

Request for Proposals
New York State Department of Transportation (on behalf of the)
New York Metropolitan Transportation Council
Regional Household Travel Survey and Development of NYMTC's Long
Term Regional Travel Data Collection Program

Contract No. C004307

Attachment 8.17.1

NYS Information Technology Services Requirements

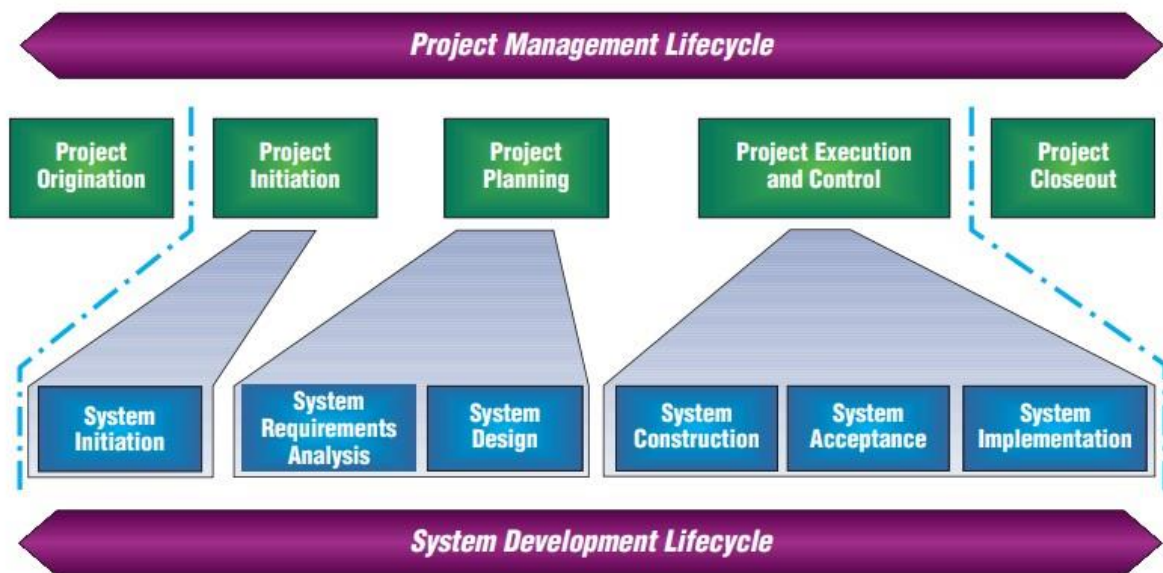
Table of Contents:

- 1. ITS PROJECT AND SYSTEM DEVELOPMENT LIFECYCLE REQUIREMENTS**
- 2. ITS QA/QC AND RELEASE AND DEPLOYMENT PROCESS REQUIREMENTS**
- 4. NEW YORK STATE TECHNOLOGY REQUIREMENTS**
- 5. NEW YORK STATE SECURITY REQUIREMENTS**
- 6. NEW YORK STATE DATA SECURITY REQUIREMENTS**

Please describe your proposed methods regarding the NYS ITS Requirements listed below.

1. ITS PROJECT AND SYSTEM DEVELOPMENT LIFECYCLE REQUIREMENTS

Rqmt. No.	Requirement Description – ITS Project and System Development Lifecycle Requirements
IT1	As applicable, any IT project work performed under this Agreement shall be required to comply with NYS Office of Information Technology Service (ITS) requirements, which features the following:



1. Project Initiation

a. System Initiation: Application Strategy, Architecture and Planning

Include a conceptual architecture diagram and description of the proposed solution. The conceptual architecture should identify and describe the overall hardware; software; database components; programming languages; development tools; documentation tools; and standards for their proposed solution. The Proposer shall provide a detailed text description in its proposal including, but not limited to, the following:

- Depiction of hardware and software layers, storage, interfaces to external systems and communications topology;
- Approach to integrating with existing systems
- Approach to support accessibility for reporting, analysis and data warehousing.
- Approach to ensuring the scalability of the application;
- Support for multiple tiers to enable quality control and assurance, testing and security for migration of new versions or enhancements.
- Approach to supporting Continuity of Operations

2. Project Planning

a. System Requirements Analysis: Detailed Functional and Non-Functional Requirements Definition

Describe the functionality of the system in detail by capturing the intended behavior of the system, expressed as services, tasks or functions.

b. Application/System Design Specification

- c. Describe how the application/system performs the business functional requirements. Include methodology on the infrastructure application, user and data layers, configuration settings, and user interfaces. System Design: Detailed Infrastructure Design

Describe which technologies the proposed solution supports including, but not limited to, its' proposed application solution platforms, databases, interfaces, production, test and training environments. The proposed solution shall be able to run effectively within a shared service, virtual server environment. The technical proposal shall include any and all peripheral hardware required to operate the Proposer's solution.

3. Project Execution and Control

- a. Application/System Construction: Configuration, Programming, Development, Integration, Data Migration, Data Governance

Describe the methodology for application/system construction and development. The approaches for integration with NYS systems and the plan for data management.

- b. Systems Acceptance: System Testing and Acceptance Test Planning

Methodology as outlined Attachment 8.17.2 - ITS CTO DOT QA/QC and Release and Deployment Process.

- c. System Implementation: Product Implementation and Deployment

All builds and configurations must comply with NYS Information Technology and Security Policies, Standards, and Best Practice Guidelines under IT3, IT4 and IT5.

4. Release & Deployment Management

Describe how the solution will be deployed to the Users and managed in throughout the infrastructure tiers as outlined in Attachment 8.17.2 - ITS CTO DOT QA/QC and Release and Deployment Process.

5. Production "Go-Live"

Production Deployment and Support Plan

Transition to Operational Support Plan

6. Post Implementation Warranty

Plans for Post Go-Live support.

NYSDOT envisions that the delivered solution will be highly configurable (i.e., can be adapted to meet changing business needs with minimal custom changes to the underlying software programming code) so that NYSDOT staff can create or configure System forms, workflows, business processes, business rules, and reports without impacting the underlying software code.

During the life of the project, NYSDOT and ITS management will review deliverables and evaluate them for completeness, clarity, adherence to generally recognized standards, and compliance with NYSDOT's intent as conveyed in this RFP and in the resulting contract. A

	deliverable, phase, or milestone will not be considered complete until sign-off has been given by NYSDOT. NYSDOT will only render payment for services and deliverables it accepts.
IT1 – Proposer Detailed Response as how your solution meets this requirement and/or what is your plan, including timeline, for your solution to come into compliance with this requirement:	

2. NEW YORK STATE TECHNOLOGY REQUIREMENTS

RQ MT. NO.	REQUIREMENT DESCRIPTION – NEW YORK STATE TECHNOLOGY REQUIREMENTS
IT2	<p>Scope This content is included in any third-party software contract or Request for Proposal (RFP). Third-party software includes the following:</p> <ul style="list-style-type: none"> • Any cloud-based software or application (solution) • Any hybrid solution (NYS Private Cloud and Vendor Hosted or Public Cloud) • Commercial of the shelf (COTS) software • Government of the shelf (GOTS) software • Any services engagement where custom software is a deliverable <p>This document <u>does not</u> apply to desktop software or low-level software utilities.</p> <p>Exceptions to these requirements must be directed to the agencies assigned ITS Enterprise Architect.</p> <p>Required for All Solutions All solutions must adhere to ITS-P20-001 System Integration Policy and ITS-S20-001 Service Oriented Architecture Standard. In summation, all system integrations that includes business information must adhere to the following requirements:</p> <ul style="list-style-type: none"> • The system integration must be implemented using one of the following protocols: <ul style="list-style-type: none"> ○ Representative State Transfer (REST) ○ Simple Object Access Protocol (SOAP) Web Service ○ Message exchange using an official ITS supported middleware ○ Secure File Transfer Protocol ○ Extract Transform and Load (ETL)

- All interfaces to ITS managed systems must use an ITS supported intermediary.
- All integrations provided by the vendor must be documented.

All solutions **MUST** integrate with ITS' standard identity providers (IDP). Please refer to Table 1 for protocol details.

Table 1: IDP Integration Details

IDP	USER BASE	INTEGRATION PROTOCOL
NY.GOV (EXTERNAL)	GENERAL PUBLIC, BUSINESS USES, CROSS-GOVERNMENT USER (FEDERAL EMPLOYEES, COUNTY WORKERS)	OPEN IDENTITY CONNECT (OIDC) USING THE AUTHORIZATION FLOW OR SECURITY ASSERTION MARKUP LANGUAGE (SAML) 2.0
SVC (INTERNAL)	STATE EMPLOYEES	OPEN IDENTITY CONNECT (OIDC) USING THE AUTHORIZATION FLOW OR SECURITY ASSERTION MARKUP LANGUAGE (SAML) 2.0

If a security vulnerability is found with any integration with an ITS system, the vendor must patch the integration in accordance with ITS Patch Management Standard NYS-S15-001.

All systems must adhere to ITS-S16-004 Web Browsers – Development and Software Support, which states that systems must support all web browsers that are used by more 2% of the existing user base. As of publication of this solicitation, the existing user base uses: Chrome v110+; Firefox v115+; EDGE v109+.

All software solutions deployed in the NYS Private Cloud (aka on premises) are required to use the following enterprise standards¹. Necessity of these requirements is determined by the agency's assigned ITS Enterprise Architect. The ITS build or platform teams will prepare the environment prior to deployment:

- Enterprise File storage
- Code Repository (GIT)
- Enterprise Continuous Integration and Deployment (CI/CD)
 - Implemented through Jenkins or Azure DevOps

¹ Unless explicitly stated, all enterprise standards are integrated using open protocols.

- Enterprise System Monitoring
- Enterprise Networking and Edge Security
- Enterprise Compute Platforms
 - Supported platforms include Red Hat Enterprise Linux, Windows Sever, IBM AIX, IBM z/Series
- Enterprise Application Programing Interface (API) Gateway
- Enterprise Managed File Transfer (MFT)
- Enterprise Content Management (ECM)
- Enterprise Database as a Service (DBaaS)
 - Supported platforms include Oracle and Microsoft SQL Server
- Enterprise Extract, Transform and Load (ETL)
 - Oracle Data Integrator, Microsoft SQL Server Integration Services

ITS will host and support the above listed platforms. Any software, code or configurations not provided by ITS **MUST** be fully supported by the Vendor.

Deviations to these requirements **MUST** be directed to the agencies assigned ITS Enterprise Architect.

As part of the Technical Proposal, each Proposer must be compliant with NYS' technology requirements. The system must incorporate compliance with NYS ITS Technical Policies and Standards posted to <https://its.ny.gov/policies> as follows:

1. ITS-P19-002 Cloud Computing
2. ITS-P20-001 System Integration
3. ITS-S16-003 TLS / SSL Certificate Standard
4. NYS-S14-011 Enterprise Mobile Management
5. NYS-S14-009 Mobile Device Security
6. NYS-P10-001 Advertisements, Endorsements and Sponsorships on State Entity Websites
7. NYS-S14-008 Secure Configuration
8. NYS-P16-004 Web Browsers – Development and Software Support
9. NYS-S15-001 Patch Management
10. NYS-P20-001 Digital Identity Standard - NYS Authentication All software must integrate with ITS' standard identity providers (IDP) as detailed in *Table 2: IDP Integration Details* above.

as well as NYS ITS Technical Standard attached as Attachment XX:

11. ITS-S20-001 Service Oriented Architecture

IT2 – Proposer Detailed Response as how your solution meets this requirement and/or what is your plan, including timeline, for your solution to come into compliance with this requirement:

3. NEW YORK STATE SECURITY REQUIREMENTS

Rqmt. No.	Requirement Description – NEW YORK STATE SECURITY REQUIREMENTS
IT3	<p>As part of the Technical Proposal, each Proposer must be compliant with NYS’ data and security requirements.</p> <p>In its performance of the project, the selected Consultant shall be responsible for complying with New York State Chief Information Security Office (CISO) policies. In addition, the work of the selected Consultant must be compliant with the following:</p> <ol style="list-style-type: none"> 1. The NYS Information Security Policies and Standards at https://its.ny.gov/policies. Click on Security in the left-hand column to access NYS Security Policies and Standards 2. NYS Information Security Breach and Notification Act: Breach Notification and Incident Reporting Office of Information Technology Services (ny.gov) 3. In addition, the selected Consultant must be compliant with any other applicable NYS ITS Policies located here: Policies Office of Information Technology Services (ny.gov)
IT3 – Proposer Detailed Response as how your solution meets these requirements and/or what is your plan, including timeline, for your solution to come into compliance with stated requirements:	

4. NEW YORK STATE DATA SECURITY REQUIREMENTS

Rqmt. No.	Requirement Description – NEW YORK STATE DATA SECURITY REQUIREMENTS
IT4	The system must incorporate safeguards to ensure the data is protected.

	<ol style="list-style-type: none"> 1. The solution must conform to all applicable NYS Office of ITS Security Standards and Policies (accessible at https://its.ny.gov/policies). 2. The system shall generate alerts when security controls are violated. 3. The system must scan all files for viruses when uploading before accepting them into the data repository. 4. When a virus is detected, the system shall quarantine external file transfers and notify appropriate users. 5. The system must enable data encryption, at the data field level, according to the Federal Information Processing Standard (FIPS) Publication 140-2. 6. The system shall not permit audit records to be physically deleted or altered, except as part of a system administration archival process. 7. The system shall restrict saving any sensitive information in any external files, including configuration, log, and data files. 8. PPSI¹ information must be secured from unintentional disclosure. 9. Any stored documents that are generated and/or uploaded to the solution must be secured from unauthorized access. <p>¹: The term ‘PPSI’ means: Personal, Private, or Sensitive Information, and includes the following:</p> <ol style="list-style-type: none"> 1. Information used to authenticate the identity of a person or process (e.g., PIN, password, passphrase, biometric data). This does not include distribution of one-time-use PINs, passwords, or passphrases. 2. Information that identifies specific structural, operational, or technical information, such as maps, mechanical or architectural drawings, floor plans, operational plans or procedures, or other detailed information relating to electric, natural gas, steam, water supplies, nuclear or telecommunications systems or infrastructure, including associated facilities, including, but not limited to: <ol style="list-style-type: none"> a. Training and security procedures at sensitive facilities and locations as determined by the Office of Homeland Security (OHS); b. Descriptions of technical processes and technical architecture. c. Plans for disaster recovery and business continuity; and d. Reports, logs, surveys, or audits that contain sensitive information.
<p>IT4 – Proposer Detailed Response as how your solution meets this requirement and/or what is your plan, including timeline, for your solution to come into compliance with this requirement:</p>	

5. System Continuity and Error Management

Rqmt.	Requirement Description –System Continuity and Error Management
No.	
IT5	

	<p>The Proposer must include a description of the Proposer’s System Continuity and Error Management plan that meets, at a minimum, the following requirements:</p> <ul style="list-style-type: none"> • The system shall be able to automatically back out incomplete processed transactions if the system fails. • The system shall handle database failovers in a clustered database server configuration. • The system shall have fully documented restart capabilities for the application’s on-line and batch processing components. • The system must be capable of functioning in a load-balanced and redundant configuration. End user session persistence, in the event of web/app server failover, would be desired.
<p>IT5 – Proposer Detailed Response as how your solution meets this requirement and/or what is your plan, including timeline, for your solution to come into compliance with this requirement:</p>	

6. Web Content Accessibility Guidelines (WCAG) and Mobile Friendly

Rqmt. No.	Requirement Description – Web Content Accessibility Guidelines (WCAG) and Mobile Friendly
IT6	<p>As part of the Technical Proposal, each Proposer must be compliant with NYS’ Web Content Accessibility Guidelines (WCAG) and Mobile Friendly requirements.</p> <p>In its performance of the project, the selected Consultant shall be responsible for complying with New York State Legislation as follows:</p> <p>A266a/S3114a - WCAG Bill - This bill requires newly created State agency websites (including web applications), or those with changes to "form or function"¹ to comply with Level AA of the most current version of WCAG.</p> <p>A6972/S5410 - Mobile Friendly Bill – This bill requires newly created State agency websites (including web applications), or those with changes to "form or function" to be "mobile friendly"².</p> <p>¹“Changes to form or function” is defined as “modifications to the visual presentation, informational organization, website infrastructure, or user utility</p>

	<p>of the website, including but not limited to: 1. redesigns of the site layout, color schemes, graphics, branding elements, or other aesthetic components; and 2. integration of dynamic interfaces.”</p> <p>²"Mobile friendly" is defined as configuring a website "...in such a way that such website may be navigated, viewed and accessed on a smartphone, tablet computer, or similar mobile device.“</p> <p>The selected Consultant shall be responsible for complying with the following NYS WDAG and Mobile Friendly policies posted to https://its.ny.gov/policies as follows:</p> <p style="padding-left: 40px;">NYS-S16-001 New York State Universal Web Navigation NYS-P08-005 Accessibility of Information Communication Technology NYS-P08-003 Domain Names for State Government Agencies</p>
<p>IT6 – Proposer Detailed Response as how your solution meets this requirement and/or what is your plan, including timeline, for your solution to come into compliance with this requirement:</p>	