation of liability does not apply to contributions among joint tortfeasors under N.C.G.S. 1B-1 *et seq.*, the receipt of court costs or attorney's fees that might be awarded by a court in addition to damages after litigation based on the Agreement. For avoidance of doubt, the Parties agree that the Service Level Agreement and Deliverable/Product Warranty Terms in the Contract are intended to provide the sole and exclusive remedies available to the State under the Contract for the Vendor's failure to comply with the requirements stated therein.

23) VENDOR'S LIABILITY FOR INJURY TO PERSONS OR DAMAGE TO PROPERTY:

a) The Vendor shall be liable for damages arising out of personal injuries and/or damage to real or tangible personal property of the State, employees of the State, persons designated by the State for training, or person(s) other than agents or employees of the Vendor, designated by the State for any purpose, prior to, during, or subsequent to delivery, installation, acceptance, and use of the Deliverables either at the Vendor's site or at the State's place of business, provided that the injury or damage was caused by the fault or negligence of the Vendor.

b) The Vendor agrees to indemnify, defend and hold the Agency and the State and its Officers, employees, agents and assigns harmless from any liability relating to personal injury or injury to real or personal property of any kind, accruing or resulting to any other person, firm or corporation furnishing or supplying work, Services, materials or supplies in connection with the performance of the

Agreement, whether tangible or intangible, arising out of the ordinary negligence, wilful or wanton negligence, or intentional acts of the Vendor, its officers, employees, agents, assigns or subcontractors.

c) Vendor shall not be liable for damages arising out of or caused by an alteration or an attachment not made or installed by the Vendor.

24) TIME IS OF THE ESSENCE: Time is of the essence in the performance of the Agreement.

25) DATE AND TIME WARRANTY: The Vendor warrants that any Deliverable, whether Services, hardware, firmware, middleware, custom or commercial software, or internal components, subroutines, and interface therein which performs, modifies or affects any date and/or time data recognition function, calculation, or sequencing, will still enable the modified function to perform accurate date/time data and leap year calculations. This warranty shall survive termination or expiration of the Contract.

26) INDEPENDENT CONTRACTORS: Vendor and its employees, officers and executives, and subcontractors, if any, shall be independent Vendors and not employees or agents of the State. The Agreement shall not operate as a joint venture, partnership, trust, agency or any other similar business relationship.

27) TRANSPORTATION: Transportation of any tangible Deliverables shall be FOB Destination; unless otherwise specified in the solicitation document or purchase order. Freight, handling, hazardous material charges, and distribution and installation charges shall be included in the total price of each item. Any additional charges shall not be honored for payment unless authorized in writing by the Purchasing State Agency. In cases where parties, other than the Vendor ship materials against this order, the shipper must be instructed to show the purchase order number on all packages and shipping manifests to ensure proper identification and payment of invoices. A complete packing list must accompany each shipment.

28) NOTICES: Any notices required under the Agreement should be delivered to the Contract Administrator for each party. Unless otherwise specified in the Solicitation Documents, any notices shall be delivered in writing by U.S. Mail, Commercial Courier or by hand.

29) TITLES AND HEADINGS: Titles and Headings in the Agreement are used for convenience only and do not define, limit or proscribe the language of terms identified by such Titles and Headings.

30) AMENDMENT: The Agreement may not be amended orally or by performance. Any amendment must be made in written form and signed by duly authorized representatives of the State and Vendor in conformance with Paragraph 36) herein.

31) TAXES: The State of North Carolina is exempt from Federal excise taxes and no payment will be made for any personal property taxes levied on the Vendor or for any taxes levied on employee wages. Agencies of the State may have additional exemptions or exclusions for federal or state taxes. Evidence of such additional exemptions or exclusions may be provided to Vendor by Agencies, as applicable, during the term of the Agreement. Applicable State or local sales taxes shall be invoiced as a separate item.

32) GOVERNING LAWS, JURISDICTION, AND VENUE:

a) The Agreement is made under and shall be governed and construed in accordance with the laws of the State of North Carolina and applicable Administrative Rules. The place of the Agreement or purchase order, its situs and forum, shall be Wake County, North Carolina, where all matters, whether sounding in Contract or in tort, relating to its validity, construction, interpretation and enforcement shall be determined. Vendor agrees and submits, solely for matters relating to the Agreement, to the jurisdiction of the courts of the State of North Carolina, and stipulates that Wake County shall be the proper venue for all matters.

b) Except to the extent the provisions of the Contract are clearly inconsistent therewith, the applicable provisions of the Uniform Commercial Code as modified and adopted in North Carolina shall govern the Agreement. To the extent the Contract entails both the supply of "goods" and "Services," such shall be deemed "goods" within the meaning of the Uniform Commercial Code, except when deeming such Services as "goods" would result in a clearly unreasonable interpretation.

33) FORCE MAJEURE: Neither party shall be deemed to be in default of its obligations hereunder if and so long as it is prevented from performing such obligations as a result of events beyond its reasonable control, including without limitation, fire, power failures, any act of war, hostile foreign action, nuclear

explosion, riot, strikes or failures or refusals to perform under subcontracts, civil insurrection, earthquake, hurricane, tornado, or other catastrophic natural event or act of God.

34) **COMPLIANCE WITH LAWS:** The Vendor shall comply with all laws, ordinances, codes, rules, regulations, and licensing requirements that are applicable to the conduct of its business, including those of federal, state, and local agencies having jurisdiction and/or authority.

35) **SEVERABILITY:** In the event that a court of competent jurisdiction holds that a provision or requirement of the Agreement violates any applicable law, each such provision or requirement shall be enforced only to the extent it is not in violation of law or is not otherwise unenforceable and all other provisions and requirements of the Agreement shall remain in full force and effect. All promises, requirement, terms, conditions, provisions, representations, guarantees and warranties contained herein shall survive the expiration or termination date unless specifically provided otherwise herein, or unless superseded by applicable federal or State statute, including statutes of repose or limitation.

36) **CHANGES:** The Agreement and subsequent purchase order(s) is awarded subject to the provision of the specified Services and the shipment or provision of other Deliverables as specified herein. Any changes made to the Agreement or purchase order proposed by the Vendor are hereby rejected unless accepted in writing by the Agency or State Award Authority. The State shall not be responsible for Services or other Deliverables delivered without a purchase order from the Agency or State Award Authority.

37) **FEDERAL INTELLECTUAL PROPERTY BANKRUPTCY PROTECTION ACT:** The Parties agree that the Agency shall be entitled to all rights and benefits of the Federal Intellectual Property Bankruptcy Protection Act, Public Law 100-506, codified at 11 U.S.C. 365(n), and any amendments thereto.

38) **ELECTRONIC PROCUREMENT (Applies to all contracts that include E-Procurement and are identified as such in the body of the solicitation document):** Purchasing shall be conducted through the Statewide E-Procurement Services. The State's third party agent shall serve as the Supplier Manager for this E-Procurement Services. The Vendor shall register for the Statewide E-Procurement Services within two (2) business days of notification of award in order to receive an electronic purchase order resulting from award of the Agreement.

   a) **The successful Vendor(s) shall pay a transaction fee of 1.75% (.0175) on the total dollar amount (excluding sales taxes) of each purchase order issued through the Statewide E-Procurement Service**. This applies to all purchase orders, regardless of the quantity or dollar amount of the purchase order. The transaction fee shall neither be charged to nor paid by the State, or by any State approved users of the contract. The transaction fee shall not be stated or included as a separate item in the proposed contract or invoice. There are no additional fees or charges to the Vendor for the Services rendered by the Supplier Manager under the Agreement. Vendor will receive a credit for transaction fees they paid for the purchase of any item(s) if an item(s) is returned through no fault of the Vendor. Transaction fees are non-refundable when an item is rejected and returned, or declined, due to the Vendor's failure to perform or comply with specifications or requirements of the contract.

   b) Vendor, or its authorized Reseller, as applicable, will be invoiced monthly for the State's transaction fee by the Supplier Manager. The transaction fee shall be based on purchase orders issued for the prior month. Unless Supplier Manager receives written notice from the Vendor identifying with specificity any errors in an invoice within thirty (30) days of the receipt of invoice, such invoice shall be deemed to be correct and Vendor shall have waived its right to later dispute the accuracy and completeness of the invoice. Payment of the transaction fee by the Vendor is due to the account designated by the State within thirty (30) days after receipt of the correct invoice for the transaction fee, which includes payment of all portions of an invoice not in dispute. Within thirty (30) days of the receipt of invoice, Vendor may request in writing an extension of the invoice payment due date for that portion of the transaction fee invoice for which payment of the related goods by the governmental purchasing entity has not been received by the Vendor. If payment of the transaction fee invoice is not received by the State within this payment period, it shall be considered a material breach of contract. The Supplier Manager shall provide, whenever reasonably requested by the Vendor in writing (including electronic documents), supporting documentation from the E-Procurement Service that accounts for the amount of the invoice.

c) The Supplier Manager will capture the order from the State approved user, including the shipping and payment information, and submit the order in accordance with the E-Procurement Services. Subsequently, the Supplier Manager will send those orders to the appropriate Vendor on State Contract. The State or State approved user, not the Supplier Manager, shall be responsible for the solicitation, offers received, evaluation of offers received, award of Contract, and the payment for goods delivered.

d) Vendor agrees at all times to maintain the confidentiality of its user name and password for the Statewide E-Procurement Services. If a Vendor is a corporation, partnership or other legal entity, then the Vendor may authorize its employees to use its password. Vendor shall be responsible for all activity and all charges for such employees. Vendor agrees not to permit a third party to use the Statewide E-Procurement Services through its account. If there is a breach of security through the Vendor's account, Vendor shall immediately change its password and notify the Supplier Manager of the security breach by e-mail. Vendor shall cooperate with the state and the Supplier Manager to mitigate and correct any security breach.

39) PATENT, COPYRIGHT, AND TRADE SECRET PROTECTION:

a) Vendor has created, acquired or otherwise has rights in, and may, in connection with the performance of Services for the State, employ, provide, create, acquire or otherwise obtain rights in various concepts, ideas, methods, methodologies, procedures, processes, know-how, techniques, models, templates and general purpose consulting and software tools, utilities and routines (collectively, the "Vendor technology"). To the extent that any Vendor technology is contained in any of the Services or Deliverables including any derivative works, the Vendor hereby grants the State a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to use such Vendor technology in connection with the Services or Deliverables for the State's purposes.

b) Vendor shall not acquire any right, title and interest in and to the copyrights for goods, any and all software, technical information, specifications, drawings, records, documentation, data or derivative works thereof, or other work products provided by the State to Vendor. The State hereby grants Vendor a royalty-free, fully paid, worldwide, perpetual, non-exclusive license for Vendor's internal use to non-confidential deliverables first originated and prepared by the Vendor for delivery to the State.

c) The Vendor, at its own expense, shall defend any action brought against the State to the extent that such action is based upon a claim that the Services or other Deliverables supplied by the Vendor, or the operation of such pursuant to a current version of vendor-supplied software, infringes a patent, or copyright or violates a trade secret in the United States. The Vendor shall pay those costs and damages finally awarded against the State in any such action; damages shall be limited as provided in N.C.G.S. 143B-1350(h1). Such defense and payment shall be conditioned on the following:
   i) That the Vendor shall be notified within a reasonable time in writing by the State of any such claim; and,
   ii) That the Vendor shall have the sole control of the defense of any action on such claim and all negotiations for its settlement or compromise, provided, however, that the State shall have the option to participate in such action at its own expense.

d) Should any Services or other Deliverables supplied by Vendor, or the operation thereof become, or in the Vendor's opinion are likely to become, the subject of a claim of infringement of a patent, copyright, or a trade secret in the United States, the State shall permit the Vendor, at its option and expense, either to procure for the State the right to continue using the Services or Deliverables, or to replace or modify the same to become non-infringing and continue to meet procurement specifications in all material respects. If neither of these options can reasonably be taken, or if the use of such Services or Deliverables by the State shall be prevented by injunction, the Vendor agrees to take back any goods/hardware or software, and refund any sums the State has paid Vendor less any reasonable amount for use or damage and make every reasonable effort to assist the state in procuring substitute Services or Deliverables. If, in the sole opinion of the State, the return of such infringing Services or Deliverables makes the retention of other Services or Deliverables acquired from the Vendor under the agreement impractical, the State shall then have the option of terminating the contract, or

applicable portions thereof, without penalty or termination charge. The Vendor agrees to take back Services or Deliverables and refund any sums the State has paid Vendor less any reasonable amount for use or damage.

e) Vendor will not be required to defend or indemnify the State if any claim by a third party against the State for infringement or misappropriation (i) results from the State's alteration of any Vendor-branded Service or Deliverable, or (ii) results from the continued use of the good(s) or services and other Services or Deliverables after receiving notice they infringe a trade secret of a third party.

f) Nothing stated herein, however, shall affect Vendor's ownership in or rights to its preexisting intellectual property and proprietary rights.

40) UNANTICIPATED TASKS In the event that additional work must be performed that was wholly unanticipated, and that is not specified in the Agreement, but which in the opinion of both parties is necessary to the successful accomplishment of the contracted scope of work, the procedures outlined in this article will be followed. For each item of unanticipated work, the Vendor shall prepare a work authorization in accordance with the State's practices and procedures.

a) It is understood and agreed by both parties that all of the terms and conditions of the Agreement shall remain in force with the inclusion of any work authorization. A work authorization shall not constitute a contract separate from the Agreement, nor in any manner amend or supersede any of the other terms or provisions of the Agreement or any amendment hereto.

b) Each work authorization shall comprise a detailed statement of the purpose, objective, or goals to be undertaken by the Vendor, the job classification or approximate skill level or sets of the personnel required, an identification of all significant material then known to be developed by the Vendor's personnel as a Deliverable, an identification of all significant materials to be delivered by the State to the Vendor's personnel, an estimated time schedule for the provision of the Services by the Vendor, completion criteria for the work to be performed, the name or identification of Vendor's personnel to be assigned, the Vendor's estimated work hours required to accomplish the purpose, objective or goals, the Vendor's billing rates and units billed, and the Vendor's total estimated cost of the work authorization.

c) All work authorizations must be submitted for review and approval by the procurement office that approved the original Contract and procurement. This submission and approval must be completed prior to execution of any work authorization documentation or performance thereunder. All work authorizations must be written and signed by the Vendor and the State prior to beginning work.

d) The State has the right to require the Vendor to stop or suspend performance under the "Stop Work" provision of the North Carolina Department of Information Technology Terms and Conditions.

e) The Vendor shall not expend Personnel resources at any cost to the State in excess of the estimated work hours unless this procedure is followed: If, during performance of the work, the Vendor determines that a work authorization to be performed under the Agreement cannot be accomplished within the estimated work hours, the Vendor will be required to complete the work authorization in full. Upon receipt of such notification, the State may:

   i) Authorize the Vendor to expend the estimated additional work hours or service in excess of the original estimate necessary to accomplish the work authorization, or

   ii) Terminate the work authorization, or

   iii) Alter the scope of the work authorization in order to define tasks that can be accomplished within the remaining estimated work hours.

   iv) The State will notify the Vendor in writing of its election within seven (7) calendar days after receipt of the Vendor's notification. If notice of the election is given to proceed, the Vendor may expend the estimated additional work hours or Services.

42) STOP WORK ORDER The State may issue a written Stop Work Order to Vendor for cause at any time requiring Vendor to suspend or stop all, or any part, of the performance due under the Agreement for a period up to ninety (90) days after the Stop Work Order is delivered to the Vendor. The ninety (90) day period may be extended for any further period for which the parties may agree.

a) The Stop Work Order shall be specifically identified as such and shall indicate that it is issued under this term. Upon receipt of the Stop Work Order, the Vendor shall immediately comply with its terms and take all reasonable steps to minimize incurring costs allocable to the work covered by the Stop Work Order during the period of work suspension or stoppage. Within a period of ninety (90) days after a Stop Work Order is delivered to Vendor, or within any extension of that period to which the parties agree, the State shall either:
   i) Cancel the Stop Work Order, or
   ii) Terminate the work covered by the Stop Work Order as provided for in the termination for default or the termination for convenience clause of the Agreement.

b) If a Stop Work Order issued under this clause is canceled or the period of the Stop Work Order or any extension thereof expires, the Vendor shall resume work. The State shall make an equitable adjustment in the delivery schedule, the Agreement price, or both, and the Agreement shall be modified, in writing, accordingly, if:
   i) The Stop Work Order results in an increase in the time required for, or in the Vendor's cost properly allocable to the performance of any part of the Agreement, and
   ii) The Vendor asserts its right to an equitable adjustment within thirty (30) days after the end of the period of work stoppage; provided that if the State decides the facts justify the action, the State may receive and act upon an offer submitted at any time before final payment under the Agreement.

c) If a Stop Work Order is not canceled and the work covered by the Stop Work Order is terminated in accordance with the provision entitled Termination for Convenience of the State, the State shall allow reasonable direct costs resulting from the Stop Work Order in arriving at the termination settlement.

d) The State shall not be liable to the Vendor for loss of profits because of a Stop Work Order issued under this term.

43) <u>TRANSITION ASSISTANCE</u> If the Agreement is not renewed at the end of the term, or is canceled prior to its expiration, for any reason, the Vendor must provide for up to six (6) months after the expiration or cancellation of the Agreement, all reasonable transition assistance requested by the State, to allow for the expired or canceled portion of the Services to continue without interruption or adverse effect, and to facilitate the orderly transfer of such Services to the State or its designees. Such transition assistance will be deemed by the parties to be governed by the terms and conditions of the Agreement, (notwithstanding this expiration or cancellation) except for those Contract terms or conditions that do not reasonably apply to such transition assistance. The State shall pay the Vendor for any resources utilized in performing such transition assistance at the most current rates provided by the Agreement for Contract performance. If the State cancels the Agreement for cause, then the State will be entitled to off set the cost of paying the Vendor for the additional resources the Vendor utilized in providing transition assistance with any damages the State may have otherwise accrued as a result of said cancellation.

Section 2: Terms and Conditions Applicable to IT Goods and Services

1) <u>SOFTWARE LICENSE FOR HARDWARE, EMBEDDED SOFTWARE AND FIRMWARE:</u>

RESERVED.

2) <u>LICENSE GRANT FOR APPLICATION SOFTWARE, (COTS):</u> This paragraph recites the scope of license granted, if not superseded by a mutually agreed and separate licensing agreement, as follows:

a) Vendor grants to the State, its Agencies and lawful customers a non-exclusive, non-transferable and non-sublicensable license to use, in object code format, Vendor's software identified in the solicitation documents, Vendor's Statement of Work (SOW), or an Exhibit thereto executed by the parties ("Software"), subject to the restrictions set forth therein, such as the authorized computer system, the data source type(s), the number of target instance(s) and the installation site. Use of the Software shall be limited to the data processing and computing needs of the State, its Agencies and lawful

customers. This license shall be perpetual or for the term of the contract (pick one, delete the other), unless terminated as provided herein. The State agrees not to distribute, sell, sublicense or otherwise transfer copies of the Software or any portion thereof. For purposes of this Agreement, a State Entity shall be defined as any department or agency of the State of North Carolina, which is controlled by or under common control of the State or who is a lawful customer of the State pursuant to Article 3D of Chapter 147 of the General Statutes.

b) Vendor shall provide all encryption or identification codes or authorizations that are necessary or proper for the operation of the licensed Software.

c) The State shall have the right to copy the Software, in whole or in part, for use in conducting benchmark or acceptance tests, for business recovery and disaster recovery testing or operations, for archival or emergency purposes, for back up purposes, for use in preparing derivative works if allowed by the solicitation documents or statements of work, or to replace a worn copy.

d) The State may modify non-personal Software in machine-readable form for its internal use in merging the same with other software program material. Any action hereunder shall be subject to uses described in this paragraph, the restrictions imposed by Paragraph 3), and applicable terms in the solicitation documents or statements of work.

3) <u>WARRANTY TERMS</u>: Notwithstanding anything in the Agreement or Exhibit hereto to the contrary, Vendor shall assign warranties for any Deliverable supplied by a third party to the State.

a) a) Vendor warrants that any Software or Deliverable will operate substantially in conformity with prevailing specifications as defined by the current standard documentation (except for minor defects or errors which are not material to the State) for a period of ninety (90) days from the date of acceptance ("Warranty Period"), unless otherwise specified in the Solicitation Documents. If the Software does not perform in accordance with such specifications during the Warranty Period, Vendor will use reasonable efforts to correct any deficiencies in the Software so that it will perform in accordance with or substantially in accordance with such specifications.

b) Vendor warrants to the best of its knowledge that:
   i) The licensed Software and associated materials do not infringe any intellectual property rights of any third party;
   ii) There are no actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party;
   iii) The licensed Software and associated materials do not contain any surreptitious programming codes, viruses, Trojan Horses, "back doors" or other means to facilitate or allow unauthorized access to the State's information systems.
   iv) The licensed Software and associated materials do not contain any timer, counter, lock or similar device (other than security features specifically approved by Customer in the Specifications) that inhibits or in any way limits the Software's ability to operate.

c) UNLESS MODIFIED BY AMENDMENT OR THE SOLICITATION DOCUMENTS, THE WARRANTIES IN THIS PARAGRAPH ARE IN LIEU OF ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, OR WHETHER ARISING BY COURSE OF DEALING OR PERFORMANCE, CUSTOM, USAGE IN THE TRADE OR PROFESSION OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NO OTHER REPRESENTATIONS OR WARRANTIES HAVE FORMED THE BASIS OF THE BARGAIN HEREUNDER.

4) <u>RESTRICTIONS:</u> State's use of the Software is restricted as follows:

a) The license granted herein is granted to the State and to any political subdivision or other entity permitted or authorized to procure Information Technology through the Department of Information Technology. If the License Grant and License Fees are based upon the number of Users, the number of Users may be increased at any time, subject to the restrictions on the maximum number of Users specified in the solicitation documents.

b) No right is granted hereunder to use the Software to perform Services for commercial third parties (so-called "service bureau" uses). Services provided to other State Departments, Agencies or political subdivisions of the State is permitted.
c) The State may not copy, distribute, reproduce, use, lease, rent or allow access to the Software except as explicitly permitted under this Agreement, and State will not modify, adapt, translate, prepare derivative works (unless allowed by the solicitation documents or statements of work,) decompile, reverse engineer, disassemble or otherwise attempt to derive source code from the Software or any internal data files generated by the Software.
d) State shall not remove, obscure or alter Vendor's copyright notice, trademarks, or other proprietary rights notices affixed to or contained within the Software.

5) SUPPORT OR MAINTENANCE SERVICES: This paragraph recites the scope of maintenance Services due under the license granted, if not superseded by a separate licensing and maintenance agreement or as may be stated in the solicitation documents. Subject to payment of a Support Service or Maintenance Fee stated in the solicitation documents for the first year and all subsequent years, if requested by the State, Vendor agrees to provide the following support Services ("Support Services") for the current version and one previous version of the Software commencing upon delivery of the Software:

a) **Error Correction:** If the error conditions reported by the State pursuant to the General Terms and Conditions are not corrected in a timely manner, the State may request a replacement copy of the licensed Software from Vendor. In such event, Vendor shall then deliver a replacement copy, together with corrections and updates, of the licensed Software within 24 hours of the State's request at no added expense to the State.
b) **Other Agreement**: This Paragraph 5 may be superseded by written mutual agreement provided that: Support and maintenance Services shall be fully described in such a separate agreement annexed hereto and incorporated herein
c) **Temporary Extension of License**: If any licensed Software or CPU/computing system on which the Software is installed fails to operate or malfunctions, the term of the license granted shall be temporarily extended to another CPU selected by the State and continue until the earlier of:
   i) Return of the inoperative CPU to full operation, or
   ii) Termination of the license.
d) **Encryption Code:** Vendor shall provide any temporary encryption code or authorization necessary or proper for operation of the licensed Software under the foregoing temporary license. The State will provide notice by expedient means, whether by telephone, e-mail or facsimile of any failure under this paragraph. On receipt of such notice, Vendor shall issue any temporary encryption code or authorization to the State within twenty-four (24) hours; unless otherwise agreed.
e) **Updates:** Vendor shall provide to the State, at no additional charge, all new releases and bug fixes (collectively referred to as "Updates") for any Software Deliverable developed or published by Vendor and made generally available to its other customers at no additional charge. All such Updates shall be a part of the Program and Documentation and, as such, be governed by the provisions of the Agreement.
f) **Telephone Assistance:** Vendor shall provide the State with telephone access to technical support engineers for assistance in the proper installation and use of the Software, and to report and resolve Software problems, during normal business hours, 8:00 AM - 5:00 PM Eastern Time, Monday-Friday. Vendor shall respond to the telephone requests for Program maintenance service, within four (4) hours or eight (8) hours or next business day, etc., for calls made at any time.

6) STATE PROPERTY AND INTANGIBLES RIGHTS: The parties acknowledge and agree that the State shall own all right, title and interest in and to the copyright in any and all software, technical information, specifications, drawings, records, documentation, data and other work products first originated and prepared by the Vendor for delivery to the State (the "Deliverables"). To the extent that any Vendor Technology is contained in any of the Deliverables, the Vendor hereby grants the State a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to use such Vendor Technology in connection with the Deliverables for the State's internal business purposes. Vendor shall not acquire any right, title and

interest in and to the copyrights for goods, any and all software, technical information, specifications, drawings, records, documentation, data or derivative works thereof, or other work products provided by the State to Vendor. The State hereby grants Vendor a royalty-free, fully paid, worldwide, perpetual, non-exclusive license to non-confidential Deliverables first originated and prepared by the Vendor for delivery to the State.

Section 3: Terms and Conditions Applicable to Personnel and Personal Services

1) **VENDOR'S REPRESENTATION:** Vendor warrants that qualified personnel will provide Services in a professional manner. "Professional manner" means that the personnel performing the Services will possess the skill and competence consistent with the prevailing business standards in the information technology industry. Vendor agrees that it will not enter any agreement with a third party that might abridge any rights of the State under the Agreement. Vendor will serve as the prime Vendor under the Agreement. Should the State approve any subcontractor(s), the Vendor shall be legally responsible for the performance and payment of the subcontractor(s). Names of any third party Vendors or subcontractors of Vendor may appear for purposes of convenience in Contract documents; and shall not limit Vendor's obligations hereunder. Such third party subcontractors, if approved, may serve as subcontractors to Vendor. Vendor will retain executive representation for functional and technical expertise as needed in order to incorporate any work by third party subcontractor(s).
   a) Intellectual Property. Vendor represents that it has the right to provide the Services and other Deliverables without violating or infringing any law, rule, regulation, copyright, patent, trade secret or other proprietary right of any third party. Vendor also represents that its Services and other Deliverables are not the subject of any actual or threatened actions arising from, or alleged under, any intellectual property rights of any third party.
   b) Inherent Services. If any Services or other Deliverables, functions, or responsibilities not specifically described in the Agreement are required for Vendor's proper performance, provision and delivery of the Services and other Deliverables pursuant to the Agreement, or are an inherent part of or necessary sub-task included within the Services, they will be deemed to be implied by and included within the scope of the Contract to the same extent and in the same manner as if specifically described in the Contract.
   c) Vendor warrants that it has the financial capacity to perform and to continue to perform its obligations under the Contract; that Vendor has no constructive or actual knowledge of an actual or potential legal proceeding being brought against Vendor that could materially adversely affect performance of the Agreement; and that entering into the Agreement is not prohibited by any Contract, or order by any court of competent jurisdiction.
2) **SERVICES PROVIDED BY VENDOR:** Vendor shall provide the State with implementation Services as specified in a Statement of Work ("SOW") executed by the parties. This Agreement in combination with each SOW individually comprises a separate and independent contractual obligation from any other SOW. A breach by Vendor under one SOW will not be considered a breach under any other SOW. The Services intended hereunder are related to the State's implementation and/or use of one or more Software Deliverables licensed hereunder or in a separate software license agreement between the parties ("License Agreement").
3) **PERSONNEL:** Vendor shall not substitute key personnel assigned to the performance of the Agreement without prior written approval by the Agency Contract Administrator. The individuals designated as key personnel for purposes of the Agreement are those specified in the Vendor's offer. Any desired substitution shall be noticed to the Agency's Contract Administrator in writing accompanied by the names and references of Vendor's recommended substitute personnel. The Agency will approve or disapprove the requested substitution in a timely manner. The Agency may, in its sole discretion, terminate the Services of any person providing Services under the Agreement. Upon such termination, the Agency may request acceptable substitute personnel or terminate the Contract Services provided by such personnel.

a) Unless otherwise expressly provided in the Contract, Vendor will furnish all of its own necessary management, supervision, labor, facilities, furniture, computer and telecommunications equipment, software, supplies and materials necessary for the Vendor to provide and deliver the Services and other Deliverables.
b) Vendor personnel shall perform their duties on the premises of the State, during the State's regular work days and normal work hours, except as may be specifically agreed otherwise, established in the specification, or statement of work.
c) The Agreement shall not prevent Vendor or any of its personnel supplied under the Agreement from performing similar Services elsewhere or restrict Vendor from using the personnel provided to the State, provided that:
    i) Such use does not conflict with the terms, specifications or any amendments to the Agreement, or
    ii) Such use does not conflict with any procurement law, regulation or policy, or
    iii) Such use does not conflict with any non-disclosure agreement, or term thereof, by and between the State and Vendor or Vendor's personnel.
d) Unless otherwise provided by the Agency, the Vendor shall furnish all necessary personnel, Services, and otherwise perform all acts, duties and responsibilities necessary or incidental to the accomplishment of the tasks specified in the Agreement. The Vendor shall be legally and financially responsible for its personnel including, but not limited to, any deductions for social security and other withholding taxes required by state or federal law. The Vendor shall be solely responsible for acquiring any equipment, furniture, and office space not furnished by the State necessary for the Vendor to comply with the Agreement. The Vendor personnel shall comply with any applicable State facilities or other security rules and regulations.

4) <u>PERSONAL SERVICES</u>: RESERVED.

ATTACHMENT C: DESCRIPTION OF VENDOR

Provide the information about the Vendor.

Vendor's full name	
Vendor's address	
Vendor's telephone number	
Ownership	☐ Public ☐ Partnership ☐ Subsidiary ☐ Other (specify)
Date established	
If incorporated, State of incorporation.	
North Carolina Secretary of State Registration Number, if currently registered	
Number of full-time employees on January 1st for the last three years or for the duration that the Vendor has been in business, whichever is less.	
Vendor's Contact for Clarification of offer: Contact's name Title Email address and Telephone Number	
Vendor's Contact for Negotiation of offer: Contact's name Title Email address and Telephone Number	
If Contract is Awarded, Vendor's Contact for Contractual Issues: Contact's name Title Email address and Telephone Number	
If Contract is Awarded, Vendor's Contact for Technical Issues: Contact's name	

Title Email address and Telephone Number	

HISTORICALLY UNDERUTILIZED BUSINESSES

Historically Underutilized Businesses (HUBs) consist of minority, women and disabled business firms that are at least fifty-one percent owned and operated by an individual(s) of the categories. Also included as HUBs are disabled business enterprises and non-profit work centers for the blind and severely disabled."

Pursuant to N.C.G.S. §§ 143B-1361(a), 143-48 and 143-128.4, the State invites and encourages participation in this procurement process by businesses owned by minorities, women, disabled, disabled business enterprises and non-profit work centers for the blind and severely disabled. This includes utilizing subcontractors to perform the required functions in this RFP. Contact the North Carolina Office of historically Underutilized Businesses at 919-807-2330 with questions concerning NC HUB certification. http://ncadmin.nc.gov/businesses/hub

Respond to the questions below.

1.0 Is Vendor a Historically Underutilized Business? ☐ Yes ☐ No

2.0 Is Vendor Certified with North Carolina as a Historically Underutilized Business? ☐ Yes ☐ No

If so, state HUB classification:

_____

ATTACHMENT D: COST FORM

See and complete Excel Workbook: Attachment D: Cost Form

ATTACHMENT E: VENDOR CERTIFICATION FORM

1) ELIGIBLE VENDOR

The Vendor certifies that in accordance with N.C.G.S. §143-59.1(b), Vendor is not an ineligible vendor as set forth in N.C.G.S. §143-59.1 (a).

The Vendor acknowledges that, to the extent the awarded contract involves the creation, research, investigation or generation of a future RFP or other solicitation; the Vendor will be precluded from bidding on the subsequent RFP or other solicitation and from serving as a subcontractor to an awarded vendor.

The State reserves the right to disqualify any bidder if the State determines that the bidder has used its position (whether as an incumbent Vendor, or as a subcontractor hired to assist with the RFP development, or as a Vendor offering free assistance) to gain a competitive advantage on the RFP or other solicitation.

2) CONFLICT OF INTEREST

Applicable standards may include: N.C.G.S. §§143B-1352 and 143B-1353, 14-234, and 133-32. The Vendor shall not knowingly employ, during the period of the Agreement, nor in the preparation of any response to this solicitation, any personnel who are, or have been, employed by a Vendor also in the employ of the State and who are providing Services involving, or similar to, the scope and nature of this solicitation or the resulting contract.

3) E-VERIFY

Pursuant to N.C.G.S. § 143B-1350(k), the State shall not enter into a contract unless the awarded Vendor and each of its subcontractors comply with the E-Verify requirements of N.C.G.S. Chapter 64, Article 2. Vendors are directed to review the foregoing laws. Vendors claiming exceptions or exclusions under Chapter 64 must identify the legal basis for such claims and certify compliance with federal law regarding registration of aliens including 8 USC 1373 and 8 USC 1324a. Any awarded Vendor must submit a certification of compliance with E-Verify to the awarding agency, and on a periodic basis thereafter as may be required by the State.

4) CERTIFICATE TO TRANSACT BUSINESS IN NORTH CAROLINA

As a condition of contract award, awarded Vendor shall have registered its business with the North Carolina Secretary of State and shall maintain such registration throughout the term of the Contract.

Signature: Date:

Printed Name:

Title:

ATTACHMENT F: LOCATION OF WORKERS UTILIZED BY VENDOR

In accordance with N.C.G.S. §143B-1361(b), Vendor must identify how it intends to utilize resources or workers located outside the U.S., and the countries or cities where such are located. The State will evaluate additional risks, costs, and other factors associated with the Vendor's utilization of resources or workers prior to making an award for any such Vendor's offer. The Vendor shall provide the following:

a) The location of work to be performed by the Vendor's employees, subcontractors, or other persons, and whether any work will be performed outside the United States. The Vendor shall provide notice of any changes in such work locations if the changes result in performing work outside of the United States.

b) Any Vendor or subcontractor providing support or maintenance Services for software, call or contact center Services shall disclose the location from which the call or contact center Services are being provided upon request.

Will Vendor perform any work outside of the United States? ☐ YES ☐ NO

If yes, Vendor MUST list what countries the employees are working and in what capacity are they accessing State Data. Specifically, the State must know if the employees are Help Desk support, Technical Support and/or Coder, etc.

ATTACHMENT G: REFERENCES

The Vendor should provide up to three (3) references of customers utilizing, or intending to utilize, the proposed solution in a setting similar to this solicitation's size, complexity, and scope of work.

The Vendor is encouraged to include any implementation of the respective proposed service within the last seven (7) years if applicable. Customer references whose business processes and data needs are similar to those performed by the Agency needing this solution in terms of functionality, size, complexity, and transaction volume are encouraged.

For each reference, the Vendor should provide the following information:

a) Customer name.

b) Customer address.

c) Current telephone number of a customer employee most familiar with the offered solution implementation.

d) Customer email address

e) Time period over which each offered solution implementation was completed.

f) Brief summary of the offered solution implementation.

g) List of offered solution products installed and operational.

h) Number of vendor or technical staff supporting, maintaining and managing the offered solution

i) Number of end users supported by the offered solution.

ATTACHMENT H: FINANCIAL REVIEW FORM

Vendor shall review the Financial Review Form, provide responses in the gray-shaded boxes, and submit the completed Form as an Excel file with its offer. Vendor shall not add or delete rows or columns in the Form, or change the order of the rows or column in the file.

1. Vendor Name:

2. Company structure for tax purposes (C Corp, S Corp, LLC, LLP, etc.):

3. Have you been in business for more than three years? ☐ Yes ☐ No

4. Have you filed for bankruptcy in the past three years? ☐ Yes ☐ No

5. In the past three years, has your auditor issued any notification letters addressing significant issues? If yes, please explain and provide a copy of the notification letters. ☐ Yes ☐ No

6. Are the financial figures below based on audited financial statements? ☐ Yes ☐ No

7. Start Date of financial statements:

   End Date of financial statements:

8. Provide a link to annual reports with financial statements and management discussion for the past three complete fiscal years:

9. Provide the following information for the past three complete fiscal years:

	Latest complete fiscal year minus two years	Latest complete fiscal year minus one year	Latest complete fiscal year
BALANCE SHEET DATA			
a. Cash and Temporary Investments			
b. Accounts Receivable (beginning of year)			
c. Accounts Receivable (end of year)			
d. Average Account Receivable for the Year (calculated)			
e. Inventory (beginning of year)			
f. Inventory (end of year)			
g. Average Inventory for the Year (calculated)			
h. Current Assets			
i. Current Liabilities			
j. Total Liabilities			
k. Total Stockholders' Equity (beginning of year)			
l. Total Stockholders' Equity (end of year)			
m. Average Stockholders' Equity during the year (calculated)			
INCOME STATEMENT DATA			
a. Net Sales			
b. Cost of Goods Sold (COGS)			
c. Gross Profit (Net Sales minus COGS) (calculated)			
d. Interest Expense for the Year			
e. Net Income after Tax			
f. Earnings for the Year before Interest & Income Tax Expense			
STATEMENT OF CASH FLOWS			
a. Cash Flow provided by Operating Activities			
b. Capital Expenditures (property, plant, equipment)			

ATTACHMENT I: FUNCTIONAL SPECIFICATIONS MATRIX

- See and complete Excel Workbook: Attachment I: Functional Specifications Matrix

ATTACHMENT J: TECHNICAL SPECIFICATIONS MATRIX

- See and complete Excel Workbook: Attachment J: Technical Specifications Matrix

ATTACHMENT K: KEY PERSONNEL AND RESUMES

The table below lists the positions determined to be "Key Personnel" as described in Section 7.14.1 of the Tax System Modernization Request for Proposal and summarizes the minimum qualifications for each Key Personnel position.

A resume template must be completed for each individual proposed for a Key Personnel position. Use additional space/pages if necessary.

Key Personnel	Responsibilities	Minimum Qualifications
Project Director	▪ Provides overall leadership, planning, coordination, and direction to the Vendor's Project Manager(s) and the team(s) ▪ Serves as the primary point of contact with North Carolina DOR's leadership, governance bodies, and other staff for activities related to contract administration and dispute resolution with North Carolina DOR throughout the life of the contract ▪ Shares responsibility for successful delivery with North Carolina DOR's leadership and governance bodies ▪ Is responsible for addressing any issues that cannot be resolved by the Vendor's Project Manager and North Carolina DOR's Project Manager ▪ Is responsible for managing all subcontractor relationships and insuring subcontractor compliance with the obligations of the contract	▪ Minimum of five (5) years of experience managing complex enterprise IT projects ▪ Demonstrated success leading large teams and the ability to manage teams effectively ▪ Strong communication and organizational skills ▪ Experience interacting at the C-suite level ▪ Excellent interpersonal and presentation skills ▪ Minimum of ten (10) years of experience in information technology project management
Project Manager	▪ Leads the Vendor's project team ▪ Serves as the primary liaison with Agency's project management team for activities related to overall project management and scheduling, correspondence between the Agency and the Vendor, and status reporting to the Agency for the duration of the contract ▪ Provides day-to-day management of the project including overall performance and contract compliance ▪ Develops, manages, and maintains the Project Implementation Schedule ▪ Is authorized to direct Vendor resources assigned to the Project, ensuring that appropriate resources are available throughout the duration of the Contract ▪ Develops and implements a quality assurance process to ensure all	▪ Minimum seven (7) years working for the Vendor ▪ Minimum five (5) years of experience as a Project Manager on large, complex system integration projects ▪ Excellent interpersonal and presentation skills

Key Personnel	Responsibilities	Minimum Qualifications
	objectives are met, milestones are achieved, and stakeholders are satisfied ▪ Immediately notifies Project Management Leadership of any deviation from agreed-upon scope, schedule, budget, resources, or level of quality	
Functional Lead	▪ Validation of future state business process flows and requirements ▪ Identification and documentation of functional gaps for the System	▪ Minimum five (5) years of experience as a Functional Lead on information technology projects of similar size and scope ▪ Minimum three (3) years of experience as a Functional Lead for the proposed solution
Technical Lead	▪ Manages all aspects of technical and system architecture development, transfer, and modification ▪ Ensures that technical requirements and tasks are understood, clearly communicated, and executed on time ▪ Plans and prioritizes software functionality within the realm of Department's requirements ▪ Participates in core project leadership discussions and decisions ▪ Tracks technical integration issues and coordinates issue resolution ▪ Ensures that routine system monitoring is provided and that issues are mitigated ▪ Ensures that appropriate security measures are properly utilized to protect sensitive data	▪ Minimum seven (7) years of experience implementing, developing, and/or managing enterprise IT systems ▪ Minimum three (3) years of experience as a technical lead for the proposed solution ▪ Experience working with tax or other sensitive datasets ▪ Expert understanding of the proposed solution architecture ▪ Expert understanding of hosted implementations for enterprise IT systems ▪ Expert understanding of the proposed solution application delivery technologies ▪ Expert understanding of IT system capacity planning ▪ Excellent interpersonal and presentation skills
Application/Solution Architect	▪ Provides input into technical architecture and design recommendations ▪ Provides support during testing and training of technical resources	▪ Minimum seven (7) years of experience as an Application Architect on information technology projects of similar size and scope ▪ Minimum five (5) years of experience in implementing the proposed solution
Security Lead	▪ Assists and supports in the design, development, and implementation of security requirements	▪ Minimum five (5) years of experience as a Security Lead on information technology projects of similar size and scope ▪ Minimum three (3) years of experience implementing security requirements for the proposed solution
Data Conversion Lead	▪ Works with agency to develop a data conversion plan ▪ Performs and supports data conversion, including testing	▪ Minimum five (5) years of experience as a Data Conversion Lead on information technology projects of similar size and scope

Key Personnel	Responsibilities	Minimum Qualifications
		▪ Minimum three (3) years of experience leading data management conversion efforts for the proposed solution
Testing Lead	▪ Develops and documents test plans and scripts ▪ Performs unit and system testing ▪ Assists North Carolina DOR in user acceptance testing (UAT) preparation ▪ Oversees execution of all other testing phases as outlined in the accepted test plan	▪ Minimum five (5) years of experience as a Testing Lead on information technology projects of similar size and scope ▪ Minimum three (3) years of experience implementing the proposed solution
Training Lead	▪ Leads end-user training ▪ Provides and assists in creation of training plan and documentation	▪ Minimum five (5) years of experience as a Training Lead on system implementation projects of similar size and scope ▪ Minimum two (2) years of experience leading the training effort for the proposed solution

KEY PERSONNEL RESUME

Vendor:	
Key Position:	**Project Director**
Minimum Qualifications	▪ Minimum of five (5) years of experience managing complex enterprise IT projects ▪ Demonstrated success leading large teams and the ability to manage teams effectively ▪ Strong communication and organizational skills ▪ Experience interacting at the C-suite level ▪ Excellent interpersonal and presentation skills ▪ Minimum of ten (10) years of experience in information technology project management
Proposed Individual:	
Years with the Company:	
Percent Project Utilization:	

RELEVANT EXPERIENCE

Describe the individual's experience in similar roles to the proposed Key Position.

EDUCATION

List the individual's training and education including institution name, city, state, degree and/or achievement and date completed/received.

CERTIFICATIONS

List any certifications relevant to the proposed Key Position

KEY PERSPNNEL RESUME

Vendor:	
Key Position:	**Project Manager**
Minimum Qualifications	▪ Minimum seven (7) years working for the Vendor ▪ Minimum five (5) years of experience as a Project Manager on large, complex system integration projects ▪ Excellent interpersonal and presentation skills
Proposed Individual:	
Years with the Company:	
Percent Project Utilization:	

RELEVANT EXPERIENCE *Describe the individual's experience in similar roles to the proposed Key Position.*

EDUCATION *List the individual's training and education including institution name, city, state, degree and/or achievement and date completed/received.*

CERTIFICATIONS *List any certifications relevant to the proposed Key Position*

KEY PERSONNEL RESUME

Vendor:	
Key Position:	**Functional Lead**
Minimum Qualifications	▪ Minimum five (5) years of experience as a Functional Lead on information technology projects of similar size and scope ▪ Minimum three (3) years of experience as a Functional Lead for the proposed solution
Proposed Individual:	
Years with the Company:	
Percent Project Utilization:	

RELEVANT EXPERIENCE

Describe the individual's experience in similar roles to the proposed Key Position.

EDUCATION

List the individual's training and education including institution name, city, state, degree and/or achievement and date completed/received.

CERTIFICATIONS

List any certifications relevant to the proposed Key Position

KEY PERSONNEL RESUME

Vendor:	
Key Position:	**Technical Lead**
Minimum Qualifications	▪ Minimum seven (7) years of experience implementing, developing, and/or managing enterprise IT systems ▪ Minimum three (3) years of experience as a technical lead for the proposed solution implementations ▪ Experience working with tax or other sensitive datasets ▪ Expert understanding of the proposed solution architecture ▪ Expert understanding of hosted implementations for enterprise IT systems ▪ Expert understanding of the proposed solution application delivery technologies ▪ Expert understanding of IT system capacity planning ▪ Excellent interpersonal and presentation skills
Proposed Individual:	
Years with the Company:	
Percent Project Utilization:	

RELEVANT EXPERIENCE *Describe the individual's experience in similar roles to the proposed Key Position.*
EDUCATION *List the individual's training and education including institution name, city, state, degree and/or achievement and date completed/received.*
CERTIFICATIONS *List any certifications relevant to the proposed Key Position*

KEY PERSONNEL RESUME

Vendor:	
Key Position:	**Application/Solution Architect**
Minimum Qualifications	▪ Minimum seven (7) years of experience as an Application Architect on information technology projects of similar size and scope ▪ Minimum five (5) years of experience in implementing the proposed solution
Proposed Individual:	
Years with the Company:	
Percent Project Utilization:	

RELEVANT EXPERIENCE *Describe the individual's experience in similar roles to the proposed Key Position.*

EDUCATION *List the individual's training and education including institution name, city, state, degree and/or achievement and date completed/received.*

CERTIFICATIONS *List any certifications relevant to the proposed Key Position*

KEY PERSONNEL RESUME

Vendor:	
Key Position:	**Security Lead**
Minimum Qualifications	▪ Minimum five (5) years of experience as a Security Lead on information technology projects of similar size and scope ▪ Minimum three (3) years of experience implementing security requirements for the proposed solution
Proposed Individual:	
Years with the Company:	
Percent Project Utilization:	
RELEVANT EXPERIENCE *Describe the individual's experience in similar roles to the proposed Key Position.*	
EDUCATION *List the individual's training and education including institution name, city, state, degree and/or achievement and date completed/received.*	
CERTIFICATIONS *List any certifications relevant to the proposed Key Position*	

KEY PERSONNEL RESUME

Vendor:	
Key Position:	**Data Conversion Lead**
Minimum Qualifications	▪ Minimum five (5) years of experience as a Data Conversion Lead on information technology projects of similar size and scope ▪ Minimum three (3) years of experience leading data management conversion efforts for the proposed solution
Proposed Individual:	
Years with the Company:	
Percent Project Utilization:	

RELEVANT EXPERIENCE *Describe the individual's experience in similar roles to the proposed Key Position.*

EDUCATION *List the individual's training and education including institution name, city, state, degree and/or achievement and date completed/received.*

CERTIFICATIONS *List any certifications relevant to the proposed Key Position*

KEY PERSONNEL RESUME

Vendor:	
Key Position:	**Testing Lead**
Minimum Qualifications	▪ Minimum five (5) years of experience as a Testing Lead on system implementation technology projects of similar size and scope ▪ Minimum three (3) years of experience implementing the proposed solution
Proposed Individual:	
Years with the Company:	
Percent Project Utilization:	

RELEVANT EXPERIENCE *Describe the individual's experience in similar roles to the proposed Key Position.*

EDUCATION *List the individual's training and education including institution name, city, state, degree and/or achievement and date completed/received.*

CERTIFICATIONS *List any certifications relevant to the proposed Key Position*

KEY PERSONNEL RESUME

Vendor:	
Key Position:	**Training Lead**
Minimum Qualifications	▪ Minimum five (5) years of experience as a Training Lead on system implementation projects of similar size and scope ▪ Minimum two (2) years of experience as the Training Lead for the implementation of the proposed solution
Proposed Individual:	
Years with the Company:	
Percent Project Utilization:	

RELEVANT EXPERIENCE *Describe the individual's experience in similar roles to the proposed Key Position.*

EDUCATION *List the individual's training and education including institution name, city, state, degree and/or achievement and date completed/received.*

CERTIFICATIONS *List any certifications relevant to the proposed Key Position*

ATTACHMENT L: STAFFING PLAN

See and complete Excel Workbook: Attachment L: Staffing Plan

ATTACHMENT M: TAX SCHEDULE MATRIX

See Excel Workbook: Attachment M: Tax Schedule Matrix (No Response Required)

ATTACHMENT N: FORMS INVENTORY

See Excel Workbook: Attachment N: Forms Inventory (No Response Required)

ATTACHMENT O: SYSTEMS INVENTORY

See Excel Workbook: Attachment O: Systems Inventory (No Response Required)

ATTACHMENT P: INTERFACES INVENTORY

See Excel Workbook: Attachment P: Interfaces Inventory (No Response Required)

ATTACHMENT Q: IMPLEMENTATION ROLES & RESPONSIBILITIES

See Excel Workbook: Attachment Q: Implementation Roles & Responsibilities (No Response Required)

ATTACHMENT R: NCDOR IT CERTIFICATION AND ACCREDITATION POLICY

OVERVIEW

This document contains the policy of the IT Division of the North Carolina Department of Revenue (Agency) with respect to the management of systems. The purpose of this document is to set forth expectations related to authorizing systems for Production in order to ensure all systems meet Agency information security requirements.

The Chief Information Officer (CIO) has approved the policy and is committed to the enforcement. The CIO, IT Directors, and IT Management agree to this policy and ensure their staff members are aware of and adhere to this policy.

All policy statements contained herein apply to anyone working on behalf of the Agency including, but not limited to, employees, officers, agents, contractors, consultants, vendors, interns, or any other person performing work for the Agency or for any individual, partnership, corporation or other entity providing goods or services to the Agency that will participate in operating systems. No exceptions to these policies are permitted unless previously approved by the CIO. Any questions related to this document should be referred to your supervisor.

PURPOSE

The purpose of this policy is to require that all systems are explicitly authorized to operate in a production environment by the CIO.

SCOPE

This policy applies to all Staff and Systems.

It is the policy of the Agency that all systems must be explicitly provided the authorization to operate (ATO) by the CIO using the NCDOR IT Certification and Accreditation (C&A) Process. The CIO may revoke an authorization at any time and all Agency Data must be sanitized from the system in accordance with Publication 1075 sanitization requirements.

a) No Agency Data may be received, stored, processed, or transmitted by systems that do not have an ATO.
b) All systems must be continuously monitored using CIO-approved processes and technologies to ensure all security and compliance requirements are met.
c) All systems must be assessed for security and compliance annually to maintain the ATO.
d) ATO’s are time limited and may be good for up to three years before expiring. Prior to ATO expiration, a new ATO request for the system must be re-submitted to initiate the C&A Process.
e) Any system undergoing enough significant changes to constitute a major change requires responsible parties and/or system owners to update the systems security plan and re-submit an ATO request to initiate the C&A Process.
f) ATO’s will be issued by the CIO for the ATO boundary described in the approved system security plan.

All Staff must:

a) ensure systems they own and/or are responsible for have an ATO through a formal request and submission to the C&A Process.

b) ensure that they do not allow Agency Data to reside on systems that do not have an ATO.

c) report a security incident if they know or suspect that Agency Data resides on systems that do not have an ATO.

d) ensure that systems they are responsible for are continuously monitored for compliance.

e) participate as needed in the C&A process and Continual Monitoring Process to ensure that all security and compliance requirements are met by all systems.

ATTACHMENT S: NCDOR CERTIFICATION AND ACCREDITATION PROCESS

ROLES AND RESPONSIBILITIES

The following describes the roles and responsibilities of key participants involved in an agency's C&A process. The C&A process is flexible, allowing the agency to effectively accomplish the intent of the specific tasks to best manage the risks to agency operations, agency assets, or individuals.

CIO

The Chief Information Officer (CIO) is the agency official who:

a) assumes responsibility and is accountable for the risks associated with operating an information system.

b) oversees the budget and operations of the information system within the agency and is often called upon to approve system security requirements, system security plans, and memorandums of agreement and/or memorandums of understanding.

c) issues an authorization to operate (ATO) for the information system under specific terms and conditions or deny authorization to operate (ATO) for the information system (or if the system is already operational, halt operations) if unacceptable security risks exist.

d) designates a senior agency information security officer.

e) develops and maintains information security policies, procedures, and control techniques to address all applicable requirements.

f) trains and oversees personnel with significant responsibilities for information security.

g) assists agency IT staff concerning their security responsibilities.

h) reports annually to the Secretary on the effectiveness of the agency information security program, including progress of remedial actions.

The CIO, with the support of the CISO, works closely with authorizing officials and their designated representatives to ensure that an agency- wide security program is effectively implemented, that the C&A required across the agency are accomplished in a timely and cost-effective manner, and that there is centralized reporting of all security-related activities.

To achieve a high degree of cost effectiveness of security, the CIO encourages the maximum reuse and sharing of security-related information including:

a) threat and vulnerability assessments.

b) risk assessments.

c) results from common security control assessments

d) any other general information that may be of assistance to information system owners and their supporting staffs.

In addition to the above duties, the CIO determines the appropriate allocation of resources dedicated to the protection of the agency's information systems based on organizational priorities.

CISO

The agency Chief Information Security Officer (CISO) is the agency official responsible for:

possessing professional qualifications, including training and experience, required to administer the information security program functions.

a) having information security duties as that official's primary duty.

b) heading the Cybersecurity office with the mission and resources to assist in ensuring agency compliance with IRS publication 1075.

c) serving as the CIO's primary liaison to the information system owners regarding the application of controls.

Technical Owner

The information system Technical Owner is an IT agency employee, or contracted vendor, responsible for the development, integration, modification, or operation and maintenance of an information system. The Technical Owner is responsible for the development and maintenance of the system security plan and ensures the system is deployed and operated according to the agreed-upon security requirements. The Technical Owner is also responsible for deciding who has administrative access to the information system (and with what types of privileges or access rights) and ensures that system administrators receive the requisite security training. The Technical Owner ensures that appropriate resources are available for the C&A and provides the necessary system-related documentation to the Governance Risk and Compliance (GRC) team. The Technical Owner receives the security assessment results from GRC or the CISO. After taking appropriate steps to reduce or eliminate vulnerabilities, the Technical Owner assembles supporting documentation and artifacts to GRC for adjudication.

GRC Analyst

The GRC Analyst, or GRC as an organization, is responsible for conducting a security certification, or comprehensive assessment of the management, operational, and technical security controls in an information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. GRC also provides recommended corrective actions to reduce or eliminate vulnerabilities in the information system. Prior to initiating the security assessment activities that are a part of the certification process, GRC provides an independent assessment of the system security plan to ensure the plan provides a set of security controls for the information system that is adequate to meet all applicable security requirements.

To preserve the impartial and unbiased nature of the security certification, GRC should be in a position that is independent from the persons directly responsible for the development of the information system and the day-to-day operation of the system. GRC should also be independent of those individuals responsible for correcting security deficiencies identified during the security certification. The independence of GRC is an important factor in assessing the credibility of the security assessment results and ensuring the CIO receives the most objective information possible to make an informed, risk-based, accreditation decision.

IT Architect

One of the most difficult and challenging problems for the CIO, CISO and GRC is identifying appropriate security accreditation boundaries for information systems. Boundaries need to be established before the conduct of initial risk assessments and development of system security plans. Boundaries that are unnecessarily expansive (i.e., including too many hardware, software, and firmware components) make the C&A process extremely unwieldy and complex. Boundaries that are unnecessarily limited (i.e., including too few hardware, software, and firmware components) increase the number of C&A that must be conducted and thus drive up the total security costs for the agency.

Establishing Boundaries

The process of uniquely assigning information resources to an information system defines the security accreditation boundary for that system. The NCDOR IT Architect has great flexibility in determining what constitutes an information system (i.e., major application or general support system) and the resulting security accreditation boundary that is associated with that system. If a set of information resources is identified as an information system, the resources should generally be under the same direct management control. Direct management control does not necessarily imply that there is no intervening management. It is quite possible for multiple information systems to be validly considered subsystems of a single, larger system provided the subsystems fall under the same higher management authority. This situation may arise when other than major applications (i.e., minor applications) are coalesced for purposes of C&A into a general support system. In addition to the consideration of direct management control, it may also be helpful to consider if the information resources being identified as an information system:

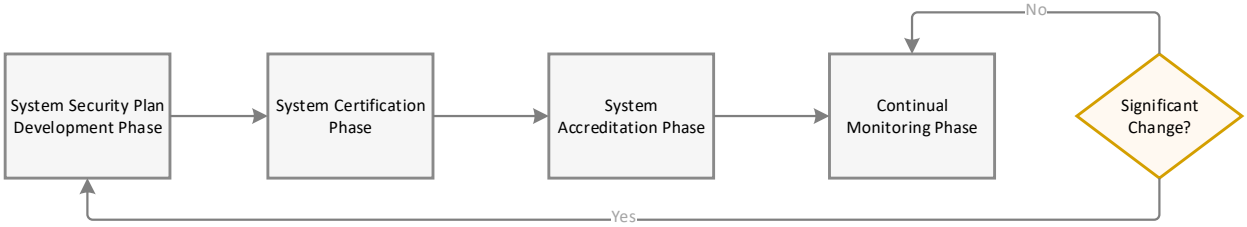
a) Have the same function or mission objective and essentially the same operating characteristics and security needs; and

b) Reside in the same general operating environment (or in the case of a distributed information system, reside in various locations with similar operating environments).

While the above considerations may be useful in determining boundaries for purposes of C&A, they should not be viewed as limiting the agency's flexibility in establishing common sense boundaries that promote effective information security within the available resources of the agency. The IT Architect should consult with prospective Technical Owners, CISO and GRC when establishing boundaries. The process of establishing boundaries is an agency-level activity that should include careful negotiation among all

key participants—considering the mission/business requirements of the agency, the technical considerations with respect to information security, and the programmatic costs to the agency.

THE PROCESS PHASES



SYSTEM SECURITY PLAN DEVELOPMENT PHASE

It is essential that CIO have the most complete, accurate, and trustworthy information possible on the security status of their information systems to make timely, credible, risk-based decisions on whether to authorize operation of those systems. The development of system security plans is an important activity in the agency's information security program that directly supports security accreditation. System security plans provide an overview of the information security requirements and describe the security controls in place or planned for meeting those requirements. System security plans can include as references or attachments, other important security-related documents (e.g., risk assessments, contingency plans, incident response plans, security awareness and training plans, information system rules of behavior, configuration management plans, security configuration checklists, privacy impact assessments, system interconnection agreements) produced as part of an agency's information security program. At a minimum, to consider system certification, the system security plan must include:

System Security Plan Deliverables

a) System Architecture

b) System Risk Analysis

c) Data Classification

d) Control Responsibility Matrix

e) Scans using the appropriate Safeguard Computer Security Evaluation Matrix (SCSEM) provided by the IRS.

f) Scans for vulnerability patches.

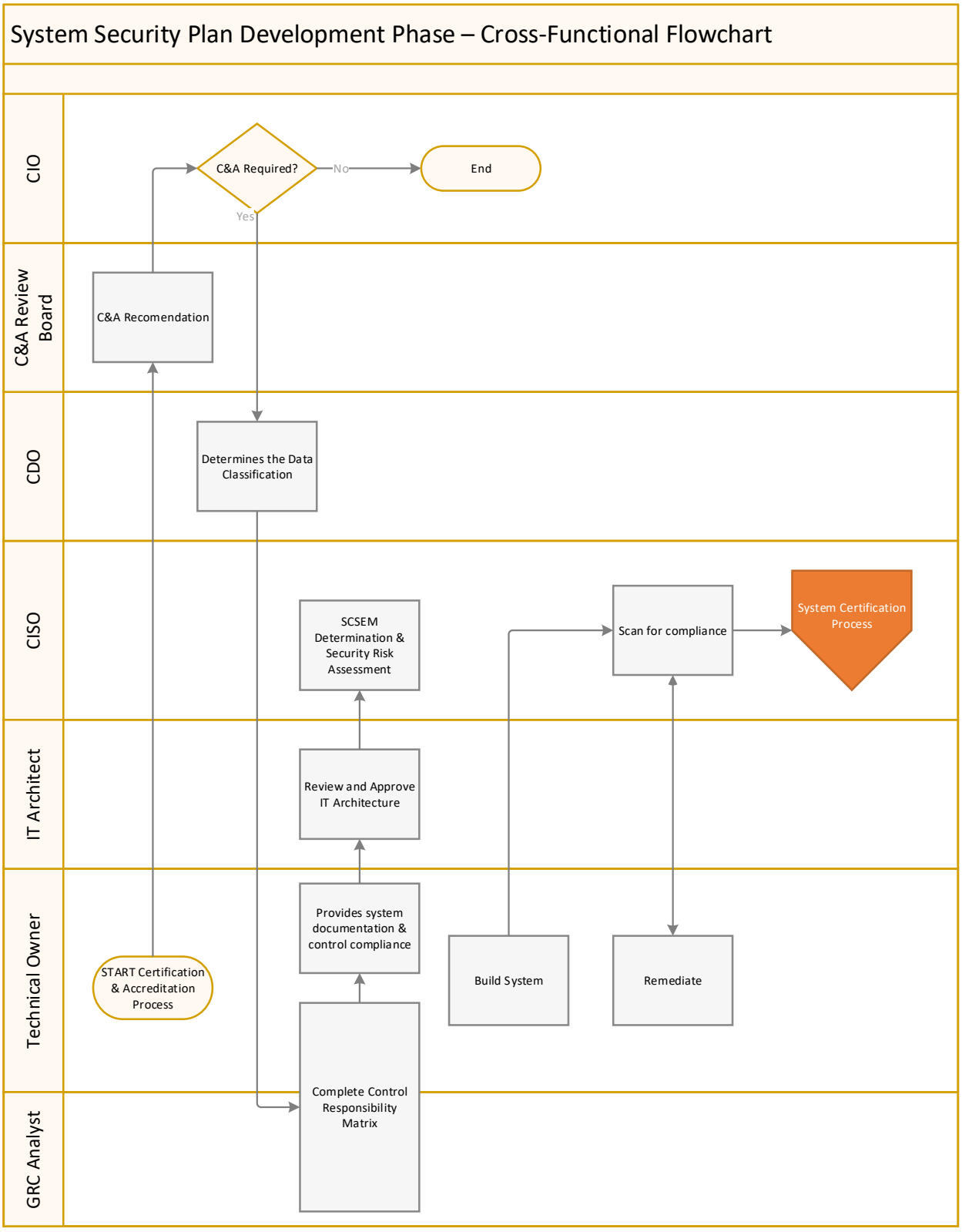
For new systems the C&A process documents will largely be produced in this phase. For existing systems that are undergoing significant change, a review team will make recommendations as to the scope of the C&A process to the CIO for determination. The review team will consist of GRC, the IT Architect and the CISO. For example, recommendations can include:

a) Update the existing System Security Plan (SSP) and add tasks to the annual certification process only.

b) Update the existing SSP and only perform compliance actions on the new parts of the system.

c) Perform a full C&A process.

System Security Plan Development Phase Cross-Functional Flowchart



System Security Plan Phase Tasks

System Build

a) ACTION: The system will be built according to the approved IT Architecture. Any deviation from the approved architecture will restart the system security plan process.

b) RESPONSIBILITY: Technical Owner

c) GUIDANCE: It is imperative that the system as built matches the approved architecture to prevent unnecessary consultations with the IT Architect. It is a best practice to build out the system and then document the architecture. It may be desirable to also apply the SCSEMs to ensure that the system will operate once hardened. Architecture changes may be necessary once SCSEMs are applied, and vulnerabilities remediated.

Information System Architecture

a) ACTION: Complete the Documentation of the Information System Architecture.

b) RESPONSIBILITY: IT Architect, Technical Owner

c) GUIDANCE: The NCDOR IT Architect will provide the standards and information required to be completed by the Technical Owner.

Data Classification Determination

a) ACTION: Determine the Data Classification of the Information System

b) RESPONSIBILITY: NCDOR Chief Data Officer, Technical Owner

c) GUIDANCE: The NCDOR Chief Data Officer will determine the data classification of the Information System in consultation with the Technical Owner.

Security Risk Assessment

a) ACTION: Complete a security risk assessment for the information system

b) RESPONSIBILITY: CISO, Technical Owner

c) GUIDANCE: The CISO or his delegate will be responsible for completing a risk assessment of the information system to determine the key areas of concern.

SCSEM Selection

a) ACTION: Appropriate IRS provided SCSEM is identified by the CISO. SCSEMs are published by IRS Safeguards. https://www.irs.gov/privacy-disclosure/computer-security-compliance-references-and-related-topics

b) RESPONSIBILITY: NCDOR CISO, Technical Owner

c) GUIDANCE: The NCDOR CISO will determine the appropriate IRS SCSEMs for the information system.

Security Controls Responsibility Matrix

a) ACTION: IRS Publication 1075 controls will be assigned to responsible parties

b) RESPONSIBILITY: GRC, Technical Owner

c) GUIDANCE: A control responsibilities matrix will be completed so that all parties are clear on which controls they are responsible for in the information system.

Compliance Scans

a) ACTION: Scans of the information system will be performed to ensure compliance with the SCSEM and that all know vulnerabilities are patched within 30 days. No findings that are Critical, High are allowed.

b) RESPONSIBILITY: NCDOR CISO, Technical Owner

c) GUIDANCE: The CISO and Technical Owner will determine who is to perform the scans and the frequency of those scans. Scans will be evaluated by the CISO or their delegate. Scans are not considered acceptable until only low risk findings exist, or higher risk findings have approved security exceptions.

Request System Certification

a) ACTION: The Technical Owner will request that the system be certified.

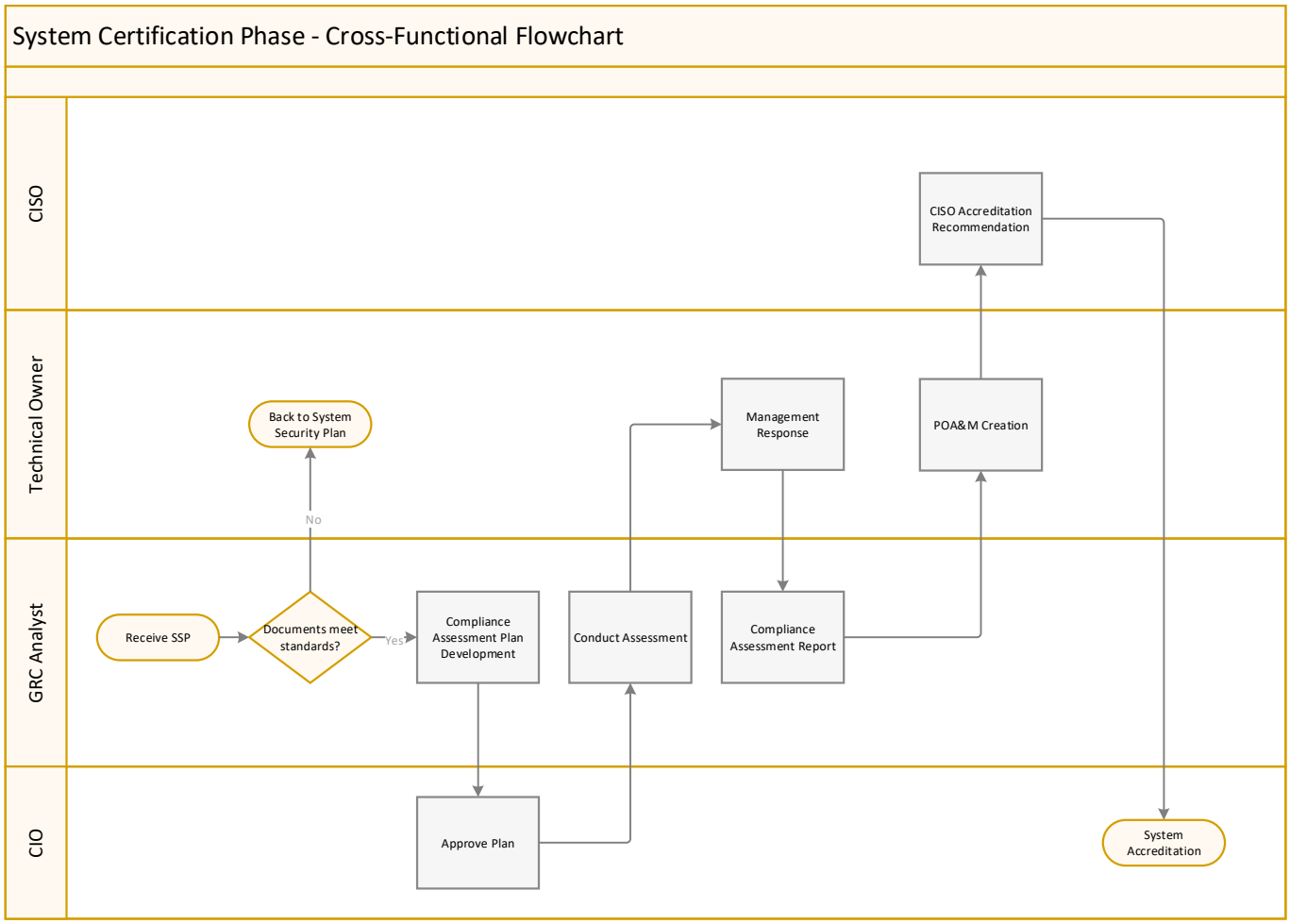
b) RESPONSIBILITY: Technical Owner

c) GUIDANCE: Once the system security plan is completed, the Technical Owner requests that the system be certified by GRC. If the system security plan is not complete or do not meet the standards set forth by GRC, the certification request will be denied and the system security plan process will restart.

SYSTEM CERTIFICATION PHASE

The Security Certification Phase consists of a security control assessment and security certification documentation. The purpose of this phase is to determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. This phase also addresses specific actions taken or planned to correct deficiencies in the security controls and to reduce or eliminate known vulnerabilities in the information system. Upon successful completion of this phase, the CIO will have the information needed to determine the risk to agency operations, agency assets, or individuals and will be able to render an appropriate security accreditation decision for the information system.

System Certification Cross-Functional Flowchart



System Certification Tasks

Documentation Review and Acceptance

a) ACTION: GRC reviews the System Security Plan and accepts or rejects the submission.

b) RESPONSIBILITY: GRC

c) GUIDANCE: GRC will review the System Security Plan and ensure that it meets the submission standards set by GRC. If the submission is rejected, the C&A process restarts so that each task can be revalidated and ensure that the documentation meets the GRC submission standards.

Compliance Assessment Plan and Approval

Identifying appropriate resources (e.g., supporting organizations, funding, and individuals with critical skills) needed for the C&A effort is an essential aspect of planning the compliance assessment. Once a GRC Analyst is selected (or certification services procured), an execution plan for conducting the security certification and accreditation is prepared. The execution plan contains specific tasks, milestones, and delivery schedule.

The level of effort required for security certification depends on:

a) the size and complexity of the information system.

b) the security controls employed to protect the system.

c) the specific methods and procedures used to assess the security controls in the system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

Preparation for the compliance assessment involves gathering appropriate planning and supporting materials, system requirements and design documentation, security control implementation evidence, and results from previous security assessments, security reviews, or compliance assessments. Preparation also involves developing specific methods and procedures to assess the security controls in the information system.

The Technical Owner should assist the GRC Analyst in gathering all relevant documents and supporting materials that will be required during the assessment of the security controls. Descriptive information about the information system is typically documented in the system identification section of the system security plan or in some cases, included by reference or as attachments to the plan. Supporting materials such as procedures, reports, logs, and records showing evidence of security control implementation should be identified as well. Assessing the security controls in an information system can be a very costly and time-consuming process.

In lieu of developing unique or specialized methods and procedures to assess the security controls in the information system, GRC Analysts should consult IRS audit standards or NIST Special Publication 800-53A, which provides standardized methods and procedures for assessing the security controls listed in NIST Special Publication 800-53. The GRC Analyst, if directed by the CIO or CISO, can supplement these assessment methods and procedures. Assessment methods and procedures may need to be created for those may need to be created for those security controls employed that are not contained in IRS 1075 or NIST Special Publication 800-53. Additionally, assessment methods and procedures may need to be tailored for specific system implementations.

In lieu of developing unique or specialized methods and procedures to assess the security controls in the information system, GRC Analysts should consult IRS audit standards or NIST Special Publication 800-53A, which provides standardized methods and procedures for assessing the security controls listed in NIST Special Publication 800-53. The GRC Analys, if directed by the CIO or CISO, can supplement these assessment methods and procedures. Assessment methods and procedures may need to be created for those.

a) ACTION: GRC reviews the System Security Plan and creates an audit plan for the CIO. The CIO will review and approve the audit plan and authorizes the resources that will be needed to conduct the audit.

b) RESPONSIBILITY: GRC, CIO

c) GUIDANCE: GRC is a subject matter expect on compliance and may use a variety of tools and frameworks to build an appropriate audit. GRC will consult with the CIO in the construction of the audit plan.

Conduct Compliance Assessment

The objective of the compliance assessment task is to conduct the assessment of the compliance of security controls and document the results of the assessment. The GRC Analyst, at the completion of this task, will be able to determine the extent to which the security controls in the information system are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the compliance requirements for the system. The GRC Analyst will also be able to make recommendations on corrective actions for security control deficiencies and offer advice to the Technical Owner and CIO on how the known vulnerabilities in the system translate into agency risk level.

a) ACTION: GRC will conduct the compliance assessment as approved.

b) RESPONSIBILITY: GRC, Technical Owner

c) GUIDANCE: GRC will conduct the compliance assessment as planed in collaboration with the Technical Owner. The compliance assessment determines the extent to which the security controls are

implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. The results of the compliance assessment, including recommendations for correcting any deficiencies in the security controls, are documented in the compliance assessment report

Compliance Assessment Report

a) ACTION: Prepare the final compliance assessment report.

b) RESPONSIBILITY: GRC Analyst

c) GUIDANCE: The compliance assessment report contains the results of the compliance assessment and recommendations for correcting deficiencies in the controls and reducing or eliminating identified vulnerabilities. The compliance assessment report is part of the final accreditation package along with the updated system security plan and plan of action and milestones. The compliance assessment report is the certification agent's statement regarding the compliance status of the information system. The Technical Owner has an opportunity to reduce or eliminate vulnerabilities in the information system prior to the assembly and compilation of the compliance assessment report and submission to the CIO. This is accomplished by implementing corrective actions recommended by the GRC Analyst. The GRC Analyst should assess any security controls modified, enhanced, or added during this process.

Plan of Action and Milestone Development

a) ACTION: Prepare the plan of action and milestones based on the results of the compliance assessment.

b) RESPONSIBILITY: GRC Analyst, Technical Owner.

c) GUIDANCE: The plan of action and milestones document, one of the three key documents in the security accreditation package, describes actions taken or planned by the Technical Owner to correct deficiencies in the security controls and to address remaining vulnerabilities in the information system (i.e., reduce, eliminate, or accept the vulnerabilities). The plan of actions and milestones document identifies the tasks needing to be accomplished, any milestones in meeting the tasks and scheduled completion dates for milestones.

CISO Accreditation Recommendation

a) ACTION: The CISO reviews the accreditation package and makes a recommendation to the CIO regarding the risk to agency operations, agency assets, or individuals based on the vulnerabilities in the information system and any planned or completed corrective actions to reduce or eliminate those vulnerabilities.

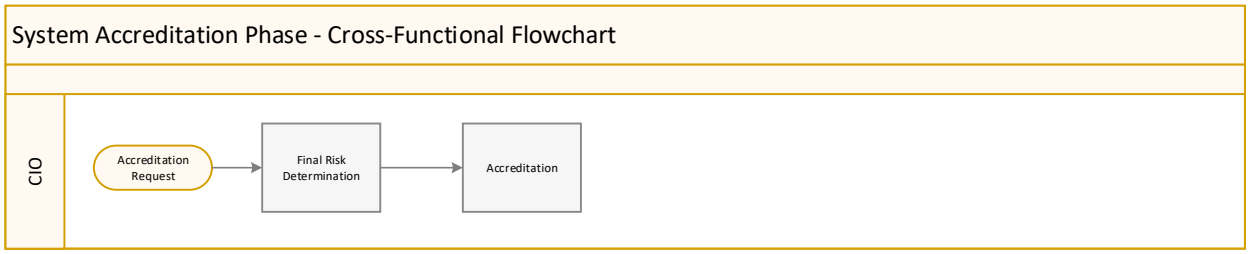
b) RESPONSIBILITY: CISO.

c) GUIDANCE: The CISO should have sufficient information to be able to determine the risk to agency operations, agency assets, or individuals based on the vulnerabilities in the information system and any planned or completed corrective actions to reduce or eliminate those vulnerabilities. This is the opportunity for the CISO to let the CIO know of any specific security issues and make recommendations that the CIO should consider when determined to allow the system to operate or not.

SYSTEM ACCREDITATION PHASE

The purpose of this phase is to determine if the remaining known vulnerabilities in the information system (after the implementation of an agreed-upon set of security controls) pose an acceptable level of risk to agency operations, agency assets, or individuals. Upon successful completion of this phase, the Technical Owner will have an authorization to operate the information system or denial of authorization to operate the information system.

System Accreditation Cross-Functional Flowchart



Final Risk Determination

The objective of the final risk determination is to determine the risk to agency operations, agency assets, or individuals and determine if the agency-level risk is acceptable.

The CIO, working with information from the Technical Owner, CISO, and GRC Analyst produced during the previous phase, has independent confirmation of the identified vulnerabilities in the information system and a list of planned or completed corrective actions to reduce or eliminate those vulnerabilities. It is this information that is used to determine the final risk to the agency and the acceptability of that risk.

a) ACTION: Determine the risk to agency operations, agency assets, or individuals based on the vulnerabilities in the information system and any planned or completed corrective actions to reduce or eliminate those vulnerabilities.

b) RESPONSIBILITY: CIO

c) GUIDANCE: The vulnerabilities in the information system confirmed by the GRC Analyst should be assessed to determine how those vulnerabilities translate into risk to agency operations, agency assets, or individuals. The CIO should judge which information system vulnerabilities are of greatest concern to the agency and which vulnerabilities can be tolerated without creating unreasonable agency-level risk. The plan of action and milestones (i.e., actions taken or planned to correct deficiencies in the security controls and reduce or eliminate vulnerabilities) submitted by the Technical Owner should also be considered in determining the risk to the agency. The CIO may consult the Technical Owner, GRC Analyst, CISO or others before making the final risk determination.

Accreditation

The CIO creates the final security accreditation decision letter. The letter includes the accreditation decision, the rationale for the decision, the terms and conditions for information system operation, and required corrective actions, if appropriate. The accreditation decision letter indicates to the Technical Owner whether the system is authorized to operate or not authorized to operate.

The supporting rationale provides the Technical Owner with the justification for the CIO's decision. The terms and conditions for the authorization provide a description of any limitations or restrictions placed on the operation of the information system that must be adhered to by the information system owner. The security accreditation letter is included in the final accreditation package. The contents of the accreditation package should be protected appropriately in accordance with agency policy.

a) ACTION: Determine if the risk to agency operations, agency assets, or individuals is acceptable and prepare the final security accreditation decision letter. Provide copies of the final security accreditation package including the accreditation decision letter to the Technical Owner, CISO, GRC, and any other agency officials having an interest (i.e., need to know) in the security of the information system.

b) RESPONSIBILITY: CIO

c) GUIDANCE: If, after assessing the results of the security certification, the CIO deems that the agency-level risk is acceptable, an authorization to operate (ATO) is issued. The information system is accredited without any restrictions or limitations on its operation. If, after assessing the results of the security certification, the CIO deems that the agency-level risk is unacceptable, the information system is not authorized for operation and thus is not accredited. Upon receipt of the security accreditation decision letter and accreditation package, the Technical Owner accepts the terms and conditions of the authorization. The CIO, CISO and GRC retain copies of the decision letter and accreditation package. The accreditation package contains important documents and as such, should be appropriately safeguarded and stored, whenever possible, in a centralized agency filing system to ensure accessibility. The accreditation package should also be readily available to auditors and oversight agencies upon request. The accreditation package should also be readily available to auditors and oversight agencies upon request. The accreditation package including all supporting documents, should be retained in accordance with the agency's records retention policy.

CONTINIOUS MONITORING PHASE

The Continuous Monitoring Phase consists of configuration management & control, security control monitoring and status reporting and documentation. The purpose of this phase is to provide oversight and monitoring of the security controls in the information system on an ongoing basis and to inform the CIO when changes occur that may impact on the security of the system. The activities in this phase are performed continuously throughout the life cycle of the information system. Reaccreditation may be required because of specific changes to the information system or because IRS, state or agency policies require periodic reaccreditation of the information system.

Continuous Monitoring Tasks

Documentation of System Changes

The objective of the documentation of system changes task is to document the proposed or actual changes to the system and determine the impact of proposed or actual changes on the security of the system. A system will typically be in a constant state of migration with upgrades to hardware, software, or firmware and possible modifications to the system environment. Documenting information system changes and assessing the potential impact on the security of the system on an ongoing basis is an essential aspect of maintaining the security accreditation.

a) ACTION: Using configuration management and control procedures, document proposed or actual changes to the information system (including hardware, software, firmware, and surrounding environment).

b) RESPONSIBILITY: Technical Owner

c) GUIDANCE: An orderly and disciplined approach to managing, controlling, and documenting changes to an information system is critical to the continuous assessment of the security controls that protect the system. It is important to record any relevant information about the specific proposed or actual changes to the hardware, firmware, or software such as version or release numbers, descriptions of new or modified features or capabilities, and security implementation guidance. It is also important to record any changes to the information system environment such as modifications to the physical plant. The Technical Owner and CISO should use this information in assessing the potential security impact of the proposed or actual changes to the information system. Significant changes to the information system should not be undertaken prior to assessing the security impact of such changes.

Security Impact Analysis

a) ACTION: Analyze the proposed or actual changes to the information system (including hardware, software, firmware, and surrounding environment) to determine the security impact of such changes.

b) RESPONSIBILITY: CISO

c) GUIDANCE: Changes to the information system may affect the security controls currently in place, produce new vulnerabilities in the system, or generate requirements for new security controls that were not needed previously. If the results of the security impact analysis indicate that the proposed or actual changes to the information system will affect or have affected the security of the information system, corrective actions should be initiated, and the plan of action and milestones revised. The Technical Owner or CISO may wish to consult with other agency officials prior to implementing any security-related changes to the information system. Conducting a security impact analysis is part of the ongoing assessment of risk within the agency.

System Security Plan Update

a) ACTION: Update the system security plan based on the documented changes to the information system (including hardware, software, firmware, and surrounding environment) and the results of the continuous monitoring process.

b) RESPONSIBILITY: Technical Owner.

GUIDANCE: The system security plan should contain the most up-to-date information about the information system. Changes to the information system should be reflected in the system security plan. The frequency of system security plan updates is at the discretion of the Technical Owner. The updates should occur at appropriate intervals to capture significant changes to the information system, but not so frequently as to generate unnecessary paperwork. The CIO, CISO, Technical Owner, and GRC Analyst will be using the system security plan to guide any future security certification and accreditation activities, when required.

Plan of Action and Milestones Update

a) ACTION: Update the plan of action and milestones (POA&M) based on the documented changes to the information system (including hardware, software, firmware, and surrounding environment) and the results of the continuous monitoring process.

b) RESPONSIBILITY: Technical Owner, GRC.

c) GUIDANCE: The plan of action and milestones is used by GRC to monitor the progress in correcting deficiencies noted during the security certification. The plan of action and milestones should:

i) report progress made on the current outstanding items listed in the plan.

ii) address vulnerabilities in the information system discovered during the security impact analysis or security control monitoring.

iii) describe how the information system owner intends to address those vulnerabilities (i.e., reduce, eliminate, or accept the identified vulnerabilities).

The frequency of the plan of action and milestones updates is quarterly. The CIO, CISO, GRC will be using the plan of action and milestones to guide any future security certification and accreditation activities, when required.

Status Reporting

a) ACTION: Report the security status of SCSEM controls and vulnerability patching of the information system to the CISO.

b) RESPONSIBILITY: Technical Owner.

c) GUIDANCE: The security status report should consist of compliance scans that show the status of compliance with SCSEM controls, and that all Critical & High-level vulnerabilities are in compliance.

ATTACHMENT T: INTERNAL REVENUE SERVICE PUBLICATION 1075, EXHIBIT 7 SAFEGUARDING CONTRACT LANGUAGE

Internal Revenue Service Publication 1075, Exhibit 7 Safeguarding Contract Language

The North Carolina Department of Revenue ("NCDOR" or "Agency") has determined that in the performance of this contract or agreement, contractor will be provided data that is classified as Federal Taxpayer Information, State Taxpayer Information, and/or Personal Identifying Information, herein referred to as "FTI", "STI", "PII", or collectively as "return or return information." Prior to NCDOR granting a contractor access to return or return information, contractor agrees to the following:

I. PERFORMANCE

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

All work will be done under the supervision of the contractor.

The contractor and contractor's officers or employees to be authorized access to return or return information must meet background check requirements defined in IRS Publication 1075. The contractor will maintain a list of officers or employees authorized access to return or return information. Such list will be provided to the agency and, upon request, to the IRS.

Any return or return information in hardcopy or electronic format shall be used only for the purpose of carrying out the provisions of this contract or agreement. Return or return information in any format 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 this contract or agreement. Inspection or disclosure to anyone other than the contractor or the contractor's officers or employees authorized is prohibited.

Return and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

The contractor will certify that the data processed during the performance of this contract or agreement will be completely purged from all physical and electronic data storage with no output to be retained by the contractor at the time the work is completed. If immediate purging of all physical and electronic data storage is not possible, the contractor will certify that any return or return information in physical or electronic storage will remain safeguarded to prevent unauthorized disclosures.

Any spoilage or any intermediate hard copy printout that may result during the processing of return or return information will be given to the agency. 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 agency with a statement containing the date of destruction, description of material destroyed, and the destruction method.

All computer systems receiving, processing, storing or transmitting return or return information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to return or return information.

Prior to providing access to return or return information, NCDOR requires the contractor's officers or employees providing services under this contract or agreement to complete DOR Security Awareness Training (DORSAT) and sign the NCDOR Non-Disclosure Agreement and Security Awareness Training Acknowledgement form. As part of the certification process, contractors are advised of the provisions of Internal Revenue Code §§7431,

7213, and 7213A. Contractors must maintain their access authorization through annual recertification. See Section II, Paragraph 5 below.

No work involving return or return information furnished under this contract will be subcontracted without prior written approval of the IRS.

Contractor will ensure that the terms of return or return information safeguards described herein are included, without modification, in any approved subcontract of work involving return or return information.

To the extent the terms, provisions, duties, requirements, and obligations of this contract or agreement apply to performing services with return or return information, the contractor shall assume toward the subcontractor all obligations, duties, and responsibilities that the agency under this contract or agreement assumes toward the contractor, and the subcontractor shall assume toward the contractor all the same obligations, duties, and responsibilities which the contractor assumes toward the agency under this contract or agreement.

In addition to the subcontractors' obligations and duties under an approved subcontract, the terms and conditions of this contract apply to the subcontractor, and the subcontractor is bound and obligated to the contractor hereunder by the same terms and conditions by which the contractor is bound and obligated to the agency under this contract or agreement.

For the purposes of this contract, the term "contractor" includes any officer or employee of the contractor with access to or who uses return or return information, and the term "subcontractor" includes any officer or employee of subcontractor with access to or who uses return or return information.

The agency will have the right to void the contract if the contractor fails to provide the safeguards described above.

II. CRIMINAL/CIVIL SANCTIONS

Each officer or employee of a contractor to whom return or return information is or may be disclosed shall be notified in writing that return 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 return or return information for a purpose not authorized 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.

Each officer or employee of a contractor to whom return or return information is or may be accessible shall be notified in writing that any return or return information accessible to such office or employee may be accessed only for the purpose and to the extent authorized herein, and that access/inspection of return or return information without an official need-to-know for a purpose no authorized herein 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.

Each officer and employee of a contractor to whom return or return information is or may be disclosed shall be notified in writing that any such unauthorized access, inspection, or disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount equal to the sum of the greater of $1,000 for each unauthorized access, inspection, or disclosure or the sum of actual damages sustained as a result of such unauthorized access, inspection, or disclosure, plus in the case of a willful unauthorized access, inspection, or disclosure or an unauthorized access/inspection which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC §§ 7213, 7213A and 7431 and set forth in 26 CFS 301.6103(n)-1.

Additionally, it is incumbent of 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.

Granting a contractor access to return or return information must be preceded by certifying that each officer or employee understands the agency's security policy and procedures for safeguarding return or return information. A contractor and each officer or employee must maintain their authorization to access return or return information through annual recertification of their understanding of the agency's security policy and procedures for safeguarding return or return information. The initial certification and re-certifications must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, a contractor and each officer or employee must be advised of the provisions of IRC §§ 7213, 7213A, and 7431. (See IRS Publication 1075 Exhibit 4, Sanctions for Unauthorized Disclosure, and Exhibit 5, Civil Damages for Unauthorized Disclosure.) The training on the agency's security policy and procedures provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See IRS Publication 1075 Section 1.8, Reporting Improper Inspections or Disclosures.) For the initial certification and the annual re-certifications, the contractor and each officer or employee must sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the NCDOR shall have the right to send its officers and employees into the offices and plants of the contractor for inspection of the facilities and operations provided for the performance of any work with return or return information under this contract or agreement for compliance with requirements defined in IRS Publication 1075. The IRS's right of inspection shall include the use of manual and/or automatic scanning tools to perform compliance and vulnerability assessments of information technology (IT) assets that access, store, process, or transmit return or return information. Based on the inspection, specific corrective actions may be required in cases where the contractor is found to be noncompliant with contract safeguards.

For additional information on IRS Publication 1075, along with detailed requirements and standards for Tax Information Guidelines for Federal, State and Local Agencies, please see http://www.irs.gov/pub/irs-pdf/p1075.pdf.

In addition to IRS Publication 1075 Exhibit 7Safeguarding Requirements, please be advised that under North Carolina General Statutes, contractor (and any subcontractors) may be subject to additional criminal and civil sanctions for unauthorized disclosures of STI or PII as follows:

A person who commits an unauthorized disclosure of return or return information is guilty of a Class 1 misdemeanor under N.C. Gen. Stat. § 105-259 (c). Further, if that individual is an officer or employee of the State, that person shall be dismissed from public office or public employment and may not hold any public office or employment in the State of North Carolina for five (5) years after the violation.

Any person who is injured as a result of an unauthorized disclosure of PII may sue for civil damages pursuant to N.C. Gen. Stat. §§ 75-65, 75-66, and 1-539.2C. For each unauthorized disclosure, the damages may be the greater of (a) an amount of up to $5000 (but no less than $500) or (b) three (3) times the amount of actual damages.

Burden of Security Breach Notifications:

The contractor must notify NCDOR of any real or suspected security breach immediately and will coordinate with NCDOR any external communications or notifications to affected individuals. The contractor will be responsible and bear the financial cost of mailing out any required notifications to any affected taxpayers involved in a security breach or unauthorized disclosure while data is in the possession of the Vendor. See NC Gen. Stat. §. 75-65 Protection from security breaches, for details on who is required to be notified and how those notifications are to be made in the event of a PII security breach. However, NCDOR will be responsible for reporting to any related agencies or entities.

ATTACHMENT U: SECURITY REQUIREMENTS FOR VENDOR STAFF AND CONTRACTORS

Security Requirements for Vendor Staff and Contractors

All Vendor-provided and Contract Staff (e.g. seasonal temps) must fulfill required security checks prior to beginning work at NCDOR. Required security checks vary based on system and information access level, and generally follow the principle of least privilege. Attachment U.1 – Vendor and Contractor Security Requirements Matrix provides a guide for the most common levels of access and the corresponding security requirements for each level. NCDOR IT Security will advise and approve access levels not represented on Attachment U.1.

Required documentation must be submitted to the NCDOR Contract Manager prior to beginning work at NCDOR.

Guidelines include the following:

a) Attachment U.1 – Vendor and Contractor Security Requirements Matrix, with the Requirements explained below.
b) IT Security review and approval if special access is required

Requirements Definitions:

a) **Nondisclosure Agreement:** Any staff performing any work under this contract must sign a NCDOR non-disclosure agreement (NDA) agreeing to maintain the confidentiality of any Agency Data to which the Vendor Staff and/or Contractor may have access.

b) **Criminal Background Checks:** Any staff who will be receiving or who will have access to NCDOR Data must submit to and pass a criminal background check to be conducted by NCDOR. These checks will be repeated every five (5) years. NCDOR determines the conditions for passing background checks.

c) **Fingerprinting:** The criminal background check referenced above must include completion of Federal Bureau of Investigation (FBI) fingerprinting, which is conducted to identify possible suitability issues. These checks will be repeated every five (5) years. Suitability issues are determined by NCDOR.

d) **Security Awareness Training:** NCDOR will provide annual Security Awareness Training (DORSAT). Each person who is performing work under this contract on behalf of the Vendor and/or Contractor must provide a valid work email to the NCDOR Contract Manager for annual DORSAT notifications.

e) **IT Role-Based Security Training:** The Vendor and/or Contractor must provide annual IT role-based security training for all applicable staff. The IT role-based training details and scope can be found in IRS Publication 1075 (rev. 11-2021) – Control AT-3. NCDOR will randomly audit compliance with this requirement.

f) **A copy of NCDOR's Security Policy Manual can be found at the following link:**

https://www.ncdor.gov/documents/dor-security-policy-manual

ATTACHMENT U.1 – VENDOR AND CONTRACTOR SECURITY REQUIREMENTS MATRIX

NOTE: Read all indicated footnotes carefully as these contain important information

Level of Access	NDA	NCDOR Policy Manual Provided	*Background Check	Security Awareness Training	Role-Based Training
[1]**Escorted access – Must Be Escorted at All Times**	YES	YES	NO	NO	NO
Physical Access – Non-Escorted (Badge Access)	YES	YES	YES	YES	YES
[2]**Logical Access to NCDOR Data/Systems/Information (Has an Account)**	YES	YES	YES	YES	YES
[3]**Logical Access to NCDOR Data/Systems/Information (Does Not Have an Account)**	YES	YES	NO	NO	NO
[4]**Offsite Contractor Staff with Physical Access to NCDOR Data/Systems/Information**	YES	YES	YES	YES	YES
Access to Unencrypted Paper or Electronic NCDOR Data	YES	YES	YES	YES	YES
[5]**Logical Access to Encrypted Data**	YES	YES	NO	NO	NO

* Background check requirements include FBI fingerprinting and criminal background checks. For a full list of requirements, please refer to the NCDOR Security Policy Manual

1. Individuals may utilize NCDOR equipment as long as they will be supervised with the equipment at all times. Unsupervised access to equipment requires a unique account that ties back to the individual and all account requirements listed in this matrix are required.

2. Accounts must be unique and must tie back to the individual.

3. Applies to individuals that will potentially view Agency Data on screens as part of logical maintenance of systems, but who do not have an account. Agency Data cannot be sent outside of the Agency without NCDOR Chief Information Officer (CIO) approval. Maintenance activities (including remote maintenance) must be supervised by badged NCDOR staff or by a badged NCDOR management-approved designee. Any systems used to facilitate remote supervision must be secure and approved by NCDOR IT Security.

4. Access to data is defined for these purposes as individuals that have access through the first barrier of the two-barrier rule. See IRS Publication 1075 – Minimum Protections Standards for more information.

5. Encryption methods must be FIPS 140-3 compliant.

ATTACHMENT V: NC STATUTORY REFERENCES

See Excel Workbook: Attachment V: NC Statutory References (No Response Required)

ATTACHMENT W: VENDOR EXPERIENCE

Relevant Experience

Use Table 3 below to describe up to three (3) projects where the Vendor was the primary Contractor that demonstrates the company's qualifications and a successful track record in leading the design, development, and deployment of a software solution. NCDOR prefers projects of similar size and complexity based on information in Table 2 Business Activity Statistics and Attachment M: Tax Schedule Matrix. Describe and highlight experience with providing self-service capabilities and implementing complex business rules and calculations. The Agency prefers descriptions of up to three (3) example projects started or completed within the past seven (7) years.

For the projects listed, complete Attachment G: References.

The major tax schedules such as Individual Income tax, Withholding tax, Sales & Use tax, Partnership and Corporate tax are within the scope of this Program and currently processed on the legacy integrated tax system. Describe your experience working with a customer to convert and implement tax types from an existing integrated tax system to the proposed tax system solution which required multiple implementation phases.

Table 3. Relevant Experience (please repeat table for each recent project)

Relevant Experience			
Client Organization/Location			
X			
Project Begin Date	**Project End Date**	**Project Cost (Award)**	**Project Cost (Completion)**
X	X	X	X
Describe the project scope, number of users and implementation timeline (major milestones)			
X			
Describe functionality similar to that requested by the Agency			
X			
List any taxes implemented that are similar to the tax schedules listed in Attachment M			
X			
Describe any challenges faced during the project and how they were managed/overcome			
X			
Please explain any delays to the originally proposed implementation schedule			
X			
Describe the Vendor's current level of operations and maintenance support			
X			

Describe any lessons learned from other similar projects, including:

a) any project or performance risks that should be addressed and/or mitigated.

b) critical factors to discuss during each phase of the project milestones.

c) technical, functional, or operational expectations/responsibilities that the Agency should undertake for project success.

d) risk mitigation concepts for both Vendor and Agency for this type of Program.