Appendix D –Technical Assessment Form

TECHNICAL ASSESSMENT FORM
Finance & Accounting ERP System

Bidder's Organization Name: _____

Bidders and their solutions must adhere to all applicable State and Federal standards, policies, and laws that correspond to the PII impact level of MTA data that will be stored, accessed, transmitted and/or controlled by the solution. These standards include the requirements listed here, as well as any other applicable legal standards, which may not be listed here. For "Type of Data" column below, respond "Yes", "No", or "N/A" in the "Comply" column and provide an explanation as applicable.

Applicable State & Federal		Comply?	Explanation
Publicly available information	§ NIST 800-171		
	§ Maine Freedom of Access Act (Title 1 MRSA c. 13) and exceptions thereto.		
Confidential Personally Identifiable Information (PII)	§ State of Maine Breach Notification Law		
	§ National Institute of Standards & Technology: NIST SP 800-53 Revision 5 "Moderate" risk controls		
	§ Privacy Act of 1974, 5 U.S.C. 552a.		
	§ Security regulations from the U.S. DHHS, Administration for Children and Families, Office of Child Support Enforcement Program, Office of Child Support Enforcement (OCSE)		
Payment Card Information	§ Payment Card Industry Data Security Standard (PCI DSS) v 4.0		
	§ Nacha Operating Rules (ACH)		
Federal Tax Information	§ Internal Revenue Service Tax Information Security Guidelines for Federal, State and Local Agencies: IRS Pub 1075		
	§ IRS Pub 1075 Contractor Language Addendum required		
Personal Information from	§ Driver's Privacy Protection Act (Title XXX) ("DPPA") 18 U.S.C. Chapter 123, §§ 2721 – 2725		

Hosting	Comply?	Explanation
Any technical solution must be hosted in a data center.		
Any hosting provider must provide back-up and disaster recovery models and plans as needed for the solution.		
Any hosting provider will abide by NIST best practices for change requests, incident management, problem management and service desk.		

Application Solution	Comply?	Explanation
Any solutions Bidder must provide for the backup/recover, data retention and disaster recovery of a contracted/hosted application solution.		
Any solutions Bidder must provide for application management and design standard of all technology platforms and environments for the application solution (Development, Staging, Productions, DR, etc.)		
Any solutions Bidder must engage MTA using SLA for system and application performance, incident reporting and maintenance.		
MTA owns any data they enter, migrate, or transmit into the solution and the Bidder shall allow the State to pull or copy this data at any time free of charge in a format defined by MTA.		

Information Security Standards	Comply?	Explanation
Bidder provides and maintains a security plan that: 1. Complies with NIST security requirements; 2. Protects the confidentiality, integrity, and availability of the MTA's information systems; and 3. Comply with all applicable federal and state laws and regulations, as well as compliance with all Maine IT contractual requirements and information security policies.		
Bidder ensures that any agent or subcontractor of the bidder to whom MTA provides access agrees to the same restrictions and conditions that apply through this Agreement and agrees to implement reasonable and appropriate safeguards to ensure the confidentiality, integrity, and availability of MTA's IS.		
Bidder will report a security incident that occurs on the Agency's information systems that may affect MTA or State of Maine systems to the CISO within 24 hours of discovery in accordance with the terms of the Maine IT NDA.		
Provide the stated cyber risk appetite statement that has been approved by the board/leadership of your company.		
Provide the SBOM of the solution you are proposing as part of this bid.		

Cloud Service Provider Requirements	Comply?	Explanation
Configuration Management Policy		
Application Deployment Certification Policy		
Digital Accessibility and Usability Policy		
Remote Hosting Policy		
Data Exchange Policy		
Information Security Policy		
Access Control Policy		
Access Control Procedures for Users		
Risk Assessment Policy		
Vulnerability Scanning Procedure		
Security Assessment and Authorization Policy		
System And Information Integrity Policy		
Configuration Management Policy		
NIST Requirements	**Comply?**	**Explanation**
Physical and Environmental Protection		
Awareness and Training		
Planning		
Audit and Accountability		
Personnel Security		
Contingency Planning		
PII Processing and Transparency		
Identification and Authentication		
Incident Response		
System and Communications Protection		
Maintenance		
Media Protection		