

THE PORT AUTHORITY OF NY & NJ

PROCUREMENT DEPARTMENT

ATTN: BID/PROPOSAL CUSTODIAN

4 WORLD TRADE CENTER

150 GREENWICH STREET, 21ST FLOOR

NEW YORK, NY 10007

REQUEST FOR PROPOSALS

Issue Date: February 23, 2016

**TITLE: ACQUISITION AND DEPLOYMENT OF AGENCY-WIDE
TRANSPORTATION MANAGEMENT SOFTWARE**

**SUBMIT PROPOSALS NO LATER THAN THE DUE DATE AND TIME TO THE
ABOVE ADDRESS**

RFP NO.: 45199

QUESTIONS DUE BY: March 9, 2016

TIME: 3:00 P.M.

PROPOSAL DUE DATE: March 22, 2016 TIME: 2:00 P.M.

CONTACT: Jeanette Anderson CONTACT: Arnaz Ali

PHONE: (212) 435-4624 (212) 435-4627

FAX: (212) 435-4695

EMAIL: jeanette.anderson@panynj.gov and aali@panynj.gov

Table of Contents

TABLE OF CONTENTS	2
1. INFORMATION FOR PROPOSERS ON THIS REQUEST FOR PROPOSALS	3
2. SCOPE OF WORK.....	8
3. PROPOSER PRE-REQUISITES.....	8
4. FINANCIAL INFORMATION.....	11
5. EVALUATION CRITERIA AND RANKING	11
6. MBE/WBE SUBCONTRACTING PROVISIONS.....	13
7. CERTIFICATION OF RECYCLED MATERIALS PROVISION.....	17
8. PROPOSAL SUBMISSION REQUIREMENTS.....	18
9. CONDITIONS FOR THE SUBMISSION OF A PROPOSAL.....	26
10. ATTACHMENTS.....	30
ATTACHMENT A - AGREEMENT ON TERMS OF DISCUSSION	31
ATTACHMENT B - PRE-REQUISITES, REQUIREMENTS.....	32
ATTACHMENT C - GENERAL CONTRACT PROVISIONS.....	36
ATTACHMENT D - CONTRACT SPECIFIC TERMS AND CONDITIONS.....	76
ATTACHMENT E - SCOPE OF WORK.....	81
APPENDIX 1 - REQUIREMENTS.....	132
APPENDIX 2 - USER NEEDS (TMDD STANDARD V3.03C)	161
APPENDIX 3 - CONCEPT OF OPERATIONS AND INVENTORIES.....	162
ATTACHMENT F - COST PROPOSAL.....	200
ATTACHMENT G - CERTIFICATE OF NO CHANGE.....	215
ATTACHMENT H - PROPOSER REFERENCE FORM.....	216
ATTACHMENT I - MBE/WBE PARTICIPATION PLAN.....	217
ATTACHMENT J - STATEMENT OF SUBCONTRACTOR PAYMENTS.....	222
ATTACHMENT K - CERTIFIED ENVIRONMENTALLY PREFERABLE PRODUCTS/PRACTICES..	224
ATTACHMENT L - PORT AUTHORITY FACILITIES.....	226
ATTACHMENT M - AUDIT SECURITY CHECKLISTS.....	228
ATTACHMENT N - STANDARDS AND GUIDELINES FOR PORT AUTHORITY TECHNOLOGY	239
ATTACHMENT O - INTELLIGENT TRANSPORTATION SYSTEMS DESIGN GUIDELINES	281

1. INFORMATION FOR PROPOSERS ON THIS REQUEST FOR PROPOSALS

General Information: The Port Authority of New York and New Jersey

The Port Authority of New York and New Jersey (the “Port Authority,” the “Authority,” or the “Agency”) is an agency of the States of New York and New Jersey, created and existing by virtue of the Compact of April 30, 1921, made by and between the two States, and thereafter consented to by the Congress of the United States. It is charged with providing transportation, terminal and other facilities of trade and commerce within the Port District. The Port District comprises an area of about 1,500 square miles in both States, centering about New York Harbor. The Port District includes the Cities of New York and Yonkers in New York State, and the cities of Newark, Jersey City, Bayonne, Hoboken and Elizabeth in the State of New Jersey, and over 200 other municipalities, including all or part of 17 counties, in the two States. The Port Authority manages and/or operates all of the region’s major commercial airports (Newark Liberty International, John F. Kennedy International, Teterboro, LaGuardia and Stewart International Airports), marine terminals in both New Jersey and New York (Port Newark-Elizabeth Port Authority Marine Terminal, Howland Hook and Brooklyn Piers); and its interstate tunnels and bridges (the Lincoln and Holland Tunnels; the George Washington, Bayonne, and Goethals Bridges; and the Outerbridge Crossing), which are vital “Gateways to the Nation.”

In addition, the Port Authority operates the Port Authority Bus Terminal in Manhattan, the largest facility of its kind in the world, and the George Washington Bridge and Journal Square Transportation Center bus stations. A key link in interstate commuter travel, the Port Authority also operates the Port Authority Trans-Hudson Corporation (PATH), a rapid rail transit system linking Newark, and the Jersey City and Hoboken waterfronts, with midtown and downtown Manhattan. A number of other key properties are managed by the Agency including but not limited to a large satellite communications facility (the Teleport) in Staten Island, and a resource recovery co-generation plant in Newark. Prior to September 11, 2001, the Port Authority’s headquarters were located in the World Trade Center, and that complex is still owned and being partially redeveloped by the Authority.

The Port Authority is hereby seeking proposals from firms to provide Advanced Transportation Management System (ATMS) software, system interface development and support services as described herein for the Port Authority’s Agency-wide Transportation Management Software (TMS) Acquisition and Deployment.

1. Brief Summary of Scope of Work

Background

The primary purpose of this project is to acquire and deploy an ATMS software package that will be the Port Authority’s Agency-wide Core Software solution. It is anticipated that separate ATMS instances will be installed at each facility and at central locations.

The facilities have either Communications Desks (CommDesk) or Operations Control Centers (OCC) that include the traffic management function. The central OCC function will be part of the concurrent development of the Port Authority Agency Operations Center (PA-AOC). Each local instance shall be used to monitor and control Intelligent Transportation System (ITS) assets located at the facility at which

2/8/16

the instance is installed. The Network Operations Center (NOC) shall collect, store, and archive all pertinent data for all facilities. The PA-AOC instance shall have the capability to monitor and control all ITS assets at all facilities. The PA-AOC shall also provide Port Authority-wide situational awareness by collecting and distributing data regarding transportation system conditions and incidents at Port Authority facilities.

A lightweight version of the software solution shall be deployed at Port Authority facilities that do not control ITS assets to provide them with situational awareness and the capability to provide information regarding conditions at or near them. Software deployment requirements are fully described in Attachment E.

To accomplish its objectives, the Port Authority is seeking to utilize a third party firm(s) specializing in the development, implementation, maintenance, support, and System Interface development for ATMS software.

The Port Authority will provide the following:

- Participation in Testing Cycles
- Strategic Direction Setting
- Business Continuity Planning and Management
- Disaster Recovery Planning and Management
- Business Processes
- Contract Management
- Acquisition of all Computer Hardware, Operating Systems, and Database Software

By utilizing best practices and methodologies, the Contractor's services shall consist of installing, configuring, supporting, and maintaining the Contractor's ATMS solution at the Port Authority facilities identified herein and in Attachment E. Services to be provided shall include, but not be limited to the following (full details can be found elsewhere within this document):

- System Interface development, as required
- Integrity, Availability and Performance of the Production Application
- Confidentiality of the Production Application and the Port Authority Information
- Synchronization of Production, Development, Quality Assurance, Training and Staging Environments
- Version Control Management
- Change Management Procedures
- Functionality Recommendations and Improvements
- Implementations, including Testing and Documentation, as Necessary
- Troubleshooting and Problem Management and Resolution
- Application Capacity Management and Performance Monitoring
- Disaster Recovery Support
- Business Continuity Support
- Cost Containment and/or Reduction Recommendations and Adherence
- Account Relationship Management

2/8/16

- Metrics and Reporting
- Database Administration
- Field Acceptance Testing

The Port Authority expects that the Contractor's environment, in which it will supply, install and maintain the proposed agency-wide system, will conform to the Control Requirements attached hereto in Attachment M.

The Contract will be for a four (4) -year Base Term. The Authority will have at its sole option the right to extend the Base Term for two one-year Option Periods. In addition, the Authority will have the sole right to extend the Base Term or Option Periods for an additional 120-day period at the end of any period.

2. Deadline for Receipt of Proposals

The due date specified on the cover page is the Proposal Due Date. Closing of due date is 2:00 P.M., Eastern Standard Time.

PLEASE READ THE FOLLOWING DELIVERY REQUIREMENTS CAREFULLY. Proposers assume all responsibility for delays or problems in delivery.

Proposal submissions will be received at:

The Port Authority of NY & NJ
Attention: Proposal Custodian
Procurement Department
4 World Trade Center
150 Greenwich Street, 21st Floor
New York, NY 10007

Clearly mark the solicitation number on the outermost package.

At this address, proposals will be accepted via (1) regular mail, (2) express delivery service (e.g. UPS), or (3) hand delivery.

Express carrier deliveries by commercial vehicles can be made via vendors approved by Silverstein Properties, the 4 World Trade Center (4 WTC) Property Manager, through the Vehicle Security Center (VSC). Presently, UPS is the only delivery vendor with approved recurring delivery times.

There is extensive security at the World Trade Center Site. Individuals must present a valid government-issued photo ID to enter 4 WTC. Individuals without valid identification shall be turned away and their packages not accepted. Individuals without packages or carrying small packages or boxes that can be conveyed by hand or on a hand truck may enter through the lobby. All envelopes, packages and boxes may be subject to additional security screening.

There is no parking available at 4 WTC/150 Greenwich Street, and parking in the surrounding area is extremely limited.

2/8/16

The Port Authority assumes no responsibility for delays caused by any delivery service.

3. Vendor Profile

To ensure maximum opportunities, it is vitally important that Proposers keep their vendor profiles up to date with an appropriate e-mail address, as this will enable their firm to receive timely notice of advertisements, reminders, solicitations and addenda. Proposers may update their vendor profile or register as a Port Authority Vendor by accessing the online registration system at <https://paprocure.com/VenLogon.asp>.

4. Submission of Proposals

One reproducible original (containing original signatures and clearly designated as such) and fourteen (14) double-sided copies of the proposal must be submitted on or before the due date and time in accordance with the information on the cover page of this RFP and sent or delivered to the RFP Custodian at the address specified on the cover page. Each copy of the proposal as well as the parcel(s) used for shipping must be conspicuously marked with the Proposer's name and address as well as the Proposer's Vendor Number, if available. In addition, the outside of the package must clearly state the title of this RFP, the number of this RFP and the Proposal Due Date. Failure to properly label proposal submissions may cause a delay in identification, misdirection or disqualification of proposal submissions.

Express carrier deliveries by commercial vehicles can be made via vendors approved by Silverstein Properties, the 4 World Trade Center (4 WTC) Property Manager, through the Vehicle Security Center (VSC). Presently, UPS is the only delivery vendor with approved recurring delivery times.

There is extensive security at the World Trade Center Site. Individuals must present a valid government-issued photo ID to enter 4 WTC. Individuals without valid identification shall be turned away and their packages not accepted. Individuals without packages or carrying small packages or boxes that can be conveyed by hand or on a hand truck may enter through the lobby. All envelopes, packages and boxes may be subject to additional security screening.

There is no parking available at 4 WTC/150 Greenwich Street, and parking in the surrounding area is extremely limited.

The Port Authority assumes no responsibility for delays caused by any delivery service.

Consistent with environmentally preferable procurement practices, the Port Authority requests all documents submitted to be in a form that can be easily recycled (i.e., no plastic covers or binding) and to provide only supporting literature which directly relates to the proposal being submitted.

5. Communications Regarding this RFP

All communications concerning this RFP should be directed to the Procurement Contract Manager listed on the cover page. All questions regarding this RFP must be submitted to the Procurement Contracts Manager at the email address listed on the cover page no later than 3:00 P.M. (EST) on the date shown on the cover page. Note: Send questions to: jeanette.anderson@panynj.gov and aali@panynj.gov

Questions should be submitted in an MS Word attachment to the email, and in the following format:

RFP Section	RFP Page	Topic	Question
-------------	----------	-------	----------

The Procurement Contracts Manager is authorized only to direct the attention of prospective Proposers to various portions of this RFP so that they may read and interpret such portions themselves.

Neither the Procurement Contracts Manager nor any other employee of the Port Authority is authorized to interpret the provisions of this RFP or give additional information as to its requirements. If interpretation or other information is required, it will be communicated to Proposers by written addenda and such writing shall form a part of this RFP.

6. Proposal Acceptance or Rejection

Acceptance shall be only by mailing to or delivering at the office designated by the Proposer in its proposal, a notice in writing signed by an authorized representative on behalf of the Port Authority specifically stating that the proposal is accepted or by execution of an agreement covering the subject matter of this RFP signed by authorized representatives of the Port Authority and the Proposer. No other act of the Port Authority, its Commissioners, officers, agents, representatives, or employees shall constitute acceptance of a proposal. Rejection of a proposal shall be only by either (a) a notice in writing specifically stating that the proposal is not accepted, signed by an authorized representative of the Port Authority and mailed to or delivered to the Proposer at the office designated in the Proposal, or (b) omission of the Port Authority to accept the proposal within 180 days after the Proposal Due Date. No other act of the Port Authority, its Commissioners, officers, agents, representatives or employees shall constitute rejection of a proposal.

7. Union Jurisdiction

Proposers are advised to ascertain whether any union now represented or not represented at the facility will claim jurisdiction over any aspect of the operations to be performed hereunder and their attention is directed to the Section of this RFP entitled “Harmony” included in the “General Contract Provisions, Attachment C” hereunder.

8. City Payroll Tax

Proposers should be aware of the payroll tax imposed by the:

- a. City of Newark, New Jersey for services performed in Newark, New Jersey;
- b. City of New York, New York for services performed in New York, New York; and
- c. City of Yonkers, New York for services performed in Yonkers, New York.

These taxes, if applicable, are the sole responsibility of the Contractor. Proposers should consult their tax advisors as to the effect, if any, of these taxes. The Port Authority provides this notice for informational purposes only and is not responsible for either the imposition or administration of such taxes. The Port Authority exemption set forth in the Paragraph entitled “Tax Exemption” in the “General Contract Provisions” (Attachment C) included herein, does not apply to these taxes.

9. Additional Proposer Information:

Prospective Proposers are advised that additional vendor information, including but not limited to forms, documents and other information, including MBE/WBE Participation Plan Submission Forms and protest procedures, may be found on the Port Authority website at:

<http://www.panynj.gov/business-opportunities/become-vendor.html>

10. Contractor Staff Background Screening

The Contractor awarded this contract will be required to have its staff, and any subcontractor's staff working under this Contract, authorize the Authority or its designee to perform background checks. Such authorization shall be in a form acceptable to the Authority. The Contractor (and subcontractor) may also be required to use an organization designated by the Authority to perform the background checks. The cost for said background checks for staff that pass and are granted a credential shall be reimbursable to the Contractor (and its subcontractors) as an out-of-pocket expense as provided herein. Staff that are rejected for a credential for any reason are not reimbursable.

As of January 29, 2007, the Secure Worker Access Consortium (S.W.A.C.) is the only Port Authority approved provider to be used to conduct background screening, except as otherwise required by federal law and/or regulation. Information about S.W.A.C., instructions, corporate enrollment, online applications, and location of processing centers can be found at <http://www.secureworker.com>, or S.W.A.C. may be contacted directly at (877)522-7922.

11. Automated Clearing House Enrollment

The Port Authority of New York and New Jersey is transitioning to an all electronic method of paying its vendors and contractors via an Automated Clearing House (ACH) funds transfer. The Contractor must complete the Port Authority's "Authorization Agreement For Direct Deposits And Direct Payments (ACH Credits)" form, which is available at <http://www.panynj.gov/business-opportunities/pdf/ach-authorization-form.pdf>, in order to receive payment. To avoid delays in payments for commodities and services provided, vendors and contractors must be enrolled in ACH. Printed accounts payable checks will not be issued. The Authorization Agreement shall remain in full force and effect until the Port Authority has received written notification from the Contractor of its termination in such time and in such manner as to afford the Port Authority and the depository financial institution(s) a reasonable opportunity to act on it. Any questions on this initiative may be directed to the ACH Enrollments contact line at 201 216-6002 or emailed to ACHENROLLMENT@PANYNJ.GOV.

2. SCOPE OF WORK

The full Scope of Work (SOW) is set forth in detail in Attachment E.

3. PROPOSER PRE-REQUISITES

I. Either the Proposer shall have been pre-qualified to perform under Collective #37893 Prequalification of Advanced Transportation Management System (ATMS) Software Package – Stage I,

2/8/16

dated May 16, 2014. Each Proposer must submit documentation showing that its firm is prequalified. In addition, Proposers must fill out and submit the Certificate of No Change, attached hereto as Attachment G. **OR**

II. Firms that have not been prequalified but desire to submit a proposal for the referenced RFP must demonstrate that they comply with the following prerequisites. Only Proposers who can demonstrate that they comply with the following should submit proposals as only proposals from such Proposers will be considered:

Proof of meeting the prerequisites must be submitted using the forms provided as **Attachment B**, supporting documentation must be submitted in a clear and concise manner as part of the Proposer's submittal.

- A. The Proposer shall have had at least four (4) years of experience within the five (5) year period immediately prior to the date of submission of the RFP, as a business actually engaged in the development, implementation, configuration, and/or customization of ATMS software for use in Transportation Management Centers (TMC) or other similar Operation Centers where vehicular traffic is both monitored and controlled using Intelligent Transportation field metric devices for data acquisition and information dissemination. Fulfillment of this pre-requisite must be demonstrated by providing a list of projects, clients, and brief project descriptions for work performed during the above period.
- B. During the 10-year period prior to the submission of the RFP, the Proposer, or persons or entities owning or controlling the Proposer, shall have satisfactorily completed installation (successfully operational for at least 1 year) and configured their proposed ATMS solution at one or more TMC/Operations Centers (as described in paragraph A above), where a minimum total of 150 ITS assets were monitored and/or controlled. Those assets can be located at any of the facilities and the aggregate total of 150 can be distributed among one or more locations and be of the following types:
 - a. Dynamic Message Signs (DMS)
 - b. Vehicle Detection Stations (VDS)
 - c. Lane-Use Control Signals (LUCS)
 - d. Variable Speed Limit Signs (VSLS)
 - e. TRANSMIT or other Vehicle Probe Systems
 - f. CCTV Cameras
 - g. Road Weather Information System (RWIS) Stations
- C. The Proposer shall demonstrate that it has earned gross revenues of at least \$1,000,000 a year for the last three (3) fiscal years from the type of services described herein. Provide a statement on letterhead signed by your Chief Financial Officer (CFO) or a Certified Public Accountant (CPA) certifying that your company meets the gross revenues specified above.

- D. The Proposer must demonstrate that the ATMS is compliant with National Transportation Communications for ITS Protocol (NTCIP) and Traffic Management Data Dictionary (TMDD) Standards for Center-to-Center (C2C) communications protocol referenced herein and in the RFP. The Proposer must have documented experience in the development of System Interfaces (SIs) for NTCIPv2 or later protocol for, at a minimum, DMS, VDS, and CCTV cameras as well as Center-to-Center (C2C) Communications conforming to TMDD Standards. Fulfillment of this pre-requisite must be demonstrated by identifying specific implementations with accompanying contact information for a reference.
- E. The Proposer must have documented experience in the development of SIs to push incident, travel time, and other travel information to external systems such as 511NY, 511NJ, Twitter, and specially developed smartphone applications. Fulfillment of the pre-requisite must be demonstrated by identifying specific implementations with accompanying contact information for reference.

In the event a Response is submitted by a joint venture the foregoing prerequisites will be considered with respect to such Response as follows:

- With respect to subparagraphs (A), (B), (C), (D), and (E) above, the prerequisite will be considered satisfied if the joint venture itself, or any of its participants individually, can meet the requirements.
- If the Response is submitted by a common law joint venture that has not been established as a distinct legal entity, each participant of the joint venture shall be held jointly and severally liable and must individually execute and perform all acts required by this proposal. Documents signed by a common law joint venture, in connection with this proposal, shall include the names of all participants of the joint venture followed by the words “acting jointly and severally”. All joint venture proposers must provide documentation of their legal status.

In the event that the Proposer intends to utilize Subcontractors to execute a portion of the work, the foregoing prerequisites will be considered with respect to the submitted Response as follows:

- With respect to subparagraphs (A), (B), (C), (D), and (E) above, the prerequisite will be considered satisfied if either the Proposer or the Subcontractor meet the requirements.
- The Proposer is obligated to ensure that the Subcontractor completes all work as indicated in the Response and subsequent Proposal, if any.
- The Contractor shall be held liable for the actions of the Subcontractor.

4. FINANCIAL INFORMATION

The Proposer will be required to demonstrate that it is financially capable of performing the contract resulting from this RFP (“Contract”). The determination of the Proposer’s financial qualifications and ability to perform this Contract will be in the sole discretion of the Port Authority. The Proposer shall submit, with its proposal, the following:

- A. (1) Certified financial statements, including applicable notes, reflecting the Proposer’s assets, liabilities, net worth, revenues, expenses, profit or loss and cash flow for the most recent year or the Proposer’s most recent fiscal year.

(2) Where the certified financial statements in (1) above are not available, then reviewed statements from an independent accountant setting forth the aforementioned information shall be provided.

Where the statements submitted pursuant to subparagraphs (1) and (2) aforementioned do not cover a period which includes a date not more than forty-five (45) days prior to the Proposal Due Date, then the Proposer shall also submit a statement in writing, signed by an executive officer or his/her designee, that the present financial condition of the Proposer is at least as good as that shown on the statements submitted.

- B. A statement of work that the Proposer has on hand, including any work on which a bid and/or proposal has been submitted, containing a description of the work, the annual dollar value, the location by City and State, the current percentage of completion, the expected date for completion, and the name of an individual most familiar with the Proposer’s work on these jobs.
- C. The name and address of the Proposer’s banking institution, chief banking representative handling the Proposer’s account, the Proposer’s Federal Employer Identification Number (i.e., the number assigned to firms by the Federal Government for tax purposes), the Proposer’s Dun and Bradstreet number, if any, the name of any credit service to which the Proposer furnished information and the number, if any, assigned by such service to the Proposer’s account.

5. EVALUATION CRITERIA AND RANKING

All proposals will be reviewed by the Port Authority to determine if they adhere to the format required in this RFP, if they contain all required submissions, and if the Proposer meets the Proposer Prerequisite and the Proposal Submission Requirements. For proposals meeting such requirements, the following criteria set forth in order of importance, will be utilized in the evaluation of proposals.

<p>A. Technical Plan; Work Approach</p>	<ul style="list-style-type: none"> • The degree to which the features and functions of the proposed System meets the requirements and objectives stated in the RFP, including the Mandatory Requirements; the proposed installation, maintenance and training plans; the Proposer’s ability and willingness to satisfy the service levels specified in the Scope of Work (SOW).
--	--

<p>B. Financial Approach</p>	<ul style="list-style-type: none"> • The Cost Proposal, including all financial compensation expected for the required services listed in this RFP. The Proposer must provide a completed set of Pricing Sheets that are included in Attachment F. • The fully burdened Hourly Rates provided by the Contractor for Extra Work and Net Cost Work that are included in Attachment F and pursuant to Attachment D (Compensation for Extra Work). • The degree and extent to which the proposal is cost-effective to the Port Authority. • The Proposer’s clear description of the methods, practices, tools and techniques that will result in cost containment, and the likelihood of those methods, practices, tools and techniques being successfully deployed.
<p>C. Management Approach and Firm Strength and Management Team Experience</p>	<ul style="list-style-type: none"> • The quality of management, the level of staff experience and knowledge of the technologies, and configuration needed to support the Port Authority’s Agency-wide Transportation Management Software solution. • The demonstrated ability to manage the functional and technical components of the Proposer’s ATMS software solution in an environment comparable to the Port Authority’s. This criterion will also take into account the Proposer’s size, financial stability, industry track record, and capability to provide the managerial, technical and physical resources to deliver the required services over an extended time period. • The Proposer’s ability, through relationships with ITS hardware vendors and experience with other clients, to provide strategic advisory services, introduce alternative solutions, and provide insight into the value and applicability of upgrades and new functionality to the Port Authority’s Core Software. • The Proposer’s MBE/WBE plan, background screen plan, Certification of Environmentally Preferable Products/Practices, On-site management plans and work plan for this Contract, and business risk, will also be evaluated.

Background Check Plan

The Proposer must submit a Background Check plan, which will be considered “pass/fail.” If the Port Authority determines that the Plan is deficient, the Proposer’s response may be removed from further consideration.

Business Risk

Consideration will be given to the degree of business risk assumed by the Port Authority. This will include, but not be limited to, assessment of the impact resulting from the possible failure of the Contractor to perform under the terms and conditions of this Contract. As part of the evaluation, business risk will also be measured by the Port Authority’s assessment of its ability to immediately replace the Contractor in a manner that maintains or improves the quality and continuity of facility.

6. MBE/WBE SUBCONTRACTING PROVISIONS

The Port Authority has a long-standing practice of making its business opportunities available to Minority Business Enterprises (MBEs) and Woman-owned Businesses (WBEs) and has taken affirmative steps to encourage such firms to seek business opportunities with the Port Authority. The successful Proposer will use good faith efforts to provide for meaningful participation by the Port Authority Port Authority certified MBE/WBEs as defined in this document, in the purchasing and subcontracting opportunities associated with this contract, including purchase of equipment, supplies and labor services.

MBE/WBE Good Faith Participation – The Contractor shall use every good-faith effort to provide for participation by Port Authority certified Minority Business Enterprises (MBEs) and Port Authority certified Woman-owned Business Enterprises (WBEs) in all purchasing and subcontracting opportunities associated with this Contract, including purchase of equipment, supplies and labor services, in accordance with the section of the Standard Terms and Conditions entitled “MBE/WBE Good Faith Participation.”

The Contractor shall use good faith efforts to achieve participation equivalent to twelve percent (12%) of the total Contract price for MBEs and five percent (5%) of the total Contract price for WBEs.

Good faith efforts to include participation by MBE/WBEs shall include, but not be limited to the following:

- a. Dividing the services and materials to be procured into small portions, where feasible.
- b. Giving reasonable advance notice of specific contracting, subcontracting and purchasing opportunities to such MBE/WBEs as may be appropriate.
- c. Soliciting services and materials from a Port Authority Port Authority certified MBE/WBE or seeking MBE/WBEs from other sources. To access the Port Authority’s Directory of MBE/WBE Port Authority certified Firms go to www.panynj.gov/supplierdiversty
- d. Ensuring that provision is made to provide progress payments to MBE/WBEs on a timely basis.
- e. Observance of reasonable commercial standards of fair dealing in the respective trade or business.

Proposers are directed to use form PA3749 as the recording mechanism for the MBE/WBE participation plan, annexed hereto as Attachment G or may be downloaded at <http://www.panynj.gov/business-opportunities/become-vendor.html>.

Proposers shall include their MBE/WBE Participation Plan with their Proposals, to be reviewed and approved by the Authority’s Office of Business Diversity and Civil Rights (OBDCR).

The MBE/WBE Plan submitted by the Contractor to the Port Authority shall contain, at a minimum, the following:

- Identification of MBE/WBEs: Provide the names and addresses of all MBE/WBEs included in the Plan. If none are identified, describe the process for selecting participant firms in order to achieve the good faith goals under this Contract.

2/8/16

- Level of Participation: Indicate the percentage of MBE/WBE participation expected to be achieved with the arrangement described in the Plan.
- Scope of Work: Describe the specific scope of work the MBE/WBEs will perform.

All MBE/WBE subcontractors listed on the MBE/WBE Participation Plan must be certified by the Port Authority in order for the Contractor to receive credit toward the MBE/WBE goals set forth in this Contract. Please go to <http://www.panynj.gov/business-opportunities/supplier-diversity.html> to search for MBE/WBEs by a particular commodity or service. The Port Authority makes no representation as to the financial responsibility of these firms or their ability to perform work under this Contract.

Subsequent to Contract award, all changes to the MBE/WBE Participation Plan must be submitted via a modified MBE/WBE Participation Plan to the Manager for review and approval by the Authority's Office of Business Diversity and Civil Rights. For submittal of modifications to the MBE/WBE Plan, Contractors are directed to use form PA3749A, which may be downloaded at <http://www.panynj.gov/business-opportunities/become-vendor.html>. The Contractor shall not make changes to its approved MBE/WBE Participation Plan or substitute MBE/WBE subcontractors or suppliers for those named in their approved plan without the Manager's prior written approval. Unauthorized changes or substitutions, including performing the work designated for a subcontractor with the Contractor's own forces, shall be a violation of this section. Progress toward attainment of MBE/WBE participation goals set forth herein will be monitored throughout the duration of this Contract.

The Contractor shall also submit to the Manager, along with invoices, the Statement of Subcontractor Payments in the form of the MBE/WBE Participation Report, which may be downloaded at <http://www.panynj.gov/business-opportunities/become-vendor.html>. The Statement must include the name and business address of each MBE/WBE subcontractor and supplier actually involved in the Contract, a description of the work performed and/or product or service supplied by each such subcontractor or supplier, the date and amount of each expenditure, and such other information that may assist the Manager in determining the Contractor's compliance with the foregoing provisions.

Prompt Payment/Retainage

The Contractor agrees to pay each subcontractor under this Contract, for satisfactory performance of its subcontract, no later than ten (10) days from the receipt of each payment the Contractor receives from the Authority. The prime contractor agrees further to return retainage payments, if any to each subcontractor within ten (10) days after the subcontractors' work is satisfactorily completed. Any delay or postponement of payment from the above referenced timeframe may occur only for good cause following written approval of the Authority.

MBE/WBE Conditions of Participation

MBE/WBE participation will be counted toward meeting the MBE/WBE contract goal, subject to all of the following conditions:

A. **Commercially Useful Function.** An MBE/WBE is considered to perform a commercially useful function when it is responsible for the execution of a distinct element of work on a contract and carries out its responsibilities by actually performing, managing, and supervising the work involved in accordance with normal industry practice. Regardless of whether an arrangement between the Contractor and the MBE/WBE represent standard industry practice, if the arrangement erodes the ownership, control or independence of the MBE/WBE or in any other way does not meet the commercially useful function requirement, that firm shall not be included in determining whether the MBE/WBE goal is met and shall not be included in MBE/WBE reports. If this occurs with respect to a firm identified as a MBE/WBE, the Contractor shall receive no credit toward the MBE/WBE goal and may be required to backfill the participation. An MBE/WBE does not perform a commercially useful function if its role is limited to that of an extra participant in a transaction or contract through which funds are passed in order to obtain the appearance of MBE/WBE participation. An MBE/WBE may rebut a determination by the Authority that the MBE/WBE is not performing a commercially useful function to the Authority.

B. **Work Force.** The MBE/WBE must employ a work force (including administrative and clerical staff) separate and apart from that employed by the Contractor, other Subcontractors on the contract, or their Affiliates. This does not preclude the employment by the MBE/WBE of an individual that has been previously employed by another firm involved in the Contract, provided that the individual was independently recruited by the MBE/WBE in accordance with customary industry practice. The routine transfer of work crews from another employer to the MBE/WBE shall not be allowed.

C. **Supervision.** All Work performed by the MBE/WBE must be controlled and supervised by the MBE/WBE without duplication of supervisory personnel from the Contractor, other Subcontractors on the contract, or their Affiliates. This does not preclude routine communication between the supervisory personnel of the MBE/WBE and other supervisors necessary to coordinate the Work.

Counting MBE/WBE Participation

The value of the Work performed by an MBE/WBE, with its own equipment, with its own forces, and under its own supervision will be counted toward the goal, provided the utilization is a commercially useful function. An MBE/WBE prime contractor shall still provide opportunities for participation by other MBE/WBEs. Work performed by MBE/WBEs will be counted as set forth below. If the Authority determines that some or all of the MBE/WBEs work does not constitute a commercially useful function, only the portion of the work considered to be a commercially useful function will be credited toward the goal.

A. **Subcontractors.** One hundred percent (100%) of the value of the Work to be performed by an MBE/WBE subcontractor will be counted toward the MBE/WBE goal. The value of such Work includes the cost of materials and supplies purchased by the MBE/WBE, except the cost of supplies or equipment leased from the Contractor, other Subcontractors or their affiliates will not be counted. When a MBE/WBE subcontracts part of the work of its contract to another firm, the value of the subcontracted work may be counted toward MBE/WBE goals only if the MBE/WBE subcontractor is itself a MBE/WBE. Work that a MBE/WBE subcontracts to a non-MBE/WBE firm does not count toward MBE/WBE goals.

2/8/16

B. Manufacturers/Fabricators. One hundred percent (100%) of the expenditure to a MBE/WBE manufacturer or fabricator will be counted towards the MBE/WBE goal.

C. Material Suppliers. Sixty percent (60%) of the expenditure to a MBE/WBE material supplier will be counted toward the MBE/WBE goal. Packagers, brokers, manufacturer's representatives, or other persons who arrange or expedite transactions are not material suppliers within the meaning of this paragraph.

D. Broker's/Manufacturer's Representatives. One hundred percent (100%) of fees or commissions charged for assistance in the procurement of the materials and supplies, or fees for transportation charges for the delivery of materials or supplies provided by an MBE/WBE broker/manufacturer's representative will be counted toward the MBE/WBE goal, provided they are determined by the Authority to be reasonable and not excessive as compared with fees customarily allowed for similar services. The cost of the materials and supplies themselves will not be counted.

E. Services. One hundred percent (100%) of fees or commissions charged by an MBE/WBE for providing a bona fide service, such as professional, technical, consultant, or managerial services, or for providing bonds or insurance specifically required for the performance of the Work will be counted toward the MBE/WBE goal, provided the fee is reasonable and not excessive as compared with fees customarily allowed for similar services.

F. Trucking Operations. If using an MBE/WBE firm for trucking operations, the MBE/WBE trucking firm of record is the firm that is listed on the MBE/WBE Participation Plan. The MBE/WBE trucking firm shall own and operate at least one registered, insured, and fully operational truck used for the performance of the Work and shall be responsible for the management and supervision of the entire trucking operation for which it is responsible on a particular contract, and there cannot be a contrived arrangement for the purpose of meeting the MBE/WBE goal. The MBE/WBE trucking firm of record shall control the day-to-day MBE/WBE trucking operations for performance of the Work, and shall be responsible for (1) negotiating and executing rental/leasing agreements; (2) hiring and terminating the work force; (3) coordinating the daily trucking needs with the Contractor; and (4) scheduling and dispatching trucks.

1. MBE/WBE Owned/Leased Trucks. One hundred percent (100%) of the value of the trucking operations the MBE/WBE provides for the performance of the Work using trucks it owns or leases on a long-term basis that are registered, insured, and operated by the MBE/WBE using drivers it employs, will be counted toward the MBE/WBE goal.

2. MBE/WBE Short-Term Leased Trucks. The MBE/WBE may lease trucks on a short-term basis from another MBE/WBE, including an owner/operator who is Port Authority certified as a MBE/WBE. 100% of the value of the trucking operations that the lessee MBE/WBE provides will be counted toward the MBE/WBE goal.

3. Non-MBE/WBE Trucks. The MBE/WBE may lease trucks on a short-term basis from a non-MBE/WBE, including an owner-operator. One hundred percent (100%) of the fee or commission the MBE/WBE receives as a result of the lease arrangement will be counted toward the MBE/WBE goal. The value of the trucking operations provided by the lessee will not be counted toward the MBE/WBE goal.

G. Joint ventures between MBE/WBEs and non-MBE/WBEs may be counted toward the MBE/WBE goal in proportion to the total dollar value of the contract equal to the distinct, clearly defined portion of the work of the contract that the MBE/WBE performs with its own forces. Please contact the Office of Business Diversity and Civil Rights at (201) 395-3958 for more information about requirements for such joint ventures.

7. CERTIFICATION OF RECYCLED MATERIALS PROVISION

Proposers shall submit, with their proposals, Attachment K entitled “Certified Environmentally Preferable Products / Practices Form” attesting that the products or items offered by the Proposer contain the minimum percentage of post-consumer recovered material in accordance with the most recent guidelines issued by the United States Environmental Protection Agency (EPA), or, for commodities not so covered, the minimum percentage of post-consumer recovered materials established by other applicable regulatory agencies.

Recycling Definitions:

For purposes of this solicitation, the following definitions shall apply:

- a. “Recovered Material” shall be defined as any waste material or by-product that has been recovered or diverted from solid waste, excluding those materials and by-products generated from, and commonly reused within, an original manufacturing process.
- b. “Post-consumer Material” shall be defined as any material or finished product that has served its intended use and has been discarded for disposal or recovery having completed its life as a consumer item. “Post-consumer material” is included in the broader category of “Recovered Material.”
- c. “Pre-consumer Material” shall be defined as any material or by-product generated after the manufacture of a product but before the product reaches the consumer, such as damaged or obsolete products. Pre-consumer Material does not include mill and manufacturing trim, scrap, or broken material that is generated at a manufacturing site and commonly reused on-site in the same or another manufacturing process.
- d. “Recycled Product” shall be defined as a product that contains the highest amount of post-consumer material practicable, or when post-consumer material is impracticable for a specific type of product, contains substantial amounts of Pre-consumer Material.
- e. “Recyclable Product” shall be defined as the ability of a product and its packaging to be reused, reconditioned for use, or recycled through existing recycling collection programs.

- f. "Waste Reducing Product" shall be defined as any product that will result in less waste generated due to its use rather than another product designed to serve the same function with a greater waste generation rate. This shall include, but not be limited to, those products that can be reused, refilled or have a longer life expectancy and contain a lesser amount of toxic constituents.

8. PROPOSAL SUBMISSION REQUIREMENTS

In order to expedite the evaluation of proposals, the Proposer's response to this RFP shall follow the format and order of items, using the same paragraph identifiers, as set forth below.

A. Letter of Transmittal

The Proposer shall submit a letter on its letterhead, signed by an authorized representative, stating its experience and qualifications in meeting the requirements of this RFP. This letter shall include a statement on whether the Proposer is submitting a proposal as a single entity, a joint venture, or is partnering with another firm in a prime/subcontracting relationship. In all cases, information required for a single entity is required for each participant in a joint venture.

PROPOSALS WILL BE DUE TO THE NEW PORT AUTHORITY PROCUREMENT DEPARTMENT LOCATION AT 4 WORLD TRADE CENTER LOCATED AT 150 GREENWICH STREET, 21ST FLOOR, NEW YORK, NEW YORK, 10007.

It is necessary to carry valid government-issued photo identification when attempting to gain access into the building to hand deliver proposals. Proposers delivering proposals should anticipate extensive delays. All packages entering the property are subject to additional layers of security screening. There is no parking available at 4 WTC/150 Greenwich Street and parking in the surrounding area is extremely limited.

The Letter of Transmittal shall contain:

- (1) Name and address of the Proposer and an original signature on the Letter of Transmittal by an authorized representative on behalf of the Proposer;
- (2) Name(s), title(s) and telephone number(s) of the individual(s) who are authorized to negotiate and execute the Contract;
- (3) Name, title and telephone number of a contact person to which the Port Authority can address questions or issues related to this RFP;
- (4) Name and address of proposed subcontractors, if any;
- (5) If a corporation: (a) a statement of the names and residences of its officers, and (b) a copy of its Certificate of Incorporation, with a written declaration signed by the secretary of the corporation, with the corporate seal affixed thereto, that the copy furnished is a true copy of the Certificate of Incorporation as of the date of the opening of the Proposals;

If a partnership: a statement of the names and residences of its principal officers, indicating which are general and which are special partners;

2/8/16

If an individual: a statement of residence;

If a joint venture: information on each of the parties consistent with the information requested above; if the Contract is awarded to a common law joint venture (a partnership of business entities) each member will be jointly and severally liable under the Contract.

B. Executive Summary

The Proposer shall submit an Executive Summary presenting the major features of its proposal and how the proposal satisfies the requirements contained in this RFP, as well as the special competencies and expertise of the Proposer to meet the requirements of this RFP.

C. Agreement on Terms of Discussion

The Proposer shall submit a copy of the "Agreement on Terms of Discussion," signed by an authorized representative of the Proposer. The Agreement format is included as Attachment A and shall be submitted by the Proposer without any alterations or deviations. Any Proposer who fails to sign the Port Authority's "Agreement on Terms of Discussion" will not have its proposal reviewed. If the Proposer is a joint venture, an authorized representative of each party must sign the Agreement.

D. Certifications With Respect to the Contractor's Integrity Provisions

The Proposer, by signing the Letter of Transmittal, makes the certifications in the "Contractor's Integrity Provisions," included as Section 34 of Attachment C entitled "General Contract Provisions" of this RFP. If the Proposer cannot make any such certifications, it shall enclose an explanation of that inability. ("Certification Statement").

E. Proposal

The Proposer must demonstrate, to the satisfaction of the Authority, that it has sufficient resources, capabilities and experience to meet the business needs and requirements as set forth in this RFP. To do so, the Proposer must provide the following:

1) Technical Plan/Work Approach:

- a) The Proposer shall explain how its proposal exceeds the minimum requirements. The Proposer shall confirm that, in its successful delivery of ATMS software implementation and System Interface development, maintenance and support services (including hardware, operating system, database, security and system administration and maintenance), that it possesses and adheres to formal processes having produced tangible results in prior engagements including, but not limited to, the following:
 - i. Detailed case studies demonstrating how the proposed system was deployed for other entities similar in size and complexity to the Port Authority.
 - ii. Proof that the Proposer is proposing the current/latest version of its system to the Port Authority

- iii. Technology Roadmap: The Proposal shall include a technology roadmap conveying planned or anticipated changes (e.g., updates) to the proposed software in the next five years. The Roadmap shall also convey any assumptions or obligations on the customer as a result of such changes.
 - iv. Required Hardware: A list of all hardware required to support the System. The list shall describe the hardware, identify its manufacturer and the manufacturer's part numbers. The proposal should include the requirements for the production, quality assurance, development, and training environments.
 - v. Detecting and resolving defects (including 24-hour on call availability);
 - vi. Providing end-user and technical documentation;
 - vii. Providing training, including training materials, as necessary;
 - viii. Enhancing existing functionality and adding new functionality to systems;
 - ix. Developing System Interfaces that adhere to the latest industry standards;
 - x. Continuously improving their ATMS solution as evidenced by new releases with increased functionality on a regular basis;
 - xi. Developing and Executing detailed Field Acceptance Test Plans;
 - xii. Rewriting, restructuring, problem/system/database tuning;
 - xiii. Program/system/database management;
 - xiv. Change Management and production turnover methodologies and procedures;
 - xv. Assessing the impact of changes to the operational environment, determining if changes are needed to the applications as a result, and implementing the changes as required;
 - xvi. Initiating and implementing productivity improvements;
 - xvii. Knowledge transfer to both Technology personnel and core functional users in understanding the application systems;
 - xviii. Answering users' and Computer Operations staff questions related to these application systems;
 - xix. Participating in disaster recovery tests and during a disaster;
 - xx. Providing a quality assurance review/methodology for maintenance activities and enforcing installation standards; and
 - xxi. Identifying areas where technology can be applied to achieve improved efficiencies including benchmarking against industry standards.
- b) The Proposer shall provide documentation on any and all security certifications (e.g., SSAE16, ISO 17999, ISO 27001) or comparable held. Information provided shall include certification expiration dates and plans to maintain certification.
- c) Transition Planning for seamless support – The Proposer shall provide a detailed plan including approach methodology, number and skill set of resources (both from the Proposer side as well as from the Authority) and toolsets used for transition in the following circumstances:
- i. At the commencement of the agreement (note – As stated herein, the transition period shall under no circumstances exceed three months);

- ii. During the course of the engagement with additional integrators; and,
 - iii. At the completion of the engagement – i.e., the Proposer's ability to work effectively and in harmony with a potential new provider.
- d) Documented methodology for the following functions:
- i. Performing application management, maintenance and support services (including hardware, operating system, database, security and system administration and maintenance), which has a goal of continuous improvement in its performance of application management and hardware infrastructure and systems and database administration functions;
 - ii. Transitioning new applications into the various development, testing and production environments, including change management and version control management;
 - iii. Quality control of all maintenance and enhancement activities, including turnover to production, documentation and knowledge transfer to operational support teams.
- e) Troubleshooting and Problem Resolution
- i. The Proposer shall submit a plan for providing problem resolution and escalation procedures.
- f) Experience of Proposer's senior management team in managing employees and conducting employee management programs, including, but not limited to:
- i. Staffing Plan
 - ii. Contract Management
 - iii. Proposed Installation and Maintenance Plans
 - Installation Plan: The Proposal shall include a plan and schedule, with assumptions, to install the software.
 - Maintenance Plan: The Proposal shall include a plan to maintain the software. The Plan shall address the provision of all software fixes, updates, patches and new releases, and to provide corrective and preventive maintenance.
- g) The Proposer shall include an affirmative response that the solution, its implementation and its ongoing administration will adhere to the control checklists in Attachment M.

To demonstrate the above, submit copies or detailed descriptions of each applicable methodology or approach.

Please Note: Company brochures alone should not be submitted for the purpose of demonstrating experience and technical expertise. Submittals should be tailored to the specific requirements of this RFP.

2) Financial Approach

The Proposer shall submit a Cost Proposal indicating the compensation that it expects to receive. The Cost Proposal must be complete and include payment for all services referenced

herein. The Proposer shall complete the Pricing Sheet in Attachment F and submit it as part of the Cost Proposal. The Proposer shall enter an amount for the Price for Implementation and then compute the Lump Sum Amounts for each Milestone using the percentages provided by the Authority.

The Proposer shall submit Pricing Sheets for Milestones 1 through 9. For each Milestone, the Proposer shall utilize the percentages assigned to the deliverable Tasks by the Authority for each Milestone to compute Lump Sum Amounts for each.

The Proposer shall also enter the Prices for Application Maintenance and Support for Years 3 through 6 as well as the Total Price for Application Maintenance and Support.

The Cost Proposal shall include the following:

- a) Completed Pricing Sheets (see Attachment F).
- b) A list of Key Staff categories and fully-burdened rates for each. These classifications and rates will be used for all Extra Work and Net Cost Work.

3) Management Approach and Firm Strength and Management Team Experience

- a) References: The Proposer shall submit a listing of key / representative ATMS application management, maintenance and support services (including hardware, operating system, database, security and system administration and maintenance) contracts that were performed by or are currently being performed by the Proposer within the last three (3) years (use "Attachment H – Proposer Reference Form").
- b) Proposed Team / Proposed Staffing: The Proposer shall provide a cover sheet indicating the qualifications and experience of technical, managerial and supervisory personnel employed by the firm who are to be assigned to the Contract, including the following: For each individual, indicate his/her role on the engagement, whether onsite or remote and whether full or part time. (If part time, indicate number of hours/week).
 - i. His/her length of service with the firm
 - ii. The anticipated function of each person on the Contract
 - iii. A summary of the relevant experience of each person listed. The resumes of the individuals who are being recommended for these positions shall be included in the proposal.
- c) The Proposer shall submit to the Port Authority, a detailed itemized description explaining technical expertise and past experience the proposed team has in the following areas:
 - i. ATMS software development and implementation;
 - ii. System Interface development, including system and types of data ;
 - iii. Application maintenance and support.
- d) The Proposal shall describe in detail which services will be provided off site and which will be conducted on site for each of the following:

- i. Describe the Contractor's Company's plan to manage the TMS Contract for all facilities, including the quality and effectiveness of the Contractor's M/W/SBE plan.
- ii. Include detailed project schedules as set forth in Attachment E, Scope of Work. The Proposer shall provide key milestone dates on the "milestone schedule" and describe all task interdependencies. (While not required, Proposers are encouraged to use GANNT charts and highlight critical path activities). The project schedule shall indicate when Authority-required tasks, including but not limited to providing test hardware, providing connectivity, etc., need to be performed. All schedules must be in Microsoft Project 2007 or later format.
- iii. The Proposal shall demonstrate the proposed System's ability to integrate with the applications listed in SOW (Attachment E). In addition, the Proposal shall identify the Proposer's authorized resellers that can integrate the proposed System with the listed applications.
- iv. The Proposer shall describe in detail its experience, including relevant contracts performed during the last three (3) years, its financial capability, management structure and proposed staffing, detailing technical training, certifications, applicable licenses, skills and experiences and capability of proposed staff and other supporting documentation demonstrating its ability to perform the work.
- v. The Proposer shall provide a Detailed Implementation Plan that addresses all the requirements of Attachment E, Scope of Work. The Proposer should describe the methodology it has used successfully in the past and describe how existing system integrity will not be lost. The Contractor must propose how it will guarantee the Authority's access to all data in the event of the termination or expiration of the new contract.
- vi. The Proposer shall provide detailed descriptions of its pre-employment screening procedures; safety and emergency procedures including, but not limited to, disaster recovery plans.
- vii. The Proposer shall include a detailed organizational chart identifying all key staff.
- viii. The Proposer shall provide a staffing plan that clearly outlines staffing needed to perform each function as described in the Scope of Work and submit training requirements for all technical employees. The Proposer shall describe how availability and response time requirements will be achieved. The Proposer shall describe the anticipated location of staff as well as the planned locations of the Proposer's nearest offices.
- ix. Reassignment of Key Staff shall require approval from the Port Authority. If approval is granted, the Proposer shall furnish a replacement with equal or higher qualifications for the same or lesser costs. The Authority will have the right to reject candidates proposed by the Contractor for cause.

- x. Proposers shall submit a list of the job titles, responsibilities, qualifications, and work associated with each key position for personnel to be assigned to Net Cost Work.
- xi. Describe the roles and responsibilities of the software support team members that will be assigned to this Contract.
- xii. Provide qualifications of support team members.
- xiii. Describe technical customer services experience and capabilities.
- xiv. Identify the Account Manager and Project Manager.
- xv. The Proposer shall submit an MBE/WBE Plan in accordance with the section of this RFP entitled "MBE/WBE Subcontracting Provisions." The Proposer shall be required to report on actual achievement against plan goals on a quarterly basis.
- xvi. Training Plan - The Proposal shall describe the plan to provide training according to the requirements specified in the SOW.
- xvii. Licensing Model: The Proposal shall describe the Proposer's licensing model for the requirements set forth in the SOW.
- xviii. License, Maintenance, Escrow Agreements: The Proposal shall include copies of all license, maintenance, escrow agreements for the proposed System.
- xix. The Proposer's Certified Environmentally Preferable Products/Practices Form must be completed ensuring compliance with all applicable federal, state and local standards in their business practices, in accordance with the Certified Environmentally Preferable Products/Practices Provision.
- xx. The Proposers proven transition planning approach that covers transitions at contract commencement; during the course of the agreement and upon contract termination must be furnished.
 - 1. Transition Planning for seamless support – The Proposer shall provide detailed plan including approach methodology, number and skill set of resources (both from the Proposer side as well as from the Authority) and toolsets used for transition in the following circumstances:
 - a. At the commencement of the Contract (note – As stated herein, the transition period shall under no circumstances exceed three months);
 - b. During the course of the Contract with additional integrators; and,
 - c. At the completion of the Contract – i.e., the Proposer's ability to work effectively and in harmony with a potential new provider.

4) Business Risk

The Proposer shall identify the five biggest risks as it relates to contract performance, internally and externally, with a plan to mitigate them.

5) Bench Strength / Company Size

Bench Strength / Company Size: Submit a statement listing the total number of staff experienced in ATMS development implementation and support listing the sites, and number of staff at each.

6) Contractor Identity Check/Background Screening Plan

The Proposer shall submit a Contractor Identity Check/Background Screening Plan, which demonstrates how the Proposer will ensure that only employees who were successfully prescreened and properly credentialed perform the services herein. This Plan shall be applicable to all years of the Contract and shall include, but not be limited to, the following:

The length of time researched for the identity check/background screening on new hires, which shall be at a minimum of 10 years of employment history or verification of what an employee documented they have done in the last 10 years preceding the date of the investigation, resources utilized to perform this, and the frequency at which it is performed on current employees.

7) Business Risk Assessment

The Proposer shall submit risk assessment and succession plans to the Port Authority, that assess the business risk in taking on the significant amount of new work that will be required under this Contract. The risk assessment plan should take into account all work currently under contract, as well as work that is under contract to companies which the Proposer owns, controls or has an interest.

8) Background Qualification Questionnaire (To be submitted directly to the Office of the Inspector General)

The Proposer shall submit a completed Background Qualifications Questionnaire (BQQ), required for itself and all consultants, contractors, subcontractors, subconsultants and vendors providing services for the Port Authority, known to the Proposer at the time of proposal submission. This document and instructions for submitting the completed BQQ to the Authority's Office of Inspector General can be obtained at the Authority's website through the following link:

<http://www.panynj.gov/inspector-general/pdf/PANYNJ-BQQ-form-Sep2011.pdf>

F. Acknowledgment of Addenda

If any Addenda are posted or sent as part of this RFP, the Proposer shall complete, sign and include with its Proposal the addenda form(s). In the event any Proposer fails to conform to these instructions, its proposal will nevertheless be construed as though the Addenda had been acknowledged.

If the Proposer downloaded this RFP document, it is the responsibility of the Proposer to periodically check the Port Authority website at <http://www.panynj.gov/DoingBusinessWith/contractors/>

html/current.php and download any addenda that might have been issued in connection with this solicitation.

G. Acceptance of General Contract Provisions

The Port Authority has attached to this RFP as Attachment C entitled “General Contract Provisions” the Terms and Conditions governing the Contract. The Proposer is expected to agree with these Contract Terms and Conditions. However, if the Proposer has any specific exceptions, such exceptions should be set forth in a separate letter included with its response to this RFP. After the proposal due date, the Proposer will be precluded from raising any exceptions unless such exceptions are justified by and directly related to substantive changes in the business or technical requirements and are agreed to by the Proposer and the Port Authority.

H. MBE/WBE Plan

The Proposer shall submit an MBE/WBE Plan in accordance with the MBE/WBE Subcontracting Provisions hereunder.

9. CONDITIONS FOR THE SUBMISSION OF A PROPOSAL

In addition to all other requirements of this RFP, the Proposer agrees to the following conditions for the submission of its proposal.

A. Changes to this RFP

At any time, in its sole discretion, the Port Authority may by written addenda, modify, correct, amend, cancel and/or reissue this RFP. If an addendum is issued prior to the date proposals are due, it will be provided to all parties in the medium in which the parties obtained the RFP. If an addendum is issued after proposals have been received, the addendum will be provided only to those whose proposals remain under consideration at such time.

B. Proposal Preparation Costs

The Port Authority shall not be liable for any costs incurred by the Proposer in the preparation, submittal, presentation, or revision of its proposal, or in any other aspect of the Proposer’s pre-contract activity. No Proposer is entitled to any compensation except under an agreement for performance of services signed by an authorized representative of the Port Authority and the Proposer.

C. Disclosure of Proposal Contents / Use of Ideas and Materials

Proposal information is not generally considered confidential or proprietary. All information contained in the proposal is subject to the “Agreement on Terms of Discussion” attached hereto as Attachment A.

D. Ownership of Submitted Materials

All materials submitted in response to or in connection with this RFP shall become the property of the Port Authority. Selection or rejection of a Proposal shall not affect this right.

E. Subcontractors

If a Proposer intends to use subcontractor(s) the Proposer must identify in its proposal the names of the subcontractor(s) and the portions of the work the subcontractor(s) will perform.

F. Conflict of Interest

If the Proposer or any employee, agent or subcontractor of the Proposer may have a possible conflict of interest, or may give the appearance of a possible conflict of interest, the Proposer shall include in its proposal a statement indicating the nature of the conflict. The Port Authority reserves the right to disqualify the Proposer if, in its sole discretion, any interest disclosed from any source could create a conflict of interest or give the appearance of a conflict of interest. The Port Authority's determination regarding any questions of conflict of interest shall be final.

G. Authorized Signature

Proposals must be signed by an authorized corporate officer (e.g., President or Vice President), General Partner, or such other individual authorized to bind the Proposer to the provisions of its proposal and this RFP.

H. References

The Port Authority may consult any reference familiar with the Proposer regarding its current or prior operations and projects, financial resources, reputation, performance, or other matters. Submission of a proposal shall constitute permission by the Proposer for the Port Authority to make such inquiries and authorization to third parties to respond thereto.

I. Evaluation Procedures and Negotiation

The Port Authority may use such procedures that it deems appropriate to evaluate submitted proposals. The Port Authority may elect to initiate contract negotiations with one or more Proposers including negotiation of costs/price(s) and any other term or condition, including modifying any requirement of this RFP. The option of whether or not to initiate contract negotiations rests solely with the Port Authority.

J. Taxes and Costs

Purchases of services and tangible personal property by the Port Authority in the States of New York and New Jersey are generally exempt from state and local sales and compensating use taxes, and from most federal excises (Taxes). All costs associated with the Contract must reflect this exemption and be stated in U.S. currency.

K. Most Advantageous Proposal/No Obligation to Award

The Port Authority reserves the right to award the Contract to a Proposer other than the Proposer proposing the lowest price. The Contract will be awarded to the Proposer whose proposal the Port Authority believes, in its sole discretion, will be the most advantageous to the Port Authority. Neither

the release of this RFP nor the acceptance of any response thereto shall compel the Port Authority to accept any proposal. The Port Authority shall not be obligated in any manner whatsoever to any Proposer until a proposal is accepted by the Port Authority in the manner provided in the Section of this RFP entitled "Proposal Acceptance or Rejection."

L. Multiple Contract Awards

The Port Authority reserves the right to award multiple Contracts for the products, work and/or services that are the subject matter of this RFP and Proposers are hereby given notice that they may not be the Port Authority's only contractor for such products, work and/or services.

M. Right to Extend Contract

If this is a proposal for a contract for a term of years, including specified options for renewal, the Port Authority reserves the additional right to extend the contract term for an additional (120) days, upon the same terms and conditions of the original Contract negotiated between the Port Authority and the successful Proposer.

N. Rights of the Port Authority

- 1) The Port Authority reserves all its rights at law and equity with respect to this RFP including, but not limited to, the unqualified right, at any time and in its sole discretion, to change or modify this RFP, to reject any and all proposals, to waive defects or irregularities in proposals received, to seek clarification of proposals, to request additional information, to request any or all Proposers to make a presentation, to undertake discussions and modifications with one or more Proposers, or to negotiate an agreement with any Proposer or third person who, at any time, subsequent to the deadline for submissions to this RFP, may express an interest in the subject matter hereof, to terminate further participation in the proposal process by a Proposer or to proceed with any proposal or modified proposal, which in its judgment will, under all circumstances, best serve the Port Authority's interest. The Port Authority may, but shall not be obliged to, consider incomplete proposals or to request or accept additional material or information. The holding of any discussions with any Proposer shall not constitute acceptance of a proposal, and a proposal may be accepted with or without discussions.
- 2) No Proposer shall have any rights against the Port Authority arising from the contents of this RFP, the receipt of proposals, or the incorporation in or rejection of information contained in any proposal or in any other document. The Port Authority makes no representations, warranties, or guarantees that the information contained herein, or in any addenda hereto, is accurate, complete, or timely or that such information accurately represents the conditions that would be encountered during the performance of the contract. The furnishing of such information by the Port Authority shall not create or be deemed to create any obligation or liability upon it for any reason whatsoever and each Proposer, by submitting its proposal, expressly agrees that it has not relied upon the foregoing information, and that it shall not hold the Port Authority liable or responsible therefor in any manner whatsoever. Accordingly, nothing contained herein and no

2/8/16

representation, statement or promise, of the Port Authority, its directors, officers, agents, representatives, or employees, oral or in writing, shall impair or limit the effect of the warranties of the Proposer required by this RFP or Contract and the Proposer agrees that it shall not hold the Port Authority liable or responsible therefor in any manner whatsoever.

At any time and from time to time after the opening of the proposals, the Port Authority may give oral or written notice to one or more Proposers to furnish additional information relating to its proposal and/or qualifications to perform the services contained in this RFP, or to meet with designated representatives of the Port Authority. The giving of such notice shall not be construed as an acceptance of a proposal. Information shall be submitted within three (3) calendar days after the Port Authority's request unless a shorter or longer time is specified therein.

O. No Personal Liability

Neither the Commissioners of the Port Authority, nor any of them, nor any officer, agent or employee thereof shall be charged personally with any liability by a Proposer or another or held liable to a Proposer or another under any term or provision of this RFP or any statements made herein or because of the submission or attempted submission of a proposal or other response hereto or otherwise.

10. ATTACHMENTS

Attachment A – Agreement on Terms of Discussion

Attachment B – Pre-requisites, Requirements

Attachment C – General Contract Provisions

Attachment D – Contract Specific Terms and Conditions

Attachment E – Scope of Work

Attachment F – Cost Proposal

Attachment G – Certificate of No Change

Attachment H– Proposer Reference Form

Attachment I – MBE/WBE Participation Plan

Attachment J – Statement of Subcontractor Payments

Attachment K – Certified Environmentally Preferable Products/Practices

Attachment L– Port Authority Facilities

Attachment M – Audit Security Checklists

Attachment N – Standards and Guidelines for Port Authority Technology

Attachment O – Intelligent Transportation Systems Design Guidelines

ATTACHMENT A - AGREEMENT ON TERMS OF DISCUSSION

The Port Authority’s receipt or discussion of any information (including information contained in any proposal, vendor qualification(s), ideas, models, drawings, or other material communicated or exhibited by us or on our behalf) shall not impose any obligations whatsoever on the Port Authority or entitle us to any compensation therefor (except to the extent specifically provided in such written agreement, if any, as may be entered into between the Port Authority and us). Any such information given to the Port Authority before, with or after this Agreement on Terms of Discussion (“Agreement”), either orally or in writing, is not given in confidence. Such information may be used, or disclosed to others, for any purpose at any time without obligation or compensation and without liability of any kind whatsoever. Any statement which is inconsistent with this Agreement, whether made as part of or in connection with this Agreement, shall be void and of no effect. This Agreement is not intended, however, to grant to the Port Authority rights to any matter, which is the subject of valid existing or potential letters patent.

Any information (including information contained in any proposal, vendor qualification(s), ideas, models, drawings, or other material communicated or exhibited by us or on our behalf) provided in connection with this procurement is subject to the provisions of the Port Authority Freedom of Information Code and Procedure adopted by the Port Authority’s Board of Commissioners on October 22, 2014, which may be found on the Port Authority website at: <http://www.panynj.gov/corporate-information/pdf/foi-code.pdf>. The foregoing applies to any information, whether or not given at the invitation of the Authority.

_____ (Company)

_____ (Signature)

_____ (Title)

_____ (Date)

ORIGINAL AND PHOTOCOPIES OF THIS PAGE ONLY.

DO NOT RETYPE.

ATTACHMENT B – PRE-REQUISITES, REQUIREMENTS

General Note – All customer references must be employees of the company providing the reference .

- A. The Respondent shall have had at least four (4) years of experience within the five (5) year period immediately prior to the date of submission of the RFP, as a business actually engaged in the development, implementation, configuration, and/or customization of ATMS software for use in TMCs or other similar Operation Centers where vehicular traffic is both monitored and controlled using Intelligent Transportation System field devices for data acquisition and information dissemination. Fulfillment of this pre-requisite must be demonstrated by providing a list of projects, clients, and brief project descriptions for work performed during the above period.

#	Customer Company Name	Description of Services Provided	Timeframe Start (MM/YYYY)	Timeframe End (MM/YYYY)
1				
2				
3				
4				
5				

CONTACTS FOR CUSTOMER #1 – #5 ABOVE

#		Contact - Name	Contact - Email	Contact - Phone
1	Prime			
	Alt			
2	Prime			
	Alt			
3	Prime			
	Alt			
4	Prime			
	Alt			
5	Prime			
	Alt			

Attach additional sheets as needed.

B. During the 10-year period prior to the submission of the RFP, the Respondent, or persons or entities owning or controlling the Respondent, shall have satisfactorily completed installation (successfully operational for at least 1 year) and configured their proposed ATMS solution at one or more TMC/Operations Centers (as described in paragraph A above), where a minimum total of 150 ITS assets were monitored and/or controlled. Those assets can be located at any of the facilities and the aggregate total of 150 can be distributed among one or more locations and be of the following types:

- a. Dynamic Message Signs (DMS)
- b. Vehicle Detection Stations (VDS)
- c. Lane Use Control Signals (LUCS)
- d. Variable Speed Limit Signs (VSLS)
- e. TRANSMIT or other Vehicle Probe Systems
- f. CCTV Cameras
- g. Road Weather Information System (RWIS) Stations

Requirement	Contract #1 Customer Company Name _____ (fill in)	Contract #2 Customer Company Name _____ (fill in)	Contract #3 Customer Company Name _____ (fill in)
Contract Duration (Dates)	Start: End:	Start: End:	Start: End:
Contract within the last five (5) Years?	Respond Yes or No	Respond Yes or No	Respond Yes or No
Completed Installation & successfully operational for at least one year	Provide Date Installation Was Completed:	Provide Date Installation Was Completed:	Provide Date Installation Was Completed:
Minimum of three (3) TMC Operation Centers (Provide list the centers.)	Provide Complete Address of TMC Centers:	Provide Complete Address of TMC Centers:	Provide Complete Address of TMC Centers:

Dynamic Message Signs (DMS)	Provide quantity of DMS:	Provide quantity of DMS:	Provide quantity of DMS:
Vehicle Detection Stations (VDS)	(Provide quantity of VDS)	(Provide quantity of VDS)	(Provide quantity of VDS)
Lane Use Control Signals (LUCS)	(Provide quantity of LUCS)	(Provide quantity of LUCS)	(Provide quantity of LUCS)
Variable Speed Limit Signs (VSLS)	(Provide quantity of VSLS)	(Provide quantity of VSLS)	(Provide quantity of VSLS)
TRANSMIT or other Vehicle Probe Systems	(Provide TRANSMIT or other Vehicle Probe System quantity)	(Provide TRANSMIT or other Vehicle Probe System quantity)	(Provide TRANSMIT or other Vehicle Probe System quantity)
CCTV Cameras –	(Provide CCTV quantity)	(Provide CCTV quantity)	(Provide CCTV quantity)
Road Weather Information System (RWIS)	(Provide RWIS quantity)	(Provide RWIS quantity)	(Provide RWIS quantity)
Contract Value	Contract Value	Contract Value	Contract Value

2/8/16

- C. The Respondent shall demonstrate that it has earned gross revenues of at least \$1,000,000 a year for the last three (3) fiscal years from the type of services described herein. Provide a statement on letterhead signed by your CFO or a CPA certifying that your company meets the gross revenues specified above.

ATTACH DOCUMENTATION CERTIFYING AND SUPPORTING THIS PREREQUISITE

- D. The Respondent must demonstrate that the ATMS is compliant with National Transportation Communications for ITS Protocol (NTCIP) and Traffic Management Data Dictionary (TMDD) Standards for Center-to-Center (C2C) communications protocol referenced herein and in the RFP. The Respondent must have documented experience in the development of SIs for NTCIPv2 or later protocol for, at a minimum, DMS, VDS, and CCTV cameras as well as Center-to-Center (C2C) Communications conforming to TMDD Standards. Fulfillment of this pre-requisite must be demonstrated by identifying specific implementations with accompanying contact information for a reference.

ATTACH DOCUMENTATION CERTIFYING AND SUPPORTING THIS PREREQUISITE

- E. The Respondent must have documented experience in the development of SIs to push incident, travel time, and other travel information to external systems such as 511NY, 511NJ, Twitter, and specially developed smart phone applications. Fulfillment of the pre-requisite must be demonstrated by identifying specific implementations with accompanying contact information for reference.

ATTACHMENT C - GENERAL CONTRACT PROVISIONS

1. GENERAL AGREEMENT

The undersigned (hereinafter referred to as the "Contractor" or "you") agrees to provide, and The Port Authority of New York and New Jersey (hereinafter referred to as the "Authority") agrees to accept to provide all the necessary supervision, personnel, equipment, materials and all other things necessary to perform the Services required by this Contract as more fully set forth in the Scope of Work attached hereto and made a part hereof. The Scope of Work requires the doing of all things necessary or proper for or incidental to the requirements as set forth in the Scope of Work. All things not expressly mentioned in the Scope of Work but involved in carrying out their intent are required by the Scope of Work and the Contractor shall perform the same as though they were specifically mentioned, described and delineated.

2. DEFINITIONS

To avoid undue repetition, the following terms, as used in this Agreement, shall be construed as follows:

Authority or Port Authority - means the Port Authority of New York and New Jersey.

Contract, Document or Agreement - mean the writings setting forth the scope, terms, conditions and Specifications for the procurement of Goods and/or Services, as defined hereunder and shall include, but not be limited to: Invitation for Bid (IFB), Request for Quotation (RFQ), Request for Proposal (RFP), Purchase Order (PO), Cover Sheet, executed Signature Sheet, AND PRICING SHEETS with Contract prices inserted, "STANDARD CONTRACT TERMS AND CONDITIONS," and, if included, attachments, endorsements, schedules, exhibits, or drawings, the Authority's acceptance and any written addenda issued over the name of the Assistant Director, Commodities and Services Division, Procurement Department.

Days or Calendar Days - mean consecutive calendar days, Saturdays, Sundays, and holidays, included.

Director - means the Director of the Department which operates the facility of the Port Authority at which the services hereunder are to be performed, for the time being, or his/her successor in duties for the purpose of this Contract, or one of his/her authorized representatives for the purpose of this Contract.

Facility- Port Authority Facilities within the Port District, as set forth in Attachment L: "Port Authority Facilities".

Project Manager (or Manager) - means the individual with day-to-day responsibility for managing the project on behalf of the Port Authority. The Project Manager will be Gary Mason.

No person shall be deemed a representative of the Director or Manager except to the extent specifically authorized in an express written notice to the Contractor signed by the Director or Manager, as the case may be. Further, no person shall be deemed a successor in duties of the Director unless the Contractor is so notified in writing signed by the Assistant Director, Commodities & Services Division, Procurement

2/8/16

Department. No person shall be deemed a successor in duties of the Manager unless the Contractor is so notified in a writing signed by the Director.

Services or Work - mean all services, equipment and materials (including materials and equipment, if any, furnished by the Authority) and other facilities and all other things necessary or proper for, or incidental to the services to be performed or goods to be furnished in connection with the service to be provided hereunder, as set forth in the Scope of Work.

Specifications- mean all requirements of this RFP, technical and otherwise, for the performance of the Scope of Work and services hereunder.

Holidays: The following legal holidays will be observed at Port Authority offices and facilities:

New Year's Day	Columbus Day
Martin Luther King, Jr. Day	Veteran's Day
Presidents Day	Thanksgiving Day
Memorial Day	Day After Thanksgiving
Independence Day	Christmas Day
Labor Day	

Do not perform any Work unless authorized by the Authority on these days.

Minority Business Enterprise (MBE) - means a business entity which is at least fifty-one percent (51%) owned and controlled by one or more members of one or more minority groups, or, in the case of a publicly held corporation, at least fifty-one percent (51%) of the stock of which is owned by one or more minority groups, and whose management and daily business operations are controlled by one or more such individuals who are citizens or permanent resident aliens.

"Minority Group" means any of the following racial or ethnic groups:

- (a) Black persons having origins in any of the Black African racial groups not of Hispanic origin;
- (b) Hispanic persons of Mexican, Puerto Rican, Dominican, Cuban, Central or South American culture or origin, regardless of race;
- (c) Asian and Pacific Islander persons having origins in any of the original peoples of the Far East, Southeast Asia, The Indian Subcontinent, or the Pacific Islands;
- (d) Native American or Alaskan native persons having origins in any of the original peoples of North America and maintaining identifiable tribal affiliations through membership and participation or community identification.
- (e) Month - unless otherwise specified, means a calendar month.

Site of the Work - or words of similar import shall mean the Facility and all buildings and properties

2/8/16

associated therewith as described in this Contract.

Small Business Enterprise (SBE) - The criteria for a Small Business Enterprise are:

- o The principal place of business must be located in New York or New Jersey;
- o The firm must have been in business for at least three years with activity;
- o Average gross income limitations by industry as established by the Port Authority.

Subcontractor - mean anyone who performs work (other than or in addition to the furnishing of materials, plant or equipment) in connection with the services to be provided hereunder, directly or indirectly for or on behalf of the Contractor (and whether or not in privity of contract with the Contractor), but shall not include any person who furnished merely his own personal labor or his own personal services. "Subcontractor", however, shall exclude the Contractor or any subsidiary or parent of the Contractor or any person, firm or corporation which has a substantial interest in the Contractor or in which the Contractor or the parent or the subsidiary of the Contractor, or an officer or principal of the Contractor or of the parent of the subsidiary of the Contractor has a substantial interest, provided, however, that for the purpose of the clause hereof entitled "Assignments and Subcontracts" the exclusion in this paragraph shall not apply to anyone but the Contractor itself.

Week - unless otherwise specified, means seven (7) consecutive calendar days, Saturdays, Sundays, and holidays.

Woman-owned Business Enterprise (WBE) - shall mean a business enterprise which is at least fifty-one percent (51%) owned by one or more women, or, in the case of a publicly held corporation, at least fifty-one percent (51%) of the stock of which is owned by one or more women and whose management and daily business operations are controlled by one or more women who are citizens or permanent or resident aliens.

Work Day- unless otherwise specified, means a day between Monday and Friday with Monday and Friday included.

3. GENERAL PROVISIONS

- A. Under no circumstances shall you or your subcontractors communicate in any way with any department, board, agency, commission, or other organization or any person whether governmental or private in connection with the services to be performed hereunder except upon prior written approval and instructions of the Director, provided, however, that data from manufacturers and suppliers of materials, devices and equipment shall be obtained by you when you find such data necessary unless otherwise instructed by the Authority.
- B. Any services performed for the benefit of the Authority at any time by you or on your behalf, even if expressly and duly authorized by the Authority, shall be deemed to be rendered under and subject to this Agreement (unless referable to another expressly written, duly executed agreement by the same parties), whether such additional services are performed prior to, during or subsequent to the services described herein, and no rights or obligations shall arise out of such additional services except as provided under this Agreement.

- C. The Contractor shall observe and obey (and compel its officers, employees, guests, invitees, and those doing business with it, to observe and obey) the rules and regulations of the Port Authority now in effect, and such further rules and regulations which may from time to time during the effective period of this Contract, be promulgated by the Port Authority for reasons of safety, health, preservation of property, or maintenance of a good and orderly appearance of the Facilities, or for the safe and efficient operation of the Facilities. The Port Authority agrees that, except in cases of emergency, it shall give notice to the Contractor of every rule and regulation hereafter adopted by it.
- D. This Contract does not constitute the Contractor as an agent or representative of the Port Authority for any purpose whatsoever. The Contractor shall perform all services hereunder as an independent Contractor and the Contractor, its officers, and employees shall not be deemed to be agents, servants, or employees of the Port Authority.

4. INTELLECTUAL PROPERTY

- A. Except as provided below: as between the Port Authority and the Contractor all process flows, codes including, but not limited to scripts, programs, routines, processes, procedures, documentation, estimates, reports, records, data, charts, documents, models, designs, renderings, drawings, specifications, photographs, computations, computer tapes or discs, and other documentation of any type whatsoever, whether electronic or in the form of writing, figures or delineations, which are prepared or compiled in connection with this Agreement, shall become the exclusive property of the Authority, and the Authority shall have the exclusive right to use or permit the use of them and any ideas or methods represented by them for any purpose and at any time without other compensation than that specifically provided for herein. With regard to training manuals or any other knowledge transfer documentation, communication or presentation prepared under this Agreement the Authority shall expressly have the right to use, alter and reproduce including electronically, said manuals for its internal business purposes. The Contractor hereby warrants and represents that the Authority will have at all times the ownership and rights provided for in the immediately preceding sentence free and clear of all claims of third persons whether presently existing or arising in the future and whether presently known to either of the parties to this Agreement or not. Any information given to the Port Authority before, with or after submission of the Agreement on Terms of Discussion, either orally or in writing, is not given in confidence and may be used, or disclosed to others, for any purpose at any time without obligation or compensation and without liability of any kind whatsoever except as otherwise set forth in the Agreement On Terms Of Discussion.

The right to use all patented materials, appliances, processes of manufacture or types of construction, trade and service marks, copyrights and trade secrets, collectively hereinafter referred to as "Intellectual Property Rights", in the performance of the work, shall be obtained by the Contractor without separate or additional compensation. Where the services under this Agreement require the Contractor to provide materials, equipment or software for the use of the Port Authority or its employees or agents, the Port Authority shall be provided with the

Intellectual Property Rights required for such use without further compensation than is provided for under this Agreement.

- B. All preexisting information or documentation including computer programs or code including source code, of the Contractor, utilized by the Contractor hereunder in the performance of his services hereunder shall be deemed licensed to the Authority for the duration and purposes of this agreement, but shall remain the property of the Contractor.
- C. When in the performance of the contract services the Contractor utilizes passwords or codes for any purpose, at any time during or after the performance of such services, upon written request by the Authority, the Contractor shall make available to the designated Authority representative all such passwords and codes.
- D. Third party software not specially prepared for the purpose of this agreement but utilized by the Contractor hereunder in the performance of his services hereunder shall be licensed to the Contractor and the Authority for the duration and purposes of this agreement but shall remain the property of said third party.
- E. The above-described software shall be furnished by the Contractor without additional compensation.

5. PROPRIETARY RIGHTS IN SUBJECT MATTER NOT WITHIN THE INTELLECTUAL PROPERTY CLAUSE

If in accordance with this Contract the Contractor furnishes research, development or consultative services in connection with the performance of the Work and if in the course of such research, development, or consultation patentable or copyrightable subject matter or trade secrets or other proprietary matter is produced by the Contractor, its officers, agents, employees, subcontractors, or suppliers, not custom software, and not covered under clause 6 entitled Intellectual Property, the Authority shall have, without cost or expense to it, an irrevocable, non-exclusive, royalty-free license to make, have made, and use, either itself or by anyone on its behalf, such subject matter in connection with any activity now or hereafter engaged in or permitted by the Authority. Promptly upon request by the Authority, the Contractor shall furnish or obtain from the appropriate person a form of license satisfactory to the Authority, but it is expressly understood and agreed that as between the Contractor and the Authority the license herein provided for shall nevertheless arise for the benefit of the Authority immediately upon the production of said subject matter and shall not await formal exemplification in a written license agreement as provided for above. Such license may be transferred by the Authority to its successors, immediate or otherwise, in the operations of or ownership of any facility now or hereafter operated by the Authority or the Authority but such license shall not be otherwise transferable.

The right of the Authority as well as the Contractor to use all patented material, compositions of matter, manufactures, apparatus, appliances, processes of manufacture or types of construction as well as any copyrightable matter, trade secrets or other proprietary matters, shall be obtained by the Contractor

without separate or additional compensation whether the same is patented or copyrighted before, during or after the performance of the Work.

6. INDEMNITY IN REGARD TO INFRINGEMENT MATTER

The Contractor shall indemnify the Authority against and save it harmless from all loss and expense incurred in the defense, settlement or satisfaction of any claims in the nature of patent, copyright, or other proprietary rights infringement arising out of or in connection with the Authority's use, in accordance with the preceding clause of such patentable subject matter or patented material, compositions of matter, manufactures, apparatus, appliances, processes of manufacture or types of construction, or copyrighted matter or other matter protected as intellectual property. If requested by the Authority and if notified promptly in writing of any such claims, the Contractor shall conduct all negotiations with respect to and defend such claim without expense to the Authority. If the Authority be enjoined from using any of the facilities which form the subject matter of this Contract, and as to which the Contractor is to indemnify the Authority against proprietary rights claims, the Authority may, at its option and without thereby limiting any other right it may have hereunder or at law or in equity, require the Contractor to supply, temporarily or permanently, facilities not subject to such injunction and not infringing any proprietary rights and if the Contractor shall fail to do so, the Contractor shall, at its expense, remove all such facilities and refund the cost thereof to the Authority and otherwise equitably adjust compensation and take such steps as may be necessary to ensure compliance by the Authority with such injunction, to the satisfaction of the Authority.

The Contractor shall promptly and fully inform the Director of any claims or disputes for infringement or otherwise, whether existing or potential, of which it has knowledge relating to any Intellectual Property used, developed or licensed in connection with the performance of the Work or otherwise in connection with this Contract.

7. CONTRACT RECORDS AND DOCUMENTS – PASSWORDS AND CODES

When the performance of the contract services requires the Contractor to produce, compile or maintain records, data, drawings, or documents of any kind, regardless of the media utilized, then all such records, drawings, data and documents which are produced, prepared or compiled in connection with this contract, shall become the property of the Port Authority, and the Port Authority shall have the right to use or permit the use of them and any ideas or methods represented by them for any purpose and at any time without other compensation than that specifically provided herein.

When in the performance of the contract services the Contractor utilizes passwords or codes for any purpose, at any time during or after the performance of such services, upon written request by the Authority, the Contractor shall make available to the designated Authority representative all such passwords and codes.

8. COMPLIANCE WITH WEB SITE TERMS OF USE AND PRIVACY POLICIES

Subject to all of the provisions of this Contract including, without limitation, the obligations of the Contractor under the section hereof entitled "Indemnification," the Contractor shall, and shall compel its employees, agents and subcontractors, to strictly abide by and comply with the policies established

by the Authority governing the use of the Authority's web sites as set forth in the Authority web sites Terms of Use and Privacy Statement as the same may be supplemented or amended. The Contractor shall immediately implement all procedures in connection with such policies and in furtherance thereof as directed by the Authority.

9. TIME IS OF THE ESSENCE

The Contractor's obligations for the performance and completion of all work within the time or times provided for in this Contract are of the essence of this Contract.

10. FINAL PAYMENT

After satisfactory completion of all services required hereunder, and upon receipt from the Contractor of such information as may be required, the Director shall certify in writing to the Contractor the total compensation earned by the Contractor.

If so required, the Contractor shall thereupon furnish to the Authority a detailed sworn statement of all claims, just and unjust, of subcontractors, materialmen and other third persons then outstanding which he has reason to believe may thereafter be made on account of the services provided under this Agreement.

Within thirty days after issuance of such certificate of total compensation earned (or within thirty days after receipt of the documents provided for in the immediately preceding paragraph, if required and if such date is later), the Port Authority shall pay to the Contractor by check the amount stated in said certificate, less all other payments and advances whatsoever to or for the account of the Contractor. All prior estimates and payments shall be subject to correction in this payment, which is throughout this Agreement called the Final Payment.

The acceptance by the Contractor, or by anyone claiming by or through him, of the Final Payment shall be and shall operate as a release to the Authority of all claims and of all liability to the Contractor for all things done or furnished in connection with this contract and for every act and neglect of the Authority and others relating to or arising out of the this contract, including claims arising out of breach of the contract and claims based on claims of third persons.

The Contractor's agreement as provided in the immediately preceding paragraph shall be deemed to be based upon the consideration forming part of this Contract as a whole and not to be gratuitous; but in any event even if deemed gratuitous and without consideration, such agreement as provided in the immediately preceding paragraph shall nevertheless be effective. Such release shall include all claims, whether or not in litigation and even though still under consideration by the Authority. Such release shall be effective notwithstanding any purported reservation of right by the Contractor to preserve such claim. The acceptance of any check designated as "Final Payment" or bearing any similar designation shall be conclusively presumed to demonstrate the intent of the Contractor that such payment was intended to be accepted as final, with the consequences provided in this numbered clause, notwithstanding any purported reservation of rights.

The Contractor agrees that he shall not be entitled to, and hereby waives any right he might otherwise have to, and shall not seek any judgment whether under this Contract or otherwise for any such Final

Payment or for an amount equivalent thereto or based thereon, or for any part thereof, if such judgment would have the effect of varying, setting aside, disregarding or making inapplicable the terms of this numbered clause or have the effect in any way of entitling the Contractor to accept such Final Payment or an amount equivalent thereto or based thereon or any part thereof other than in the same fashion as a voluntary acceptance of a Final Payment subject to all the terms of this Contract including this numbered clause, unless and until the Contractor should obtain a judgment on any claim arising out of or in connection with this Contract (including a claim based on breach of contract) for an amount not included in said Final Payment.

11. DEFAULT, REVOCATION OR SUSPENSION OF CONTRACT

A. If one or more of the following events shall occur:

1. If fire or other event shall destroy all or a substantial part of the Facility, asset or infrastructure necessary to perform the Scope of Work.

If any governmental agency shall condemn or take a temporary or permanent interest in all or a substantial part of the Facility, or all of a part of the Port Authority's interest herein;

then upon the occurrence of such event or at any time thereafter during the continuance thereof, the Port Authority shall have the right on twenty-four (24) hours written notice to the Contractor to revoke this Contract, such revocation to be effective upon the date and time specified in such notice.

In such event this Contract shall cease and expire on the effective date of revocation as if said date were the date of the expiration of this Contract. Such revocation shall not, however, relieve the Contractor of any liabilities or obligations hereunder which shall have accrued on or prior to the effective date of revocation.

B. If one or more of the following events shall occur:

1. The Contractor shall become insolvent, or shall take the benefit of any present or future insolvency statute, or shall make a general assignment for the benefit of creditors, or file a voluntary petition in bankruptcy or a petition or answer seeking an arrangement or its reorganization or the readjustment of its indebtedness under the federal bankruptcy laws or under any other law or statute of the United States or of any State thereof, or consent to the appointment of a receiver, trustee, or liquidator of all or substantially all its property; or
2. By order or decree of a court the Contractor shall be adjudged bankrupt or an order shall be made approving a petition filed by any of the creditors, or, if the Contractor is a corporation, by any of the stockholders of the Contractor, seeking its reorganization or the readjustment of its indebtedness under the federal bankruptcy laws or under any law or statute of the United States or of any State thereof; or
3. A petition under any part of the federal bankruptcy laws or an action under any present or future insolvency law or statute shall be filed against the Contractor and shall not be

dismissed within thirty (30) days after the filing thereof; or

4. The interest of the Contractor under this Contract shall be transferred to, passed to or devolve upon, by operation of law or otherwise, any other person, firm or corporation, or
5. The Contractor, if a corporation, shall, without the prior written approval of the Port Authority, become a surviving or merged corporation in a merger, a constituent corporation in a consolidation, or a corporation in dissolution; or
6. If the Contractor is a partnership, and the said partnership shall be dissolved as the result of any act or omission of its copartners or any of them, or by operation of law or the order or decree of any court having jurisdiction, or for any other reason whatsoever; or
7. By or pursuant to, or under authority of any legislative act, resolution or rule, or any order or decree of any court or governmental board, agency or officer having jurisdiction, a receiver, trustee, or liquidator shall take possession or control of all or substantially all of the property of the Contractor and such possession or control of all or substantially all of the property of the Contractor and shall continue in effect for a period of fifteen (15) days;

then upon the occurrence of any such event or at any time thereafter during the continuance thereof, the Port Authority shall have the right upon five (5) days notice to the Contractor to terminate this Contract and the rights of the Contractor hereunder; termination to be effective upon the date and time specified in such notice as if said date were the date of the expiration of this Contract. Termination shall not relieve the Contractor of any liabilities or obligations hereunder which have accrued on or prior to the effective date of termination.

C. If any of the following shall occur:

1. The Contractor shall cease, abandon any part of the service, desert, stop or discontinue its services in the premises for any reason whatsoever and regardless of the fault of the Contractor; or
2. The Contractor shall fail to keep, perform and observe each and every other promise, covenant and agreement set forth in this Contract on its part to be kept, performed or observed, within five (5) days after receipt of notice of default thereunder from the Port Authority (except where fulfillment of its obligations requires activity over a greater period of time, and the Contractor shall have commenced to perform whatever may be required for fulfillment within five (5) days after receipt of notice and continues such performance without interruption except for causes beyond its control);

then upon the occurrence of any such event or during the continuance thereof, the Port Authority shall have the right on twenty four (24) hours notice to the Contractor to terminate this Contract and the rights of the Contractor hereunder, termination to be effective upon the date and time specified in such notice. Termination shall not relieve the Contractor of any liabilities, which shall have

accrued on or prior to the effective date of termination.

- D. If any of the events enumerated in this Section shall occur prior to commencement date of this Contract the Port Authority upon the occurrence of any such event or any time thereafter during the continuance thereof by twenty-four (24) hours notice may terminate or suspend this Contract and the rights of the Contractor hereunder, such termination or suspension to be effective upon the date specified in such notice.
- E. No payment by the Port Authority of any monies to the Contractor for any period or periods after default of any of the terms, covenants or conditions hereof to be performed, kept and observed by the Contractor and no act or thing done or omitted to be done by the Port Authority shall be deemed to be a waiver of the right of the Port Authority to terminate this Contract or of any other right or remedies to which the Port Authority may be entitled because of any breach thereof. No waiver by the Port Authority of any default on the part of the Contractor in the performance of any of the terms, covenants and conditions hereof to be performed, kept or observed by the Contractor shall be or be construed to be a waiver by the Port Authority of any other subsequent default in the performance of any of the said terms, covenants and conditions.
- F. In addition to all other rights of revocation or termination hereunder and notwithstanding any other provision of this Contract the Port Authority may terminate this Contract and the rights of the Contractor hereunder without cause at any time upon five (5) days written notice to the Contractor and in such event this Contract shall cease and expire on the date set forth in the notice of termination as fully and completely as though such dates were the original expiration date hereof and if such effective date of termination is other than the last day of the month, the amount of the compensation due to the Contractor from the Port Authority shall be prorated when applicable on a daily basis. Such cancellation shall be without prejudice to the rights and obligations of the parties arising out of portions already performed but no allowance shall be made for anticipated profits.
- G. Any right of termination contained in this paragraph, shall be in addition to and not in lieu of any and all rights and remedies that the Port Authority shall have at law or in equity consequent upon the Contractor's breach of this Contract and shall be without prejudice to any and all such other rights and remedies. It is hereby specifically agreed and understood that the exercise by the Port Authority of any right of termination set forth in this paragraph shall not be or be deemed to be an exercise by the Port Authority of an election of remedies so as to preclude the Port Authority from any right to money damages it may have for the period prior to the effective date of termination to the original expiration date of the Contract, and this provision shall be deemed to survive the termination of this Contract as aforesaid.
- H. If (1) the Contractor fails to perform any of its obligations under this Contract or any other agreement between the Port Authority and the Contractor (including its obligation to the Port Authority to pay any claim lawfully made against it by any supplier, subcontractor or worker or other person which arises out of or in connection with the performance of this Contract or any other agreement with the Port Authority) or (2) any claim (just or unjust) which arises out of or

in connection with this Contract or any other agreement between the Port Authority and the Contractor is made against the Port Authority or (3) any subcontractor under this Contract or any other agreement between the Port Authority and the Contractor fails to pay any claims lawfully made against it by any supplier, subcontractor, worker or other third person which arises out of or in connection with this Contract or any other agreement between the Port Authority and the Contractor or if in the opinion of the Port Authority any of the aforesaid contingencies is likely to arise, then the Port Authority shall have the right, in its discretion, to withhold out of any payment (final or otherwise) such sums as the Port Authority may deem ample to protect it against delay or loss or to assure the payment of just claims of third persons, and to apply such sums in such manner as the Port Authority may deem proper to secure such protection or satisfy such claims. All sums so applied shall be deducted from the Contractor's compensation. Omission by the Port Authority to withhold out of any payment, final or otherwise, a sum for any of the above contingencies, even though such contingency has occurred at the time of such payment, shall not be deemed to indicate that the Port Authority does not intend to exercise its right with respect to such contingency. Neither the above provisions for rights of the Port Authority to withhold and apply monies nor any exercise or attempted exercise of, or omission to exercise, such rights by the Port Authority shall create any obligation of any kind to such supplier, subcontractors, worker or other third persons. If, however, the payment of any amount due the Contractor shall be improperly delayed, the Port Authority shall pay the Contractor interest thereon at the rate of 6% per annum for the period of the delay, it being agreed that such interest shall be in lieu of and in liquidation of any damages to the Contractor because of such delay.

- I. If the Port Authority has paid any sum or has incurred any obligation or expense which the Contractor has agreed to pay or reimburse the Port Authority, or if the Port Authority is required or elects to pay any sum or sums or incurs any obligations or expense by reason of the failure, neglect or refusal of the Contractor to perform or fulfill any one or more of the conditions, covenants, or agreements contained in this Contract, or as a result of an act of omission of the Contractor contrary to the said conditions, covenants and agreements, the Contractor shall pay to the Port Authority the sum or sums so paid or expense so incurred, including all interests, costs and damages, promptly upon the receipt of the Port Authority's statement therefore. The Port Authority may, however, in its discretion, elect to deduct said sum or sums from any payment payable by it to the Contractor.
- J. If the Port Authority pays any installment to the Contractor without reducing said installment as provided in this Contract, it may reduce any succeeding installment by the proper amount, or it may bill the Contractor for the amount by which the installment paid should have been reduced and the Contractor shall pay to the Port Authority any such amount promptly upon receipt of the Port Authority's statement therefore.
- K. The Port Authority shall also have the rights set forth above in the event the Contractor shall become insolvent or bankrupt or if his affairs are placed in the hands of a receiver, trustee or assignee for the benefit of creditors.

12. WITHHOLDING OF PAYMENT

If (1) the Contractor fails to perform any of its obligations under this Contract or any other agreement between the Authority and the Contractor (including his obligation to the Authority to pay any claim lawfully made against him by any materialman, subcontractor or workman or other person which arises out of or in connection with the performance of this Contract or any other agreement with the Authority) or (2) any claim (just or unjust) which arises out of or in connection with this Contract or any other agreement between the Authority and the Contractor is made against the Authority or (3) any subcontractor under this Contract or any other agreement between the Authority and the Contractor fails to pay any claims lawfully made against him by any materialman, subcontractor, workman or other third person which arises out of or in connection with this Contract or any other agreement between the Authority and the Contractor or if in the opinion of the Authority any of the aforesaid contingencies is likely to arise, then the Authority shall have the right, in its discretion, to withhold out of any payment (final or otherwise and even though such payment has already been certified as due) such sums as the Authority may deem ample to protect it against delay or loss or to assure the payment of just claims of third persons, and to apply such sums in such manner as the Port Authority may deem proper to protect it against delay or loss or to satisfy such claims. All sums so applied shall be deducted from the Contractor's compensation. Omission by the Authority to withhold out of any payment, final or otherwise, a sum for any of the above contingencies, even though such contingency has occurred at the time of such payment, shall not be deemed to indicate that the Authority does not intend to exercise its right with respect to such contingency. Neither the above provisions for rights of the Authority to withhold and apply monies nor any exercise or attempted exercise of, or omission to exercise, such rights by the Authority shall create any obligation of any kind to such materialman, subcontractors, workman or other third persons.

Until actual payment to the Contractor, its right to any amount to be paid under this Contract (even though such amount has already been certified as due) shall be subordinate to the rights of the Authority under this clause.

13. CONTRACTOR PERSONNEL STANDARDS OF PERFORMANCE

The Contractor shall furnish sufficiently trained management, supervisory, technical and operating personnel to perform the services required of the Contractor under this Contract. If, in the opinion of the Director, any of the Contractor's personnel are not satisfactory in the performance of services to be furnished hereunder, the Contractor shall remove such personnel and replace them with personnel satisfactory to the Director.

At the time the Contractor is carrying out its operations there may be other persons working physically in the vicinity or in the same logical or technical infrastructure. . The Contractor shall so conduct its operations as to work in harmony and not endanger, interfere with or delay the operations of others, all to the best interests of The Authority and others and as may be directed by the Director.

14. DESIGNATED SECURE AREAS

Services under the Contract may be required in designated secure areas, as the same may be designated

by the Manager from time to time ("Secure Areas"). The Port Authority shall require the observance of certain security procedures with respect to Secure Areas, which may include the escort to, at, and/or from said high security areas by security personnel designated by the Contractor or any subcontractor's personnel required to work therein. All personnel that require access to designated secure areas who are not under positive escort by an authorized individual will be required to undergo background screening and personal identity verification.

Forty-eight (48) hours prior to the proposed performance of any work in a Secure Area, the Contractor shall notify the Manager. The Contractor shall conform to the procedures as may be established by the Manager from time to time and at any time for access to Secure Areas and the escorting of personnel hereunder. Prior to the start of work, the Contractor shall request a description from the Manager of the Secure Areas which will be in effect on the commencement date. The description of Secure Areas may be changed from time to time and at any time by the Manager during the term of the Contract.

15. NOTIFICATION OF SECURITY REQUIREMENTS

The Authority has the responsibility of ensuring safe, reliable and secure transportation facilities, systems, and projects to maintain the well-being and economic competitiveness of the region. Therefore, the Authority reserves the right to deny access to certain documents, sensitive security construction sites and facilities (including rental spaces) to any person that declines to abide by Port Authority security procedures and protocols, any person with a criminal record with respect to certain crimes or who may otherwise poses a threat to the construction site or facility security. The Authority reserves the right to impose multiple layers of security requirements on the Contractor, its staff and subcontractors and their staffs depending upon the level of security required, or may make any amendments with respect to such requirements as determined by the Authority.

These security requirements may include but are not limited to the following:

- Contractor/ Subcontractor identity checks and background screening

The Port Authority's designated background screening provider may require inspection of not less than two forms of valid/current government issued identification (at least one having an official photograph) to verify staff's name and residence; screening federal, state, and/or local criminal justice agency information databases and files; screening of any terrorist identification files; access identification to include some form of biometric security methodology such as fingerprint, facial or iris scanning, or the like.

The Contractor may be required to have its staff, and any subcontractor's staff, material-men, visitors or others over whom the Contractor/subcontractor has control, authorize the Authority or its designee to perform background checks, and a personal identity verification check. Such authorization shall be in a form acceptable to the Authority. The Contractor and subcontractors may also be required to use an organization designated by the Authority to perform the background checks.

As of January 29, 2007, the Secure Worker Access Consortium (S.W.A.C.) is the only Port Authority approved provider to be used to conduct background screening and personal identity verification,

except as otherwise required by federal law and/or regulation (such as the Transportation Worker Identification Credential for personnel performing in secure areas at Maritime facilities). Information about S.W.A.C., instructions, corporate enrollment, online applications, and location of processing centers can be found at <http://www.secureworker.com>, or S.W.A.C. may be contacted directly at (877) 522-7922 for more information and the latest pricing. The cost for said background checks for staff that pass and are granted a credential shall be reimbursable to the Contractor (and its subcontractors) as an out-of-pocket expense as provided herein. Staff that are rejected for a credential for any reason are not reimbursable.

- Issuance of Photo Identification Credential

No person will be permitted on or about the Authority construction site or facility (including rental spaces) without a facility-specific photo identification credential approved by the Authority. If the authority requires facility-specific identification credential for the Contractor's and the subcontractor's staff, the Authority will supply such identification at no cost to the Contractor or its subcontractors. Such facility-specific identification credential shall remain the property of the Authority and shall be returned to the Authority at the completion or upon request prior to completion of the individual's assignment at the specific facility. It is the responsibility of the appropriate Contractor or subcontractor to immediately report to the Authority the loss of any staff member's individual facility-specific identification credential. The Contractor or subcontractor shall be billed for the cost of the replacement identification credential. Contractor's and subcontractor's staff shall display Identification badges in a conspicuous and clearly visible manner, when entering, working or leaving an Authority construction site or facility.

Employees may be required to produce not less than two forms of valid/current government issued identification having an official photograph and an original, un laminated social security card for identify and SSN verification. Where applicable, for sensitive security construction sites or facilities, successful completion of the application, screening and identify verification for all employees of the Contractor and subcontractors shall be completed prior to being provided a S.W.A.C. ID Photo Identification credential.

- Access control, inspection, and monitoring by security guards

The Authority may provide for Authority construction site or facility (including rental spaces) access control, inspection and monitoring by Port Authority Police or Authority retained contractor security guards. However, this provision shall not relieve the Contractor of its responsibility to secure its equipment and work and that of its subconsultant/subcontractor's and service suppliers at the Authority construction site or facility (including rental spaces). In addition, the Contractor, subcontractor or service provider is not permitted to take photographs, digital images, electronic copying and/or electronic transmission or video recordings or make sketches on any other medium at the Authority construction sites or facilities (including rental spaces), except when necessary to perform the Work under this Contract, without prior written permission from the Authority. Upon request, any photograph, digital images, video recording or sketches made of the Authority construction site or facility shall be submitted to the Authority to

determine compliance with this paragraph, which submission shall be conclusive and binding on the submitting entity.

- Compliance with the Port Authority Information Security Handbook

The Contract may require access to Port Authority information considered Protected Information (“PI”) as defined in the Port Authority Information Security Handbook (“Handbook”), dated October, 2008, corrected as of November 14, 2013, and as may be further amended. The Handbook and its requirements are hereby incorporated into this agreement and will govern the possession, distribution and use of PI if at any point during the lifecycle of the project or solicitation it becomes necessary for the Contractor to have access to PI. Protecting sensitive information requires the application of uniform safeguarding measures to prevent unauthorized disclosure and to control any authorized disclosure of this information within the Port Authority or when released by the Port Authority to outside entities. The following is an outline of some of the procedures, obligations and directives contained in the Handbook:

- (1) require that the Contractor and subcontractors, when appropriate, sign Non-Disclosure Agreements (NDAs), or an Acknowledgment of an existing NDA, provided by the Authority as a condition of being granted access to Confidential Information categorized and protected as per the Handbook;
- (2) require that individuals needing access to PI be required to undergo a background check, pursuant to the process and requirements noted in § 3.2 of the Information Security Handbook.
- (3) require Contractors and commercial enterprises to attend training to ensure security awareness regarding Port Authority information;
- (4) specific guidelines and requirements for the handling of PI to ensure that the storage and protection of PI;
- (5) restrictions on the transfer, shipping, and mailing of PI;
- (6) prohibitions on the publication, posting, modifying, copying, reproducing, republishing, uploading, transmitting, or distributing PI on websites or web pages. This may also include restricting persons, who either have not passed a pre-screening background check, or who have not been granted access to PI, from viewing such information;
- (7) require that PI be destroyed using certain methods, measures or technology pursuant to the requirements set forth in the Handbook;
- (8) require the Contractor to mandate that each of its subcontractors maintain the same levels of security required of the Contractor under any Port Authority awarded contract.
- (9) prohibit the publication, exchange or dissemination of PI developed from the project or contained in reports, except between Contractors and subcontractors, without prior approval of the Port Authority;
- (10) require that PI only be reproduced or copied pursuant to the requirements set forth in the Handbook.

- Audits for Compliance with Security Requirements

The Port Authority may conduct random or scheduled examinations of business practices under this section entitled "NOTIFICATION OF SECURITY REQUIREMENTS" and the Handbook in order to assess the extent of compliance with security requirements, Confidential Information procedures, protocols and practices, which may include, but not be limited to, verification of background check status, confirmation of completion of specified training, and/or a site visit to view material storage locations and protocols.

The Authority may impose, increase, and/or upgrade security requirements for the Contractor, subcontractors and their staffs during the term of this Contract to address changing security conditions and/or new governmental regulations.

16. INSURANCE PROCURED BY THE CONTRACTOR

The Contractor shall take out, maintain, and pay the premiums on Commercial General Liability Insurance, including but not limited to premises-operations, products-completed operations, deletion of the electronic data exclusion and independent contractors coverage, with contractual liability language covering the obligations assumed by the Contractor under this Contract and, if vehicles are to be used to carry out the performance of this Contract, then the Contractor shall also take out, maintain, and pay the premiums on Automobile Liability Insurance covering owned, non-owned, and hired autos in the following minimum limits:

Commercial General Liability Insurance - \$5 million combined single limit per occurrence for bodily injury and property damage liability.

Automobile Liability Insurance - \$ 5 million combined single limit per accident for bodily injury and property damage liability.

In addition, the liability policy (ies) shall name The Port Authority of New York and New Jersey, its related entities, the City of New York, Trends Urban Renewal Ltd., 4 World Trade Center LLC, 4 World Trade Center Holdings LLC, Silverstein Properties Inc., and other entities as required and their successors and assigns as additional insured, including but not limited to premise-operations, products-completed operations on the Commercial General Liability Policy. Moreover, the Commercial General Liability Policy shall not contain any provisions for exclusions from liability other than provisions for exclusion from liability forming part of the most up to date ISO form or its equivalent unendorsed Commercial General Liability Policy. The liability policy (ies) and certificate of insurance shall contain cross-liability language providing severability of interests so that coverage will respond as if separate policies were in force for each insured. Any and all excess and umbrella policies shall 'follow form' by conforming to the underlying policies. Furthermore, the Contractor's insurance shall be primary insurance as respects to the above additional insureds. Any insurance or self-insurance maintained by the above additional insureds shall not contribute to any loss or claim. These insurance requirements shall be in effect for the duration of the contract to include any warranty/guarantee period.

2/8/16

The certificate of insurance and liability policy (ies) must contain the following endorsement for the above liability coverages:

“The insurer(s) shall not, without obtaining the express advance written permission from the General Counsel of the Port Authority, raise any defense involving in any way the jurisdiction of the Tribunal over the person of the Port Authority, the immunity of the Port Authority, its Commissioners, officers, agents or employees, the governmental nature of the Port Authority, or the provisions of any statutes respecting suits against the Port Authority.”

Also, to the extent permitted by law, the Contractor and their subcontractors’ insurance policies and their certificate of insurance must contain a waiver of subrogation in favor of all the additional insured entities.

The Contractor shall also take out, maintain, and pay premiums on **Workers’ Compensation Insurance** in accordance with the requirements of law in the state(s) where work will take place, and Employer’s Liability Insurance with limits of not less than \$1 million each accident.

In addition, the policy (ies) and its certificate must be specifically endorsed to contain a provision that the policy may not be canceled, terminated, or modified without thirty (30) days’ prior written notice to the Port Authority of NY and NJ, Att: Facility Contract Administrator, at the location where the work will take place and to the General Manager, Risk Financing.

The Port Authority may at any time during the term of this agreement change or modify the limits and coverages of insurance. Should the modification or change results in an additional premium, The General Manager, Risk Financing for the Port Authority may consider such cost as an out-of-pocket expense.

Within five (5) days after the award of this agreement or contract and prior to the start of work, the Contractor must submit an original certificate of insurance, to the Port Authority of NY and NJ, Facility Contract Administrator, at the location where the work will take place. This certificate of insurance MUST show evidence of the above insurance policy (ies), stating the agreement/contract number prior to the start of work. The Contractor is also responsible for maintain and conforming to all insurance requirements from the landlords and their representatives. The General Manager, Risk Financing must approve the certificate(s) of insurance before any work can begin. Upon request by the Port Authority, the Contractor shall furnish to the General Manager, Risk Financing, a certified copy of each policy, including the premiums.

If at any time the above liability insurance should be canceled, terminated, or modified so that the insurance is not in effect as above required, then, if the Manager shall so direct, the Contractor shall suspend performance of the contract at the premises. If the contract is so suspended, no extension of time shall be due on account thereof. If the contract is not suspended (whether or not because of omission of the Manager to order suspension), then the Authority may, at its option, obtain insurance affording coverage equal to the above required, the cost of such insurance to be payable by the Contractor to the Port Authority.

2/8/16

Renewal certificates of insurance or policies shall be delivered to the Facility Contractor Administrator, Port Authority and to the landlord(s) at least fifteen (15) days prior to the expiration date of each expiring policy. The General Manager, Risk Financing must approve the renewal certificate(s) of insurance before work can resume on the facility. If at any time any of the certificates or policies shall become unsatisfactory to the Port Authority or to the landlord(s), the Contractor shall promptly obtain a new and satisfactory certificate and policy.

The requirements for insurance procured by the Contractor shall not in any way be construed as a limitation on the nature or extent of the contractual obligations assumed by the Contractor under this contract. The insurance requirements are not a representation by the Authority as to the adequacy of the insurance to protect the Contractor against the obligations imposed on them by law or by this or any other Contract. (CITS#4641N)

17. ASSIGNMENTS AND SUBCONTRACTS

Any assignment or other transfer by the Contractor of this Contract or any part hereof or of any of his rights hereunder or of any monies due or to become due hereunder and any delegation of any of his duties hereunder without the express written consent of the Director shall be void and of no effect as to the Authority, provided, however, that the Contractor may subcontract portions of the Work to such persons as the Director, may, from time to time, expressly approve in writing. For each individual, partnership or corporation proposed by the Contractor as a subcontractor, the Contractor shall submit to the Authority a certification or, if a certification cannot be made, a statement by such person, partnership or corporation to the same effect as the certification or statement required from the Contractor pursuant to the clauses of the "Integrity" Section entitled "Certification of No Investigation Indictment, Conviction, Debarment Suspension, Disqualification and Disclosure of Other Information and "Non-Collusive Bidding and Code of Ethics Certification; Certification of No Solicitation Based on Commission, Percentage, Brokerage Contingent or Other Fee". All further subcontracting by any subcontractor shall also be subject to such approval of the Director

No consent to any assignment or other transfer, and no approval of any subcontractor, shall under any circumstances operate to relieve the Contractor of any of his obligations; no subcontract, no approval of any subcontractor and no act or omission of the Authority or the Director shall create any rights in favor of such subcontractor and against the Authority; and as between the Authority and the Contractor, all assignees, subcontractors, and other transferees shall for all purposes be deemed to be agents of the Contractor. Moreover, all subcontractors and all approvals of subcontractors, regardless of their form, shall be deemed to be conditioned upon performance by the subcontractor in accordance with this Contract; and if any subcontractor shall fail to perform the Contract to the satisfaction of the Director, the Director shall have the absolute right to rescind his approval forthwith and to require the performance of the Contract by the Contractor personally or through other approved subcontractors.

18. CERTAIN CONTRACTOR'S WARRANTIES

The Contractor represents and warrants:

- A. That it is financially responsible and experienced in, and competent to perform this Contract; that no representation, promise or statement, oral or in writing, has induced it to submit its Proposal, saving only those contained in the papers expressly made part of this Contract; that the facts stated or shown in any papers submitted or referred to in connection with his Proposal are true; and, if the Contractor be a corporation, that it is authorized to perform this Contract;
- B. That it has carefully examined and analyzed the provisions and requirements of this Contract, that from its own investigations it has satisfied itself as to the nature of all things needed for the performance of this Contract, the general and local conditions and all other matters which in any way affect this Contract or its performance, and that the time available to it for such examination, analysis, inspection and investigations was adequate;
- C. That the Contract is feasible of performance in accordance with all its provisions and requirements and that it can and will perform it in strict accordance with such provisions and requirements;
- D. That no Commissioner, officer, agent or employee of the Authority is personally interested directly or indirectly in this Contract or the compensation to be paid hereunder;
- E. That, except only for those representations, statements or promises expressly contained in this Contract, no representation, statement or promise, oral or in writing, of any kind whatsoever by the Authority, its Commissioners, officers, agents, employees or consultants has induced the Contractor to enter into this Contract or has been relied upon by the Contractor, including any with reference to: (1) the meaning, correctness, suitability or completeness of any provisions or requirements of this Contract; (2) the nature, existence or location of materials, structures, obstructions, utilities or conditions, which may be encountered at the installation sites; (3) the nature, quantity, quality or size of the materials, equipment, labor and other facilities needed for the performance of this Contract; (4) the general or local conditions which may in any way affect this Contract or its performance; (5) the price of the Contract; or (6) any other matters, whether similar to or different from those referred to in (1) through (5) immediately above, affecting or having any connection with this Contract, the bidding thereon, any discussions thereof, the performance thereof or those employed therein or connected or concerned therewith.
- F. That, notwithstanding any requirements of this Contract, any inspection or approval of the Contractor's services by the Authority, or the existence of any patent or trade name, the Contractor nevertheless warrants and represents that the services and any intellectual property supplied to the Authority hereunder shall be of the best quality and shall be fully fit for the purpose for which they are to be used. The Contractor unconditionally guarantees against defects or failures of any kind, including defects or failures in design, workmanship and materials, excepting solely defects or failures which the Contractor demonstrates to the satisfaction of the Authority have arisen solely from accident, abuse or fault of the Authority occurring after issuance of Final Payment hereunder and not due to fault on the Contractor's part. In the event of defects or failures in said services, or any part thereof, then upon receipt of notice thereof from the Authority, the Contractor shall correct such defects or failures as may be necessary or desirable, in the sole opinion of the Authority, to comply with the above guaranty.

Moreover, the Contractor accepts the conditions at the sites of work as they may eventually be found to exist and warrants and represents that it can and will perform the Contract under such

conditions and that all materials, equipment, labor and other facilities required because of any unforeseen conditions (physical or otherwise) shall be wholly at its own cost and expense, anything in this Contract to the contrary notwithstanding.

Nothing in the Scope of Work or any other part of the Contract is intended as or shall constitute a representation by the Authority as to the feasibility of performance of this Contract or any part thereof. Moreover, the Authority does not warrant or represent either by issuance of the Scope of Work or by any provision of this Contract as to time for performance or completion or otherwise that the Contract may be performed or completed by the times required herein or by any other times.

The Contractor further represents and warrants that it was given ample opportunity and time and by means of this paragraph was requested by the Authority to review thoroughly all documents forming this Contract prior to execution of this Contract in order that it might request inclusion in this Contract of any statement, representation, promise or provision which it desired or on which it wished to place reliance; that it did so review said documents; that either every such statement, representation, promise or provision has been included in this Contract or else, if omitted, that it expressly relinquishes the benefit of any such omitted statement, representation, promise or provision and is willing to perform this Contract without claiming reliance thereon or making any other claim on account of such omission.

The Contractor further recognizes that the provisions of this clause (though not only such provisions) are essential to the Authority's consent to enter into this Contract and that without such provisions; the Authority would not have entered into this Contract.

19. RIGHTS AND REMEDIES OF THE AUTHORITY

The Authority shall have the following rights in the event the Director shall deem the Contractor guilty of a breach of any term whatsoever of this contract:

- a) The right to take over and complete the Work or any part thereof as agent for and at the expense of the Contractor, either directly or through other Contractors;
- b) The right to cancel this Contract as to any or all of the Work yet to be performed;
- c) The right to specific performance, an injunction or any other appropriate equitable remedy;
- d) The right to money damages.

For the purpose of this Contract, breach shall include but not be limited to the following, whether or not the time has yet arrived for performance of an obligation under this Contract: a statement by the Contractor to any representative of The Authority indicating that he cannot or will not perform any one or more of his obligations under this Contract; any act or omission of the Contractor or any other occurrence which makes it improbable at the time that he will be able to perform any one or more of his obligations under this Contract; any suspension of or failure to proceed with any part of the Work by the Contractor which makes it improbable at the time that he will be able to perform any one or more of his obligations under this Contract; any false certification at any time by the Contractor as to any material

item certified pursuant to the clauses hereof entitled "Certification of No Investigation (Criminal or Civil Anti-Trust), Indictment, Conviction, Debarment, Suspension, Disqualification and Disclosure of Other Required Information" and "Non-Collusive Bidding and Code of Ethics Certification; Certification of No Solicitation Based on Commission, Percentage, Brokerage, Contingent or Other Fee", or the willful or fraudulent submission of any signed statement pursuant to such clauses which is false in any material respect; or the Contractor's incomplete or inaccurate representation of its status with respect to the circumstances provided for in such clauses.

The enumeration in this numbered clause or elsewhere in this Contract of specific rights and remedies of The Authority shall not be deemed to limit any other rights or remedies which The Authority would have in the absence of such enumeration; and no exercise by The Authority of any right or remedy shall operate as a waiver of any other of its rights or remedies not inconsistent therewith or to stop it from exercising such other rights or remedies.

Neither the acceptance of the work or any part thereof, nor any payment therefor, nor any order or certificate issued under this Agreement or otherwise issued by the Authority, or any officer, agent or employee of the Authority, nor any permission or direction to continue with the performance or work, nor any performance by the authority of any of the Contractor's duties or obligations, nor any aid provided to the Contractor by the Authority in his performance of such duties or obligations, nor any other thing done or omitted to be done by the Authority, its Commissioners, officers, agents or employees shall be deemed to be a waiver of any provision of this agreement or of any rights or remedies to which the Authority may be entitled because of any breach hereof, excepting only a resolution of its Commissioners, providing expressly for such waiver. No cancellation, rescission or annulment hereof, in whole or as to any part of the work, because of any breach hereof, shall be deemed a waiver of any money damages to which the Authority may be entitled because of such breach. Moreover, no waiver by the Authority of any breach of this Agreement shall be deemed to be a waiver of any other or any subsequent breach.

20. RIGHTS AND REMEDIES OF THE CONTRACTOR

Inasmuch as the Contractor can be adequately compensated by money damages for any breach of this Contract which may be committed by the Authority, the Contractor expressly agrees that no default, act or omission of the Authority shall constitute a material breach of this Contract, entitling him to cancel or rescind it or (unless the Director shall so direct) to suspend or abandon performance.

21. TAX EXEMPTIONS

Purchases of services and tangible personal property by the Port Authority are exempt from New York and New Jersey state and local sales and compensating use taxes. (Sales Taxes). Therefore, the Port Authority's purchase of the Contractor's services under this Contract is exempt from Sales Taxes. Accordingly, the Contractor must not include Sales Taxes in the price charged to the Port Authority for the contractor's services under this Contract.

22. TITLE TO EQUIPMENT

Title to all equipment to be furnished hereunder by the Contractor shall be transferred to the Authority upon its delivery to the installation site.

The Contractor shall furnish such bills of sale and affidavits of title as the Authority shall reasonably request.

23. NOTICE REQUIREMENTS

No claim against the Authority shall be made or asserted in any action or proceeding at law or in equity, and the Contractor shall not be entitled to allowance of such claim, unless the Contractor shall have complied with all requirements relating to the giving of written notice and of information with respect to such claim as provided in this clause. The failure of the Contractor to give such written notice and information as to any claim shall be conclusively deemed to be a waiver by the Contractor of such claim, such written notice and information being conditions precedent to such claim. As used herein "claim" shall include any claim arising out of this agreement (including claims in the nature of breach of contract or fraud or misrepresentation before or subsequent to execution of this Agreement and claims of a type which are barred by the provisions of this agreement) for damages, payment or compensation of any nature or for performance of any part of this Agreement.

The requirements as to the giving of written notice and information with respect to claims shall be as follows:

- A. In the case of any claims for which requirements are set forth elsewhere in this Agreement as to notice and information, such requirements shall apply.
- B. In the case of all other types of claims, notice shall have been given to the Director, as soon as practicable, and in any case within forty eight (48) hours after occurrence of the act, omission, or other circumstances upon which the claim is or will be based, stating as fully as practicable at the time all information relating thereto. Such information shall be supplemented with any further information as soon as practicable after it becomes or should become known to the Contractor, including daily records showing all costs which the Contractor may be incurring or all other circumstances which will affect any claim to be made which records shall be submitted to the Authority.

The above requirements for notices and information are for the purpose of enabling the Authority to avoid waste of public funds by affording it promptly the opportunity to cancel or revise any order, change its plans, mitigate or remedy the effects of circumstances giving rise to a claim or take such other action as may seem desirable and to verify any claimed expense or circumstance as they occur and the requirements herein for such notice and information are essential to this Agreement and are in addition to any notice required by statute with respect to suits against the Authority.

The above referred to notices and information are required whether or not the Authority is aware of the existence of any circumstances which might constitute a basis for a claim and whether or not the Authority has indicated it will consider a claim.

No, act, omission or statement of any kind shall be regarded as a waiver of any of the provisions of this clause or may be relied upon as such waiver except only either a written statement signed by the Executive Director of the Authority or a resolution of the Commissioners of the Authority expressly stating that a waiver is intended as to any particular provision of this clause, and more particularly, no discussion, negotiation, consideration, correspondence or requests for information with respect to a claim by any Commissioner, officer, employees or agent of the Authority shall be construed as a waiver of any provision of this clause or as authority or apparent authority to effect such a waiver.

Since merely oral notice or information may cause disputes as to the existence or substance thereof, and since notice, even if written, to other than the Authority representative above designated to receive it may not be sufficient to come to the attention of the representative of the Authority with the knowledge and responsibility of dealing with the situation, only notice and information complying with the express provisions of this clause shall be deemed to fulfill the Contractor's obligation under this Agreement.

24. SERVICE OF NOTICES ON THE CONTRACTOR

Whenever provision is made in this Contract for the giving of any notice to the Contractor, its deposit in any post office box, enclosed in a postpaid wrapper addressed to the Contractor at his/her office, or its delivery to his/her office, shall be sufficient service thereof as of the date of such deposit or delivery, except to the extent, if any, otherwise provided in the clause entitled "Submission to Jurisdiction". Until further notice to the Authority the Contractor's office will be that stated in his/her Proposal. Notices may also be served personally upon the Contractor; or if a corporation, upon any officer, director or managing or general agent; or if a partnership upon any partner.

25. NO THIRD PARTY RIGHTS

Nothing contained in this Agreement is intended for the benefit of third persons, except to the extent that the Agreement specifically provides otherwise by use of the words "benefit" or "direct right of action".

26. INDEMNIFICATION AND RISKS ASSUMED BY THE CONTRACTOR

To the extent permitted by law, the Contractor shall indemnify and hold harmless the Port Authority, its Commissioners, officers, representatives and employees from and against all claims and demands, just or unjust, of third persons (including Contractor's employees, employees, officers, and agents of the Port Authority) arising out of or in any way connected or alleged to arise out of or alleged to be in any way connected with the Contract and all other services and activities of the Contractor under this Contract and for all expenses incurred by it and by them in the defense, settlement or satisfaction thereof, including without limitation thereto, claims and demands for death, for personal injury or for property damage, direct or consequential, whether they arise from the acts or omissions of the Contractor, the Port Authority, third persons (including Contractor's employees, employees, officers, and agents of the Port Authority), or from the acts of God or the public enemy, or otherwise, including claims and demands of any local jurisdiction against the Port Authority in connection with this Contract.

2/8/16

The Contractor assumes the following risks, whether such risks arise from acts or omissions (negligent or not) of the Contractor, the Port Authority or third persons (including Contractor's employees, employees, officers, and agents of the Port Authority) or from any other cause, excepting only risks occasioned solely by affirmative willful acts of the Port Authority done subsequent to the opening of proposals on this Contract, and shall to the extent permitted by law indemnify the Port Authority for all loss or damage incurred in connection with such risks:

- a. The risk of any and all loss or damage to Port Authority property, equipment (including but not limited to automotive and/or mobile equipment), materials and possessions, on or off the premises, the loss or damage of which shall arise out of the Contractor's operations hereunder. The Contractor shall if so directed by the Port Authority, repair, replace or rebuild to the satisfaction of the Port Authority, any and all parts of the premises or the Facility which may be damaged or destroyed by the acts or omissions of the Contractor, its officers, agents, or employees and if the Contractor shall fail so to repair, replace, or rebuild with due diligence the Port Authority may, at its option, perform any of the foregoing work and the Contractor shall pay to the Port Authority the cost thereof.
- b. The risk of any and all loss or damage of the Contractor's property, equipment (including but not limited to automotive and/or mobile equipment) materials and possessions on the Facility.
- c. The risk of claim, whether made against the Contractor or the Port Authority, for any and all loss or damages occurring to any property, equipment (including but not limited to automotive and/or mobile equipment), materials and possessions of the Contractor's agents, employees, materialmen and others performing work hereunder.
- d. The risk of claims for injuries, damage or loss of any kind just or unjust of third persons arising or alleged to arise out of the performance of work hereunder, whether such claims are made against the Contractor or the Port Authority.

If so directed, the Contractor shall at its own expense defend any suit based upon any such claim or demand, even if such suit, claim or demand is groundless, false or fraudulent, and in handling such shall not, without obtaining express advance permission from the General Counsel of the Port Authority, raise any defense involving in any way the jurisdiction of the tribunal over the person of the Port Authority, the immunity of the Port Authority, its Commissioners, officers, agents or employees, the governmental nature of the Port Authority or the provision of any statutes respecting suits against the Port Authority.

Neither the requirements of the Port Authority under this Contract, nor of the Port Authority of the methods of performance hereunder nor the failure of the Port Authority to call attention to improper or inadequate methods or to require a change in the method of performance hereunder nor the failure of the Port Authority to direct the Contractor to take any particular precaution or other action or to refrain from doing any particular thing shall relieve the Contractor of its liability for injuries to persons or damage to property or environmental impairment arising out of its operations.

27. APPROVAL OF METHODS

Neither the approval of the Port Authority of the methods of furnishing services hereunder nor the failure of the Port Authority to call attention to improper or inadequate methods or to require a change in the method of furnishing services hereunder, nor the failure of the Port Authority to direct the Contractor to take any particular precautions or to refrain from doing any particular thing shall relieve the Contractor of its liability for injuries to persons or damage to property or environmental impairment arising out of its operations.

28. PORT AUTHORITY TECHNOLOGY STANDARDS AND GUIDELINES AND SUPPLEMENTAL GUIDELINES FOR THE PORT AUTHORITY TECHNOLOGY SERVICES DEPARTMENT

The Contractor and any subcontractors shall follow the Port Authority Technology Standard and Guidelines and the Supplemental Guidelines for the Port Authority Technology Services Department attached hereto and made a part hereof, and shall comply with any updates to or changes in best practices related to such Standards and Guidelines.

29. PORT AUTHORITY AUDIT DEPARTMENT CONTROLS REQUIREMENT CONTRACT CHECKLIST

The Contractor and any subcontractors shall follow the Audit Department Controls Requirement Contract Checklist attached hereto and made a part hereof, and shall comply with any updates to or changes in best practices related to such requirements.

30. SSAE 16 COMPLIANCE AND REPORTING

Contractor agreed to produce an "Independent Service Auditor's Report on a Description of Service Organization's System and the Suitability of Design of Controls" in accordance with the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements No 16 (SSAE 16). The scope of the SSAE 16 audit report will include services such as those provided within this contract and are reasonably expected within the industry, and as mutually agreed to by the two parties. The Contractor further agrees to maintain, SSAE 16 SOC 2 Type II, or similar certification for the duration of Agreement. The copy of the report and subsequent updates shall be submitted to the Authority throughout the term of this contract within 4 months following each report's audit period close date, confirming compliance. Contractor agrees to remain "SSAE 16 Compliant" throughout the term of its contract with the Authority at no additional cost. This should also include all datacenters where the Authority's data may be stored or transmitted. The Contractor agrees to include the Authority in the sample tested by the independent auditor.

Further the Contractor has agreed that each month beyond the 4th month following such audit period closing date that the SSAE 16 compliance report is not submitted will result in liquidated damages of \$5,000 per month until the report is received by the Authority.

31. SUBMISSION TO JURISDICTION

The Contractor hereby irrevocably submits itself to the jurisdiction of the Courts of the State of New York and New Jersey, in regard to any controversy arising out of, connected with, or in any way concerning this Contract.

The Contractor agrees that the service of process on the Contractor in relation to such jurisdiction may be made, at the option of the Port Authority, either by registered or certified mail addressed to it at the address of the Contractor indicated on the signature sheet, or by actual personal delivery to the Contractor, if the Contractor is an individual, to any partner if the Contractor be a partnership or to any officer, director or managing or general agent if the Contractor be a corporation.

Such service shall be deemed to be sufficient when jurisdiction would not lie because of the lack of basis to serve process in the manner otherwise provided by law. In any case, however, process may be served as stated above whether or not it might otherwise have been served in a different manner.

32. APPLICABLE LAW

This Contract shall be construed in accordance with the laws of the State of New York. The Contractor hereby consents to the exercise by the courts of the States of New York and New Jersey of jurisdiction in personam over it with respect to any matter arising out of or in connection with this Contract and waives any objection to such jurisdiction which it might otherwise have; and the Contractor agrees that mailing of process by registered mail addressed to it at the address of the Contractor set forth in the Proposal, shall have the same effect as personal service within the States of New York or New Jersey upon a domestic corporation of said State.

33. AUTHORITY OF THE DIRECTOR

Inasmuch as the public interest requires that the Project to which this Contract relates shall be performed in the manner which the Authority, acting through the Director deems best, the Director shall have absolute authority to determine what is or is not necessary or proper for or incidental thereto and the Specifications shall be deemed merely the Director's present determination on this point. In the exercise of this authority, the Director shall have power to alter the Specifications, to require the performance of Work not required by them in their present form, even though of a totally different character from that not required, and to vary, increase and diminish the character, quantity and quality of, or to countermand any Work now or hereafter required. If at any time it shall be, from the viewpoint of the Authority, impracticable or undesirable in the judgment of the Director to proceed with or continue the performance of the Contract or any part thereof, whether or not for reasons beyond the control of the Authority, the Director shall have authority to suspend performance of any part or all of the Contract until such time as the Director may deem it practicable or desirable to proceed. Moreover, if at any time it shall be, from the viewpoint of the Authority impracticable or undesirable in the judgment of the Director to proceed with or continue the performance of the Contract or any part thereof for reasons within or beyond the control of the Authority, the Director shall have authority to cancel this Contract as to any or all portions not yet performed and as to any materials not yet installed even though delivered. Such cancellation shall be without prejudice to the rights and obligations of the

parties arising out of portions already satisfactorily performed, but no allowance shall be made for anticipated profits. To resolve all disputes and to prevent litigation, the parties to this Contract authorize the Director to decide all questions of any nature whatsoever arising out of, under, or in connection with, or in any way related to or on account of, this Contract (including claims in the nature of breach of contract or fraud or misrepresentation before or subsequent to acceptance of the Contractor's Proposal and claims of a type which are barred by the provisions of this Contract) and such decision shall be conclusive, final and binding on the parties. The Director's decision may be based on such assistance as she may find desirable. The effect of the decision shall not be impaired or waived by any negotiation or settlement offers in connection with the question decided, whether or not she participated therein, or by any prior decision of her or others, which prior decisions shall be deemed subject to review, or by any termination or cancellation of this Contract.

All such questions shall be submitted in writing by the Contractor to the Director for a decision together with all evidence and other pertinent information in regard to such questions, in order that a fair and impartial decision may be made. In any action against the Authority relating to any such question the Contractor must allege in the complaint and prove such submission, which shall be a condition precedent to any such action. No evidence or information shall be introduced or relied upon in such an action that has not been so presented to the Director.

In the performance of the Contract, the Contractor shall conform to all orders, directions and requirements of the Director and shall perform the Contract to her satisfaction at such times and places, by such methods and such manner and sequence as she may require, and the Contract shall at all stages be subject to her inspection. The Contractor shall employ no equipment, materials, methods or men to which she objects, and shall remove no materials, equipment or other facilities from the Authority site without permission. Upon request, she shall confirm in writing any oral order, direction, requirements or determination.

The enumeration herein or elsewhere of particular instances in which the opinion, judgment, discretion or determination of the Director shall control or in which the Contract shall be performed to her satisfaction or subject to her inspection, shall not imply that only the matters of a nature similar to those enumerated shall be so governed and performed, but without exception the entire Contract shall be so governed and performed.

This provision shall be construed in accordance with the laws of the State of New York excluding its conflict of law provisions.

34. APPROVALS BY THE DIRECTOR

The approval by the Director of any service required hereunder, shall be construed merely to mean that at that time the Director knows of no good reason for objecting thereto and no such approval shall release the Contractor from its full responsibility for the satisfactory performance of the services to be supplied. "Approved equal" shall mean approved by the Director.

35. CONTRACT REVIEW AND COMPLIANCE AUDITS

The Contractor, and any subcontractors, shall provide system access and reasonable assistance to the Authority's External and Internal Audit staff or its consultants in their performance of work under the contract, including producing specific requested information, extraction of data and reports. The Contractor, and any subcontractors, shall support requests related to audits of the agreement and administration tasks and functions covered by this Contract.

The Authority reserves the right to use and load security and system software to evaluate the level of security and vulnerabilities in all systems which control, collect, dispense, contain, manage, administer, or monitor revenue "owned" by the Port Authority.

The Authority reserves the right to use as required and load security and system software to evaluate the level of security and vulnerabilities in any applicable environment-covered under this Contract. If such right is exercised, then both parties shall work in good faith to ensure there is no access or potential access to third party proprietary data within the applicable environment or access to other systems not covered under this Contract.

36. AUTHORITY ACCESS TO RECORDS

The Authority shall have access during normal business hours to all records and documents of the Contractor relating to any service provided under this Agreement, amounts for which it has been compensated, or claims he should be compensated, by The Authority above those included in the lump sum compensation set forth elsewhere herein. All Contractor records shall be kept in the Port District. The Contractor shall obtain for The Authority similar access to similar records and documents of subcontractors. Such access shall be given or obtained both before and within a period of three (3) years after Final Payment to the Contractor, provided, however, that if within the aforesaid one year period The Authority has notified the Contractor in writing of a pending claim by The Authority under or in connection with this Contract to which any of the aforesaid records and documents of the Contractor or of his subcontractors relate either directly or indirectly, then the period of such right of access shall be extended to the expiration of six (6) years from the date of Final Payment with respect to the records and documents involved.

Upon request of the Port Authority, the Contractor shall furnish or provide access to the federal Form I-9 (Employment Eligibility Verification) for each individual performing work under this Contract. This includes citizens and noncitizens.

The Contractor shall provide, at no cost to the Authority, access for and reasonable assistance to such auditors from the Authority or the Authority's external auditors that may, from time to time, be designated to audit detail records which support Contractor charges to the Authority. The Authority shall have access to the detail records that support Contractor charges to the Authority for up to three (3) years following the termination of the Contract.

No provision in this Contract giving The Authority a right of access to records and documents is intended to impair or affect any right of access to records and documents that The Authority would have in the absence of such provision.

37. HARMONY

- a. The Contractor shall not employ any persons or use any labor, or use or have any equipment, or permit any condition to exist which shall or may cause or be conducive to any labor complaints, troubles, disputes or controversies at the Facility which interfere or are likely to interfere with the operation of the Port Authority or with the operations of lessees, licensees or other users of the Facility or with the operations of the Contractor under this Contract.

The Contractor shall immediately give notice to the Port Authority (to be followed by written notices and reports) of any and all impending or existing labor complaints, troubles, disputes or controversies and the progress thereof. The Contractor shall use its best efforts to resolve any such complaint, trouble, dispute or controversy. If any type of strike, boycott, picketing, work stoppage, slowdown or other labor activity is directed against the Contractor at the Facility or against any operations of the Contractor under this Contract, whether or not caused by the employees of the Contractor, and if any of the foregoing, in the opinion of the Port Authority, results or is likely to result in any curtailment or diminution of the services to be performed hereunder or to interfere with or affect the operations of the Port Authority, or to interfere with or affect the operations of lessees, licensees, or other users of the Facility or in the event of any other cessation or stoppage of operations by the Contractor hereunder for any reason whatsoever, the Port Authority shall have the right at any time during the continuance thereof to suspend the operations of the Contractor under this Contract, and during the period of the suspension the Contractor shall not perform its services hereunder and the Port Authority shall have the right during said period to itself or by any third person or persons selected by it to perform said services of the Contractor using the equipment which is used by the Contractor in its operations hereunder as the Port Authority deems necessary and without cost to the Port Authority. During such time of suspension, the Contractor shall not be entitled to any compensation. Any flat fees, including management fees, shall be prorated. Prior to the exercise of such right by the Port Authority, it shall give the Contractor notice thereof, which notice may be oral. No exercise by the Port Authority of the rights granted to it in the above subparagraph shall be or be deemed to be a waiver of any rights of termination or revocation contained in this Contract or a waiver of any rights or remedies which may be available to the Port Authority under this Contract or otherwise.

- b. During the time that the Contractor is performing the Contract, other persons may be engaged in other operations on or about the worksite including Facility operations, pedestrian, bus and vehicular traffic and other Contractors performing at the worksite, all of which shall remain uninterrupted.

The Contractor shall so plan and conduct its operations as to work in harmony with others engaged at the site and not to delay, endanger or interfere with the operation of others (whether or not specifically mentioned above), all to the best interests of the Port Authority and the public as may be directed by the Port Authority.

38. CLAIMS OF THIRD PERSONS

The Contractor undertakes to pay all claims lawfully made against him by subcontractors, materialmen and workmen, and all claims lawfully made against him by other third persons arising out of or in connection with or because of the performance of this Contract and to cause all subcontractors to pay all such claims lawfully made against them.

39. NON-DISCRIMINATION REQUIREMENTS

The Contractor shall take all necessary and reasonable steps to ensure non-discrimination in the performance and administration of all aspects of this Contract.

- A. Contractor hereby agrees that no person on the ground of race, color, national origin, creed/religion, sex, age or handicap/disability shall be excluded from participation in, denied the benefits of, or be otherwise subjected to discrimination in the furnishing of goods or services or in the selection and retention of subcontractors and/or vendors under this Contract. Contractor shall also ascertain and comply with all applicable federal, state and local laws, ordinances, rules, regulations, and orders that pertain to equal employment opportunity, affirmative action, and non-discrimination in employment.
- B. Contractor agrees that these “Non-Discrimination Requirements” are a binding part of this Contract. Without limiting the generality of any other term or provision of this Contract, in the event the Authority, or a state or federal agency finds that the Contractor or any of its subcontractors or vendors has not complied with these “Non-Discrimination Requirements”, the Authority may cancel, terminate or suspend this Contract in accordance with Section 11 of these Terms and Conditions entitled “Default, Revocation, or Suspension of Contract.”
- C. Contractor agrees to cooperate fully with the Authority’s investigation of allegations of discrimination. Cooperation includes, but is not limited to, allowing the Authority to question employees during the investigation of allegations of discrimination, and complying with directives that the Authority or the State or Federal government deem essential to ensure compliance with these “Non-Discrimination Requirements.”

40. CONTRACTOR’S INTEGRITY PROVISIONS

1. Certification of No Investigation (criminal or civil anti-trust), Indictment, Conviction, Debarment, Suspension, Disqualification and Disclosure of Other Information

By bidding on this Contract, each Bidder and each person signing on behalf of any Bidder certifies, and in the case of a joint bid each party thereto certifies as to its own organization, that the Bidder and each parent and/or affiliate of the Bidder has not

- a. been indicted or convicted in any jurisdiction;
- b. been suspended, debarred, found not responsible or otherwise disqualified from entering into any contract with any governmental agency or been denied a government contract for failure to meet standards related to the integrity of the Bidder;

- c. had a contract terminated by any governmental agency for breach of contract or for any cause based in whole or in part on an indictment or conviction;
- d. ever used a name, trade name or abbreviated name, or an Employer Identification Number different from those inserted in the Bid;
- e. had any business or professional license suspended or revoked or, within the five years prior to bid opening, had any sanction imposed in excess of fifty thousand dollars (\$50,000) as a result of any judicial or administrative proceeding with respect to any license held or with respect to any violation of a federal, state or local environmental law, rule or regulation;
- f. had any sanction imposed as a result of a judicial or administrative proceeding related to fraud, extortion, bribery, bid rigging, embezzlement, misrepresentation or anti-trust regardless of the dollar amount of the sanctions or the date of their imposition; and
- g. been, and is not currently, the subject of a criminal investigation by any federal, state or local prosecuting or investigative agency and/or a civil anti-trust investigation by any federal, state or local prosecuting or investigative agency, including an inspector general of a governmental agency or public authority.

2. Non-Collusive Bidding, and Code of Ethics Certification, Certification of No Solicitation Based On Commission, Percentage, Brokerage, Contingent or Other Fees

By bidding on this Contract, each Bidder and each person signing on behalf of any Bidder certifies, and in the case of a joint bid, each party thereto certifies as to its own organization, that

- a. the prices in its bid have been arrived at independently without collusion, consultation, communication or agreement for the purpose of restricting competition, as to any matter relating to such prices with any other bidder or with any competitor;
- b. the prices quoted in its bid have not been and will not be knowingly disclosed directly or indirectly by the Bidder prior to the official opening of such bid to any other bidder or to any competitor;
- c. no attempt has been made and none will be made by the Bidder to induce any other person, partnership or corporation to submit or not to submit a bid for the purpose of restricting competition;
- d. this organization has not made any offers or agreements or taken any other action with respect to any Authority employee or former employee or immediate family member of either which would constitute a breach of ethical standards under the Code of Ethics dated March 11, 2014, or as may be revised, (a copy of which is available upon request) nor does this organization have any knowledge of any act on the part of an Authority employee or former Authority employee relating either directly or indirectly to this organization which constitutes a breach of the ethical standards set forth in said Code;
- e. no person or selling agency other than a bona fide employee or bona fide established

commercial or selling agency maintained by the Bidder for the purpose of securing business, has been employed or retained by the Bidder to solicit or secure this Contract on the understanding that a commission, percentage, brokerage, contingent, or other fee would be paid to such person or selling agency; and

- f. the Bidder has not offered, promised or given, demanded or accepted, any undue advantage, directly or indirectly, to or from a public official or employee, political candidate, party or party official, or any private sector employee (including a person who directs or works for a private sector enterprise in any capacity), in order to obtain, retain, or direct business or to secure any other improper advantage in connection with this Contract.
- g. no person or organization has been retained, employed or designated on behalf of the Bidder to impact any Port Authority determination with respect to (i) the solicitation, evaluation or award of this Contract, or (ii) the preparation of specifications or request for submissions in connection with this Contract.

The foregoing certifications in 40 (1) and 40 (2) above, shall be deemed to have been made by the Bidder as follows:

- * if the Bidder is a corporation, such certification shall be deemed to have been made not only with respect to the Bidder itself, but also with respect to each parent, affiliate, director, and officer of the Bidder, as well as, to the best of the certifier's knowledge and belief, each stockholder of the Bidder with an ownership interest in excess of 10%;
- * if the Bidder is a partnership, such certification shall be deemed to have been made not only with respect to the Bidder itself, but also with respect to each partner.

Moreover, the foregoing certifications, if made by a corporate Bidder, shall be deemed to have been authorized by the Board of Directors of the Bidder, and such authorization shall be deemed to include the signing and submission of the bid and the inclusion therein of such certification as the act and deed of the corporation.

In any case where the Bidder cannot make the foregoing certifications, the Bidder shall so state and shall furnish with the signed bid a signed statement which sets forth in detail the reasons therefor. If the Bidder is uncertain as to whether it can make the foregoing certifications, it shall so indicate in a signed statement furnished with its bid, setting forth in such statement the reasons for its uncertainty. With respect to the foregoing certification in paragraph "2g", if the Bidder cannot make the certification, it shall provide, in writing, with the signed bid: (i) a list of the name(s), address(es), telephone number(s), and place(s) of principal employment of each such individual or organization; and (ii) a statement as to whether such individual or organization has a "financial interest" in this Contract, as described in the Procurement Disclosure Policy of the Authority (a copy of which is available upon request to the Chief Procurement Officer of the Procurement Department of the Authority). Such disclosure is to be updated, as necessary, up to the time of award of this Contract. As a result of such disclosure, the Port Authority shall take appropriate action up to and including a finding of non-responsibility.

Failure to make the required disclosures shall lead to administrative actions up to and including a finding of non-responsiveness or non-responsibility.

Notwithstanding that the Bidder may be able to make the foregoing certifications at the time the bid is submitted, the Bidder shall immediately notify the Authority in writing during the period of irrevocability of bids and the term of the Contract, if Bidder is awarded the Contract, of any change of circumstances which might under this clause make it unable to make the foregoing certifications, might render any portion of the certifications previously made invalid, or require disclosure. The foregoing certifications or signed statement shall be deemed to have been made by the Bidder with full knowledge that they would become a part of the records of the Authority and that the Authority will rely on their truth and accuracy in awarding and continuing this Contract. In the event that the Authority should determine at any time prior or subsequent to the award of this Contract that the Bidder has falsely certified as to any material item in the foregoing certifications, has failed to immediately notify the Port Authority of any change in circumstances which might make it unable to make the foregoing certifications, might render any portion of the certifications previously made invalid, or require disclosure, or has willfully or fraudulently furnished a signed statement which is false in any material respect, or has not fully and accurately represented any circumstance with respect to any item in the foregoing certifications required to be disclosed, the Authority may determine that the Bidder is not a responsible Bidder with respect to its bid on the Contract or with respect to future bids on Authority contracts and may exercise such other remedies as are provided to it by the Contract with respect to these matters. In addition, Bidders are advised that knowingly providing a false certification or statement pursuant hereto may be the basis for prosecution for offering a false instrument for filing (see e.g. New York Penal Law, Section 175.30 et seq.). Bidders are also advised that the inability to make such certification will not in and of itself disqualify a Bidder, and that in each instance the Authority will evaluate the reasons therefor provided by the Bidder. Under certain circumstances the Bidder may be required as a condition of Contract award to enter into a Monitoring Agreement under which it will be required to take certain specified actions, including compensating an independent Monitor to be selected by the Port Authority, said Monitor to be charged with, among other things, auditing the actions of the Bidder to determine whether its business practices and relationships indicate a level of integrity sufficient to permit it to continue business with the Port Authority.

3. Bidder Eligibility for Award of Contracts - Determination by an Agency of the State of New York or New Jersey Concerning Eligibility to Receive Public Contracts

Bidders are advised that the Authority has adopted a policy to the effect that in awarding its contracts it will honor any determination by an agency of the State of New York or New Jersey that a Bidder is not eligible to bid on or be awarded public contracts because the Bidder has been determined to have engaged in illegal or dishonest conduct or to have violated prevailing rate of wage legislation.

The policy permits a Bidder whose ineligibility has been so determined by an agency of the State of New York or New Jersey to submit a bid on a Port Authority contract and then to establish that it is eligible to be awarded a contract on which it has bid because (i) the state agency determination relied upon does not apply to the Bidder, or (ii) the state agency determination relied upon was made without affording the Bidder the notice and hearing to which the Bidder was entitled by the requirements of due process

2/8/16

of law, or (iii) the state agency determination was clearly erroneous or (iv) the state determination relied upon was not based on a finding of conduct demonstrating a lack of integrity or violation of a prevailing rate of wage law.

The full text of the resolution adopting the policy may be found in the Minutes of the Authority's Board of Commissioners meeting of September 9, 1993.

4. Contractor Responsibility, Suspension of Work and Termination

During the term of this Contract, the Contractor shall at all times during the Contract term remain responsible. The Contractor agrees, if requested by the Port Authority to present evidence of its continuing legal authority to do business in the States of New Jersey or New York, integrity, experience, ability, prior performance, and organizational and financial capacity.

The Port Authority, in its sole discretion, reserves the right to suspend any or all activities under this Contract, at any time, when it discovers information that calls into question the responsibility of the Contractor. In the event of such suspension, the Contractor will be given written notice outlining the particulars of such suspension. Upon issuance of such notice, the Contractor must comply with the terms of the suspension order. Contract activity may resume at such time as the Port Authority issues a written notice authorizing a resumption of performance under the Contract.

Upon written notice to the Contractor, and an opportunity to be heard with appropriate Port Authority officials or staff, the Contract may be terminated by Port Authority at the Contractor's expense where the Contractor is determined by the Port Authority to be non-responsible. In such event, the Port Authority or its designee may complete the contractual requirements in any manner he or she may deem advisable and pursue available legal or equitable remedies for breach, including recovery of costs from Contractor associated with such termination.

5. No Gifts, Gratuities, Offers of Employment, Etc.

At all times, the Contractor shall not offer, give or agree to give anything of value either to a Port Authority employee, agent, job shopper, consultant, construction manager or other person or firm representing the Port Authority, or to a member of the immediate family (i.e., a spouse, child, parent, brother or sister) of any of the foregoing, in connection with the performance by such employee, agent, job shopper, consultant, construction manager or other person or firm representing the Port Authority of duties involving transactions with the Contractor on behalf of the Port Authority, whether or not such duties are related to this Contract or any other Port Authority contract or matter. Any such conduct shall be deemed a material breach of this Contract.

As used herein "anything of value" shall include but not be limited to any (a) favors, such as meals, entertainment, transportation (other than that contemplated by the Contract or any other Port Authority contract), etc. which might tend to obligate the Port Authority employee to the Contractor, and (b) gift, gratuity, money, goods, equipment, services, lodging, discounts not available to the general public, offers or promises of employment, loans or the cancellation thereof, preferential treatment or business opportunity. Such term shall not include compensation contemplated by this Contract or any other Port Authority contract. Where used herein, the term "Port Authority" shall be deemed to include

2/8/16

all subsidiaries of the Port Authority.

The Contractor shall insure that no gratuities of any kind or nature whatsoever shall be solicited or accepted by it and by its personnel for any reason whatsoever from the passengers, tenants, customers or other persons using the Facility and shall so instruct its personnel.

In the event that the Contractor becomes aware of the occurrence of any conduct that is prohibited by this section entitled "No Gifts, Gratuities, Offers of Employment, Etc.", it shall report such occurrence to the Port Authority's Office of Inspector General within three (3) business days of obtaining such knowledge. (See "<http://www.panynj.gov/inspector-general>" for information about to report information to the Office of Inspector General). Failing to report such conduct shall be grounds for a finding of non-responsibility.

In addition, during the term of this Contract, the Contractor shall not make an offer of employment or use confidential information in a manner proscribed by the Code of Ethics and Financial Disclosure dated March 11, 2014, or as may be revised (a copy of which is available upon request to the Office of the Secretary of the Port Authority).

The Contractor shall include the provisions of this clause in each subcontract entered into under this Contract.

6. Conflict of Interest

During the term of this Contract, the Contractor shall not participate in any way in the preparation, negotiation or award of any contract (other than a contract for its own services to the Authority) to which it is contemplated the Port Authority may become a party, or participate in any way in the review or resolution of a claim in connection with such a contract if the Contractor has a substantial financial interest in the contractor or potential contractor of the Port Authority or if the Contractor has an arrangement for future employment or for any other business relationship with said contractor or potential contractor, nor shall the Contractor at any time take any other action which might be viewed as or give the appearance of conflict of interest on its part. If the possibility of such an arrangement for future employment or for another business arrangement has been or is the subject of a previous or current discussion, or if the Contractor has reason to believe such an arrangement may be the subject of future discussion, or if the Contractor has any financial interest, substantial or not, in a contractor or potential contractor of the Authority, and the Contractor's participation in the preparation, negotiation or award of any contract with such a contractor or the review or resolution of a claim in connection with such a contract is contemplated or if the Contractor has reason to believe that any other situation exists which might be viewed as or give the appearance of a conflict of interest, the Contractor shall immediately inform the Chief Procurement Officer in writing of such situation giving the full details thereof. Unless the Contractor receives the specific written approval of the Chief Procurement Officer, the Contractor shall not take the contemplated action which might be viewed as or give the appearance of a conflict of interest. The Chief Procurement Officer may require the Contractor to submit a mitigation plan addressing and mitigating any disclosed or undisclosed conflict, which is subject to the approval of the Chief Procurement Officer and shall become a requirement, as though fully set forth in this Contract. In the event the Chief Procurement Officer shall determine that the performance by the

Contractor of a portion of its Services under this Agreement is precluded by the provisions of this numbered paragraph, or a portion of the Contractor's said Services is determined by the Chief Procurement Officer to be no longer appropriate because of such preclusion, then the Chief Procurement Officer shall have full authority on behalf of both parties to order that such portion of the Contractor's Services not be performed by the Contractor, reserving the right, however, to have the Services performed by others and any lump sum compensation payable hereunder which is applicable to the deleted work shall be equitably adjusted by the parties. The Contractor's execution of this document shall constitute a representation by the Contractor that at the time of such execution the Contractor knows of no circumstances, present or anticipated, which come within the provisions of this paragraph or which might otherwise be viewed as or give the appearance of a conflict of interest on the Contractor's part. The Contractor acknowledges that the Authority may preclude it from involvement in certain disposition/privatization initiatives or transactions that result from the findings of its evaluations hereunder or from participation in any contract, which results, directly or indirectly, from the Services provided by the Contractor hereunder. The Port Authority's determination regarding any questions of conflict of interest shall be final.

7. Definitions

As used in this Section 38, the following terms shall mean:

Affiliate - Two or more firms are affiliates if a parent owns more than fifty percent of the voting stock of each of the firms, or a common shareholder or group of shareholders owns more than fifty percent of the voting stock of each of the firms, or if the firms have a common proprietor or general partner.

Agency or Governmental Agency - Any federal, state, city or other local agency, including departments, offices, public authorities and corporations, boards of education and higher education, public development corporations, local development corporations and others.

Investigation - Any inquiries made by any federal, state or local criminal prosecuting and/or law enforcement agency and any inquiries concerning civil anti-trust investigations made by any federal, state or local governmental agency. Except for inquiries concerning civil anti-trust investigations, the term does not include inquiries made by any civil government agency concerning compliance with any regulation, the nature of which does not carry criminal penalties, nor does it include any background investigations for employment, or Federal, State, and local inquiries into tax returns.

Officer - Any individual who serves as chief executive officer, chief financial officer, or chief operating officer of the Bidder by whatever titles known.

Parent - An individual, partnership, joint venture or corporation which owns more than 50% of the voting stock of the Bidder.

If the solicitation is a Request for Proposal:

Bid - shall mean Proposal;

2/8/16

Bidder - shall mean Proposer;

Bidding - shall mean submitting a Proposal.

In a Contract resulting from the taking of bids:

Bid - shall mean bid;

Bidder - shall mean Bidder; except and until the Contract has been awarded, then it shall mean Contractor

Bidding - shall mean executing this Contract.

In a Contract resulting from the taking of Proposals:

Bid - shall mean Proposal;

Bidder - shall mean Proposer;

Bidding - shall mean executing this Contract.

41. CONFIDENTIAL INFORMATION/NON-PUBLICATION

A. As used herein, confidential information shall mean all information disclosed to the Contractor or the personnel provided by the Contractor hereunder which relates to the Authority's and/or PATH's past, present, and future research, development and business activities including, but not limited to, software and documentation licensed to the Authority or proprietary to the Authority and/or PATH and all associated software, source code procedures and documentation. Confidential information shall also mean any other tangible or intangible information or materials including but not limited to computer identification numbers, access codes, passwords, and reports obtained and/or used during the performance of the Contractor's Services under this Contract.

B. Confidential information shall also mean and include collectively, as per *The Port Authority of New York & New Jersey Information Security Handbook (October 15, 2008, corrected as of November 14, 2013)*, Protected Information, Confidential Proprietary Information, Confidential Privileged Information and information that is labeled, marked or otherwise identified by or on behalf of the Authority so as to reasonably connote that such information is confidential, privileged, sensitive or proprietary in nature. Confidential Information shall also include all work product that contains or is derived from any of the foregoing, whether in whole or in part, regardless of whether prepared by the Authority or a third-party or when the Authority receives such information from others and agrees to treat such information as Confidential.

C. The Contractor shall hold all such confidential information in trust and confidence for the Authority, and agrees that the Contractor and the personnel provided by the Contractor hereunder shall not, during or after the termination or expiration of this Contract, disclose to any person, firm or corporation, nor use for its own business or benefit, any information obtained by it under or in connection with the supplying of services contemplated by this Contract. The Contractor and the personnel provided by the Contractor hereunder shall not violate in any manner any patent, copyright,

trade secret or other proprietary right of the Authority or third persons in connection with their services hereunder, either before or after termination or expiration of this Contract. The Contractor and the personnel provided by the Contractor hereunder shall not willfully or otherwise perform any dishonest or fraudulent acts, breach any security procedures, or damage or destroy any hardware, software or documentation, proprietary or otherwise, in connection with their services hereunder. The Contractor shall promptly and fully inform the Director/General Manager in writing of any patent, copyright, trade secret or other intellectual property rights or disputes, whether existing or potential, of which the Contractor has knowledge, relating to any idea, design, method, material, equipment or other matter related to this Contract or coming to the Contractor's attention in connection with this Contract."

D. The Contractor shall not issue nor permit to be issued any press release, advertisement, or literature of any kind, which refers to the Port Authority or to the fact that goods have been, are being or will be provided to it and/or that services have been, are being or will be performed for it in connection with this Agreement, unless the vendor first obtains the written approval of the Port Authority. Such approval may be withheld if for any reason the Port Authority believes that the publication of such information would be harmful to the public interest or is in any way undesirable.

42. PROVISIONS OF LAW DEEMED INSERTED

Each and every provision of law and clause required by law to be inserted in this Contract shall be deemed to be inserted herein and the Contract shall be read and enforced as though it were included therein, and if through mistake or otherwise any such provision is not inserted, or is not correctly inserted, then upon the application of either party, the Contract shall forthwith be physically amended to make such insertion.

43. INVALID CLAUSES

If any provision of this Contract shall be such as to destroy its mutuality or to render it invalid or illegal, then if it shall not appear to have been so material that without it the Contract would not have been made by the parties, it shall not be deemed to form part thereof but the balance of the Contract shall remain in full force and effect.

44. NO ESTOPPEL OR WAIVER

The Authority shall not be precluded or estopped by any acceptance, certificate or payment, final or otherwise, issued or made under this Contract or otherwise issued or made by it, the Director or any officer, agent or employee of The Authority, from showing at any time the true amount and character of Work performed, or from showing that any such acceptance, certificate or payment is incorrect or was improperly issued or made; and The Authority shall not be precluded or estopped, notwithstanding any such acceptance, certificate or payment, from recovering from the Contractor any damages which it may sustain by reason of any failure on his part to comply strictly with this Contract, and any monies which may be paid to him or for his account in excess of those to which he is lawfully entitled.

45. NON-LIABILITY OF THE AUTHORITY REPRESENTATIVES

Neither the Commissioners of the Authority, nor any officer, agent, or employee thereof shall be charged personally by the Contractor with any liability or held liable under any term or provision of this Contract, or because of its execution or attempted execution, or because of any breach hereof.

46. MODIFICATION OF CONTRACT

No change in or modification, termination or discharge of this Contract, in any form whatsoever, shall be valid or enforceable unless it is in writing and signed by the party to be charged therewith or his duly authorized representative, provided, however, that any change in or modification, termination or discharge of this Contract expressly provided for in this Contract shall be effective as so provided.

47. M/WBE GOOD FAITH PARTICIPATION

The Contractor shall use every good-faith effort to provide for participation by Port Authority certified Minority Business Enterprises (MBEs) and Port Authority certified Woman-owned Business Enterprises (WBEs) in all purchasing and subcontracting opportunities associated with this Contract, including purchase of equipment, supplies and labor services. If this Contract contains participation goals, the Contractor shall use good faith efforts to achieve the goals.

Good faith efforts to include participation by Port Authority certified MBE/WBEs shall include, but not be limited to the following:

- A. Dividing the services and materials to be procured into small portions, where feasible.
- B. Giving reasonable advance notice of specific contracting, subcontracting and purchasing opportunities to such MBE/WBEs as may be appropriate.
- C. Soliciting services and materials from a Port Authority certified MBE/WBE or seeking MBE/WBEs from other sources. To access the Port Authority's Directory of MBE/WBE Certified Firms go to www.panynj.gov/supplierdiversty
- D. Ensuring that provision is made to provide progress payments to MBE/WBEs on a timely basis.
- E. Observance of reasonable commercial standards of fair dealing in the respective trade or business.

48. TRASH REMOVAL

The Contractor shall remove daily from the Facility by means provided by the Contractor all garbage, debris and other waste material (solid or liquid) arising out of or in connection with its operations hereunder, and any such garbage, debris and other waste material not immediately removed shall be temporarily stored in a clear and sanitary condition, approved by the Manager of the Facility, and shall be kept covered except when filling or emptying them. The Contractor shall exercise care in removing such garbage, debris and other waste materials from the Facility. The manner of such storage and removal shall always be subject in all respects to the continual approval of the Port Authority. No equipment or facilities of the Port Authority shall be used in such removal unless with its prior consent

2/8/16

in writing. No such garbage, debris or other waste materials shall be or be permitted to be thrown, discharged or disposed into or upon the waters at or bounding the Facility.

49. ENTIRE AGREEMENT

This Contract including the Request for Proposals for # (including its Scope of Works and other attachments, endorsements and exhibits, if any,) as well as the Proposal submitted by the Contractor contains the entire agreement between the parties. In the event of any inconsistency between this Contract and other attachments, endorsements and exhibits, if any, including the Proposal submitted by the Contractor, this Contract shall be controlling.

ATTACHMENT D - CONTRACT SPECIFIC TERMS AND CONDITIONS

1. GENERAL AGREEMENT

Subject to all of the terms and conditions of this Contract, the Contractor hereby offers and agrees to provide all the necessary labor, supervision, personnel, equipment, materials and all other things necessary to perform the work required by this Contract, as set forth in the Scope of Work (Attachment E) ("Work" or "Services"), and do all other things necessary or proper therefor or incidental thereto, all in strict accordance with the provisions of the Contract and any future changes therein; and the Contractor further agrees to assume and perform all other duties and obligations imposed upon it by this Contract.

In addition, all things not expressly mentioned in the Scope of Work but involved in the carrying out of its intent and in the complete and proper execution of the matters referred to in and required by this Contract are required by the Scope of Work, and the Contractor shall perform the same as though they were specifically delineated, described and mentioned therein.

2. DURATION

- a. The term of the Contract (hereinafter called the "Base Term") is for four (4) year period and is estimated to commence on [REDACTED], 2016 at 12:01 o'clock a.m. (said date and time hereinafter sometimes called "the Commencement Date") and unless sooner terminated or revoked or extended as provided in Paragraph (b) and (c) hereof shall expire on February 28, 2020 at 11:59 o'clock p.m. (said date and time hereinafter sometimes called the "Expiration Date"). The Base Term of the contract as described in Attachment E: Scope of Work, in detail, herein as described below.

- **Implementation Phase:**

The Contractor shall complete the performance of the Work under this Contract within two (2) years after receipt of a Contract award letter by the Authority.

- **Maintenance Phase:**

Upon completion of the Implementation Phase, and upon written notice of Final Acceptance, by the Port Authority, the Contractor shall provide application maintenance and support services for the maintenance of the software for a period of two (2) years (herein after referred to as the "Maintenance Phase").

- b. The Port Authority shall have the right to extend this Contract for additional period(s) (hereinafter referred to as the "Option Period(s)") following the Expiration Date, upon the same terms and conditions. If the Port Authority shall elect to exercise the Option(s) to extend this Contract, then, no later than thirty (30) days prior to the Expiration Date, the Port Authority shall send a notice that it is extending the Base Term of this Contract, and this Contract shall thereupon be extended for the applicable Option Period. If the Contract

provides for more than one Option Period, the same procedure shall apply with regard to extending the term of this Contract for succeeding Option Periods.

- c. The Port Authority shall have the absolute right to extend the Base Term for an additional period of up to one hundred and twenty (120) days subsequent to the Expiration Date of the Base Term, or the Expiration Date of the final exercised Option Period (hereinafter called the "Extension Period"), subject to the same terms and conditions as the previous contract period. The prices quoted by the Contractor for the previous contract period shall remain in effect during this Extension Period without adjustment. If it so elects to extend this Contract, the Port Authority will advise the Contractor, in writing, that the term is so extended, and stipulate the length of the extended term, at least thirty (30) days prior to the expiration date of the previous contract period.

3. INCREASE AND DECREASE IN AREAS OR FREQUENCIES

The Port Authority shall have the right, at any time and from time to time in its sole discretion, to increase and/or decrease the services required hereunder, frequencies of all or any part of the services required hereunder or to add areas not described herein in the Scope of Work or remove areas or parts of areas which are hereunder so described. In the event the Port Authority decides to change any frequencies or areas such change shall be by written notice not less than 24 hours, said changes to be effective upon the date specified in said notice.

In the event of an increase or decrease in services, areas or frequencies, the Contractor's compensation will be adjusted to reflect such change in areas or frequencies utilizing the applicable hourly rates for such services as set forth on the Authority-accepted proposal from the Contractor.

Where no specific Unit Price has been quoted for the type of services to be increased or decreased, the Port Authority shall have the right to negotiate the compensation to reflect such change, whether an increase or decrease in areas or frequencies, which, in the opinion of the Authority, are necessary to complete the work, by multiplying the increased or decreased amount by the negotiated rate. In the event of a decrease in services, the Contractor shall not be entitled to compensation for Work not performed.

No such changes in areas or frequencies will be implemented which results in a total increase or decrease in compensation that is greater than 50% of the Total Price for the Base Term or, if changes are to be implemented during an Option Period, 50% for that Option Period.

4. PAYMENTS

Subject to the provisions of this Contract, the Authority agrees to pay to the Contractor and the Contractor agrees to accept from the Authority as full and complete consideration for the performance by the Contractor, of all its duties and obligations under this Contract and as sole compensation for the Services performed by the Contractor hereunder, a compensation calculated from the services performed and the respective prices inserted by the Contractor in the Pricing Sheets, Attachment F and accepted by the Port Authority, forming a part of this Contract, subject only to such additions or

2/8/16

deductions in the compensation as may be provided for in the sections hereof entitled Extra Work and the Compensation for Extra Work.

The manner of submission of all bills for payment to the Contractor by the Authority for Services rendered under this Contract will be subject to the approval of the Contract Manager in all respects, including, but not limited to, format, breakdown of items presented and verifying records. All computations made by the Contractor and all billing and billing procedures shall be done in conformance with the following:

Payment will be made in accordance with the prices applicable to the Milestones that appear on the Attachment F, Summary Sheet of the Pricing Sheets (page 1 of 10), as accepted by the Authority, as same may have been adjusted hereunder minus any deductions for services not performed and/or any applicable liquidated damages. All Services must be completed within the time frames specified or as designated by the Contract Manager. The Contractor will be due payment only upon acceptance of each deliverable by the Authority. Contractor shall submit to the Contract Manager by the fifth day of each month following the month of commencement of this Contract and on or by the fifth day of each month thereafter (including the month following the termination, revocation or expiration of this Contract) a complete and correct invoice for the Services performed during the preceding month accompanied by such information as may be required by the Contract Manager for verification. The invoice must show the Contractor's Federal Tax Identification Number. Payment will be made within thirty (30) days of Authority verification of the invoice. No certificate, payment, acceptance of any Services or any other act or omission of any representative of the Authority shall operate to release the Contractor from any obligation under or upon this Contract, or to stop the Authority from showing at any time that such certificate, payment, acceptance, act or omission was incorrect or to preclude the Authority from recovering any monies paid in excess of those lawfully due and any damage sustained by the Authority.

The Contractor shall submit all invoices to the following:

The Port Authority of New York and New Jersey
Technology Department
Two Montgomery Street, 5th Floor
Jersey City, New Jersey 07302

A. If the Authority directs the Contractor to provide services as Net Cost Work, the Contractor shall provide a technical scope of work, completion schedule, and cost estimate. Costs will be calculated by determining the number of hours that each Key Staff member will be assigned to the work, multiplying those hours by the fully burdened hourly rate for each Key Staff member, and summing those values for each.

B. Payments for Net Cost Work shall be deliverables-based. The Authority will identify the deliverables in each Net Cost Work assignment and designate percentage values for each deliverable. The Contractor will receive payment for each deliverable upon its acceptance by the Authority's Contract Manager.

C. Payments for Maintenance services during the Base Term and Option Years if exercised shall be a monthly lump sum cost equal to one twelfth (1/12) the annual Maintenance cost in the Contractor's Pricing Sheet.

D. In the event an audit of received invoices indicates that the correct sum due the Contractor for the relevant billing period is less than the amount actually paid by the Authority, the Contractor shall pay to the Authority the difference promptly upon receipt of the Authority's statement thereof. The Authority may, however, in its discretion elect to deduct said sum or sums from any subsequent payments payable to the Contractor hereunder.

5. EXTRA WORK

Except as specifically hereinafter provided in this numbered clause, the Contractor shall immediately supply such modified or additional products and services as the Authority may direct ("Extra Work"). If such changes or additions are without fault on his part, or on the part of others performing on behalf of the Contractor whether or not in privity of contract with the Contractor, and if solely as a result thereof, the Contractor incurs additional costs in the performance of his obligations hereunder, the Contractor may request compensation for such changes or additions in addition to the compensation provided for elsewhere herein. Agreement by the Authority, if such is forthcoming, shall be in writing. The execution of the aforementioned written agreement shall be a condition precedent to payment of any additional compensation for changes or additions. Accordingly, if the Authority directs the Contractor to make any change in or addition to products or services which entitle him to compensation in addition to that provided for elsewhere herein, he shall not proceed with such changes or additions prior to execution of the aforementioned written agreement except as set forth in the clause hereof entitled "Compensation for Extra Work."

If, as a result of any changes in, or additions to, the products or services the Authority directs the Contractor to make, the costs of performance of his obligations hereunder are decreased, the parties agree to make such adjustments by way of reduction in the compensation provided for elsewhere herein as they may deem equitable and reasonable and, in making such adjustments, no allowance shall be made for anticipated profits.

The Director shall have the authority to order Extra Work up to an amount equal to six percent (6%) of the Price for the Implementation Phase of this Contract, plus six-percent (6%) of the Price for the Maintenance Phase, plus six-percent (6%) of the Price for Option Period 1, plus six-percent (6%) of the Price for Option Period 2, unless the Contractor is advised of a greater authorization in a letter signed by the Authority's Chief Procurement Officer. Nothing herein shall be construed as a presentation that any changes or additions will be ordered.

6. COMPENSATION FOR EXTRA WORK

The Director and the Contractor may agree, in writing, on lump sum or other compensation for Extra Work. In the event that no such agreement is reached, compensation shall be increased by the sum of the following amounts and such amounts only:

- A. for labor, compensation equal to the applicable hourly rates set forth in Attachment F - Cost Proposal, as accepted by the Authority;
- B. the actual net cost in money of the materials required for the work; and
- C. in addition to the foregoing, if the extra work is performed by a subcontractor, five percent (5%) of the amounts under (A) and (B). No extra work shall be performed by a subcontractor without the prior written approval of the Director.

7. EXTRA WORK PROCEDURES

Whenever any Extra Work is performed by the Contractor on a basis other than on a lump sum basis, the Contractor shall, as a condition precedent to payment for such work, furnish to the Director or his/her authorized representative at the end of each day daily time slips showing (a) the name and employee number of each person employed thereon, and the number of hours in each day during which they performed Extra Work; (b) a brief description of the nature of the work performed and a list of material and equipment used and the Port Authority authorized representative who approved the Extra Work. Item (b) shall be supplemented by the Contractor at a later date with a statement indicating from whom materials were purchased and the amount paid therefor. Such daily time slips are for the purpose of enabling the Director or his authorized representatives to determine the accuracy of the amounts claimed by the Contractor.

8. PERFORMANCE OF EXTRA WORK

The provisions of this Contract relating generally to the Work shall apply without exception to any Extra Work required and to the performance thereof, except to the extent that a written order in connection with any particular item of Extra Work may expressly provide otherwise.

9. NET COST WORK AND COMPENSATION FOR NET COST WORK

The Contractor shall provide additional services in addition to those stipulated in the Scope of Work, which the Authority will separately compensate the Contractor for, and which herein are called "Net Cost Work." At the request of the Director, the Contractor shall develop or modify, and test software to support (a) the addition of systems, subsystems, hardware or devices which require monitoring and controlling from the Software (b) new or modified interfaces between the software and other systems or equipment for the purpose of sharing or exchanging data and (c) modifications to the Software related to Facility or Authority operations requirements.

Net Cost Work shall be paid in addition to the compensation inserted by the Contractor in the form of Contract clause entitled Attachment C – General Contract Provisions, and shall be computed in the same manner as is compensation for Extra Work, including any percentage addition to cost, as set forth in the clause of the Contract providing compensation for Extra Work. Performance of such Net Cost Work shall be subject to all provisions of the Contract relating to performance of Extra Work. Compensation for said Net Cost Work shall not be charged against the total amount of compensation authorized for Extra Work.

ATTACHMENT E - SCOPE OF WORK

I. DESCRIPTION

This scope of work defines the Contractor requirements and integration criteria for a fully functional Advanced Transportation Management System (ATMS) Software platform desired by the Port Authority of New York and New Jersey. The software is to be installed, configured, maintained and supported by the Contractor at all specified Authority facilities for the duration of the Contract.

II. OVERVIEW

- a. The Authority is seeking the procurement of an Enterprise License for a Commercial Off-The-Shelf (COTS) software product that will serve as its Agency-wide Transportation Management Software solution (the Software). A total of twenty-one (21) instances will be installed, configured, maintained and supported by the Contractor at the following locations:
 - Separate instances of the Software will be deployed at ten (10) Authority facilities to monitor and control ITS assets located at each. Those facilities are George Washington Bridge, Lincoln Tunnel, Holland Tunnel, Outerbridge Crossing, Goethals Bridge, Bayonne Bridge, JFK International Airport, LaGuardia Airport, Newark Liberty International Airport, and Port Newark-Elizabeth Port Authority Marine Terminal.
 - One instance will be installed at the Port Authority Agency Operations Center (PA-AOC) that is being planned at this time. That installation will have the capability to (when necessary) assume control of any/all facility-based ITS assets.
 - Exact replicas of the PA-AOC installation shall be installed at the Backup PA-AOC and at the Agency's undisclosed Disaster Recovery site to maintain business continuity in case of a disaster.
 - A "read-only" instance of the PA-AOC configuration shall be installed at the Traffic Engineering Center (TEC). All capabilities of the PA-AOC instance except for the ability to control facility assets must be provided.
 - "Lightweight" web-based two-way applications/interfaces shall be developed to allow communications between the PA-AOC instance and PATH, Ferry Transportation Unit, the Port Authority Bus Terminal, the George Washington Bridge Bus Station, Teterboro Airport, and Stewart International Airport (see Requirements I-13, I-14, I-16, I-17, and I-18). Information from the PA-AOC regarding incidents, planned construction work, and all other activities that would potentially impact operations at those facilities shall be made accessible via the "lightweight" applications to be developed by the Contractor. Operators will access these applications through a standard browser from their work areas. Those applications will also be used to communicate to the PA-AOC instance any incidents or service disruptions that occur at those locations.

- A "lightweight" one-way web-based application/interface shall be developed to provide Public Affairs with up-to-date information regarding incidents at or near the Authority facilities.
- b. The Software and database shall maintain an open architecture, allowing for integration with data mining tools and other Authority tools.
- c. The Software shall meet or exceed the requirements in Appendix 1 and Attachments M & N.
- d. The Software shall utilize System Interfaces developed by the Contractor to monitor and control Authority ITS assets. Where feasible, all System Interfaces shall be National Transportation Communications for ITS Protocol NTCIP conformant. The Contractor shall be responsible for developing/providing all interfaces (including any required middleware) between the Software and the ITS assets. Neither the Authority nor anyone working on its behalf (outside of this Contractor_ will be responsible for the development or provision of any interface components.
- e. The Software shall include a System Interface to enable Center-to-Center communications in accordance with the User Needs referenced in Appendix 2.
- f. The Software shall include all interfaces as noted in Requirements I-1 through I-18. The interfaces with OpenReach and WebEOC must include the capability to automatically send and receive real-time incident data. The intent is that facility operators enter information into one system (the ATMS) and that it then be automatically transmitted to and processed by OpenReach and WebEOC as if the information were input directly to those applications. The Contractor shall be responsible for all coordination and interface development activities between the Contractor and TRANSCOM (for OpenReach) and Intermedix Corporation (for WebEOC).
- g. The Software shall provide one single head-end web-based graphical user interface (GUI), wherein a single sign-on, reporting, and policy creation environment is used for operator interaction.
- h. All hardware (server, workstations, network equipment) for this project will be provided by the Authority. The Contractor shall prepare a report documenting its recommendations for the number of CPUs and required memory to be installed on each server as noted in Requirement PM-1, in Appendix 1 hereof. The recommendations will be utilized to develop specifications for hardware to be obtained by the Authority for this project. The Contractor may also refer to the following Attachment for additional information: Standards and Guidelines for Port Authority Technology (see Attachment N hereof).

III. NOMENCLATURE

There are variations in the industry with respect to Intelligent Transportation System (ITS) nomenclature. For the purposes of this document, the following terms and definitions apply:

ATMS – Refers to an Advanced Transportation Management System software solution with the ability to monitor multiple field assets in real-time for awareness of traffic and network

conditions, status of messages and signals and other metrics. ATMS software has the ability to control field assets such as cameras, signs, signals, and gates. ATMS software can record, log, and provide reports. ATMS software packages have a rule-based function allowing for multiple scenarios and response/action plans based on those scenarios.

CCTV – Refers to closed-circuit television cameras or video management system that operates the cameras. Cameras may either be analog with encoders or digital IP.

DMS – Refers to any type or variation of Dynamic Message Sign including LED, fiber optic, rotating drum, flip-disk, flip-vane, or blank-out. Various types, sizes, pixel arrays, pixel pitch and other parameters are listed for each facility in Appendix 3 of this Attachment.

LUCS – Refers to any type of lane-use control signal used for managed lanes over a roadway including LED X-Arrow, red-yellow-green bullseye, or flashing signals.

NOC – Refers to Network Operations Centers (the primary data center at Telecenter and the secondary data center at Port Authority Technical Center). The application/database software shall be installed on redundant VMware hosts (provided by the Authority) at the NOCs.

OCC – Refers to a Facility Operations Control Center. These are local centers and their main purpose is to manage the traffic and facility systems. The exception to this are the Staten Island Bridges (SIB) at which three (3) facilities are monitored from one OCC located at the Goethals Bridge.¹ All other Authority facilities currently have their own OCC.

OpenReach – Refers to a web-based software application sponsored by the I-95 Corridor Coalition through TRANSCOM. OpenReach has the functionality to provide regional awareness of logged incidents and major events by its multi-agency users. OpenReach has the ability to display VMS messages for most signs of any agency, view camera feeds, and provide traffic information through its Data Fusion Engine (DFE). DFE obtains its data from best available sources in the following order of priority: TRANSMIT, NAVTEQ, INRIX, and BlueTOAD. OpenReach does not have the ability to control field assets, as its purpose and goal is to provide full regional awareness for all agencies in the Tri-State region.

PA-AOC – Refers to the Agency Operations Center that will be the central hub of data, regional awareness, and, if necessary, control of field assets for the purpose of optimizing traffic flow and managing incidents on the roadway. Multi-modal applications are intended to share and exchange alerts and travel information with TMCs for various modes of transportation. The Authority TMC function will be conducted at a PA-AOC facility. The location of that facility is to be determined.

¹ As part of this project, three instances of the Software will be deployed at Staten Island Bridges (SIB): one each at the Goethals Bridge, Bayonne Bridge, and Outerbridge Crossing.

TMC – Refers to a Transportation Management Center.

TMS – Refers to the Agency-wide Transportation Management Software. This will be a specially configured ATMS software solution licensed to the Authority by the Contractor. The license will be an Enterprise License that will be in effect in perpetuity.

TTS – Refers to any type of vehicle probe system including TRANSMIT and Bluetooth detectors for the purpose of having a Travel Time System. These devices employ a check-in/check-out system based on at least two stations, essentially monitoring flow. This is also known as a vehicle probe system as TRANSMIT monitors travelers with E-ZPass tags and Bluetooth technology monitors the presence/ID of Bluetooth devices such as cellular phones. Multiple locations can be set up as links to monitor travel times with origin and destination points. Third party data may also be obtained from INRIX to provide TTS data.

VDS – Refers to any type of vehicle detection system including camera-based video analytics, microwave, loop detectors, or wireless magnetometers. These point detection stations are capable of monitoring vehicular volume, occupancy and speed (VOS) based on a single location or point station. VOS data is commonly employed in ATMS algorithms for real-time incident detection.

VSLS – Refers to any type or variation of Variable Speed Limit Sign including LED, flip-vane, or blank-out.

IV. ABBREVIATIONS

The following abbreviations are used to identify Authority facilities:

- **BB** – Bayonne Bridge
- **GB** – Goethals Bridge
- **GWB** – George Washington Bridge
- **GWBBS** – GWB Bus Station
- **EWR** – Newark Liberty International Airport
- **HT** – Holland Tunnel
- **JFK** – John F. Kennedy International Airport
- **LGA** – LaGuardia Airport
- **LT** – Lincoln Tunnel
- **OBX** – Outerbridge Crossing
- **PABT** – Port Authority Bus Terminal
- **PATH** – Port Authority Trans-Hudson
- **PAWANET** – Port Authority Wide Area Network
- **PN-EPAMT** – Port Newark-Elizabeth Port Authority Marine Terminal
- **Proposed Backup PA-AOC** – Will serve as a backup Center at a location to be determined.

- **Proposed Primary PA-AOC** – The primary OCC for Agency-wide monitoring and control of ITS equipment at a location to be determined.
- **SIB** – Staten Island Bridges
- **SWF** – Stewart International Airport
- **TEB** – Teterboro Airport
- **Traffic Engineering Center (TEC)** – The TEC will house an instance of the Software to provide monitoring capabilities only.

V. CONTRACTOR RESPONSIBILITIES

A. Management of the Work

The Contractor shall be responsible for the effective management of the work detailed herein and of the staff assigned to the work, including implementing sufficient management controls and utilizing such tools as are necessary to ensure the work is accomplished in an effective and efficient manner.

B. Organization

The Contractor shall be responsible for establishing and maintaining an organizational and operational structure appropriate to the work to be performed under this agreement. This shall include, but not be limited to:

- Assigning an appropriate number of staff with requisite certifications, and skills acceptable to the Authority, for the tasks to be performed.
- Supplying direct supervision of the staff assigned to carry out the work as defined herein.
- Providing qualified staff, acceptable to the Authority, for relief of the assigned staff in the event of vacation, illness, personal business or any other absence of the assigned staff.
- Providing the staff assigned with procedures for escalating issues that cannot be solved on-site and providing for the support of these individuals where such support is required to ensure prompt resolution.

C. Labor Force

The Contractor shall furnish sufficiently trained management, supervisory, functional and technical personnel to perform the services required of the Contractor under this Contract, with all such personnel subject to review and approval by the Authority.

If any such personnel is deemed unsatisfactory or does not perform the services to be furnished hereunder in a proper manner and satisfactory to the Authority, or in the determination of the Authority's Contract Manager may have taken any action which constitutes a conflict of interest or which is inconsistent with the highest level of honesty, ethical conduct or public trust or which the Authority's Contract Manager determines is adverse to the public interest or to the best interest of the Authority, the Contractor shall remove any such personnel from performing further work under

this Contract immediately, and replace them with personnel satisfactory to the Authority within two weeks, upon notice from the Authority.

D. Program Management – Appointment of Staff

The Contractor shall appoint member(s) of its organization to oversee the management of the Contract. The Contractor shall assign a full time, on site, technically proficient, experienced and fully qualified Project Manager. The Authority will require:

- Notification of the proposed assignment
- Information (resume, background, history with the Contractor, etc.) regarding the proposed Project Manager and the Contractor shall arrange for the individual(s) to be available for interview(s) at no cost to the Authority.
- The Project Manager shall meet the requirements in Attachment E, Appendix 1 as they relate to Project Management and be subject to approval by the Authority and subject to removal at the Authority's sole discretion.
- The Contractor shall provide the Authority with thirty (30) days prior notice of change of Project Manager and turnover shall be limited to once per twenty-four (24) month interval.

E. Application Management Methodology

The Contractor shall recommend an Application Management Methodology, subject to the review and approval of the Authority. This will include a methodology for recording changes made, new System Interfaces, documenting fixes and updates made to the software or interfaces, managing all environments (production, development, training, etc.), putting new software into production and keeping users of the software informed.

Security and control processes requiring various levels of review, signoff and segregation of duties shall be put in place for the application and it is expected the Contractor shall adhere to the existing processes, modifying them only as required and with Authority pre-approval, to ensure at least the same level of documentation and control that will allow it to meet or exceed provisions stipulated by the Authority.

The Contractor must notify the Authority when Security Patches have been tested with the Software and are available for installation on the Authority Servers. This process must be completed for Operating System and Database Security Patches within ten (10) business days of the release by the Operating System and/or Database Vendors pursuant to Section VIII - Service Levels.

F. Status Meetings

The Authority will identify a set of performance, utilization and status reports the Contractor shall be required to provide on a periodic basis. The Contractor shall deliver suggested reports and or changes to existing reports to the Authority, within the first thirty (30) days of the start of the Contract term, for Authority approval.

The Authority will determine the frequency of reporting, typically weekly, and the Contractor shall provide reports accordingly.

The Contractor shall schedule and conduct regular status meetings (both various Authority Departments focused and Contract Management focused) at an Authority-selected site no less frequently than on a weekly basis with the Authority. Contract Management meetings, with Technology Department, are anticipated to be weekly. Customer focused meetings, with Authority business owners and Technology Department, are anticipated to be bi-weekly. The Contractor shall facilitate participation by Authority personnel who cannot attend in person by providing web access to the meetings using Webex or an equivalent product.

At the sole discretion of the Authority, the frequency of meetings may be adjusted. These meetings will be held for the following purposes, but will not be limited to:

- Tracking the progress of the application and/or systems management activities;
- Reporting on the operational status of the system;
- Reviewing the Contractor's performance to the contracted service level metrics;
- Reviewing Contractor's invoices for services provided;
- Resolving disputes; and
- Tracking the progress of projects.

The Contractor's Project Manager shall produce and deliver to the Authority, at least twenty four (24) hours prior to each status meeting, a project status report and lead the meetings as appropriate. The report shall, at a minimum, provide a complete statement of the system's status, performance measure reporting, and indicate progress made during the reporting period. Also included shall be progress made on work to correct deficiencies, activities to be undertaken in the next reporting period, activities/tasks behind schedule and identification of problems/concerns related to the system, as well as statistics on problems encountered/resolved in the reporting period and year-to-date.

G. Security

1. Safeguarding Data

All information concerning the business of the Authority which becomes accessible, or known, to the Contractor, its employees or subcontractors including, but not limited to, financial information, customers, customer lists, business plans, operational plans, data and computer programs, documentation, engineering/technical data, design process, pricing, research and development, strategic plans, and operating data resident on electronic media, or other media processed, stored, archived or maintained, shall be protected from loss, erroneous alteration, and shall be held in strict confidence and protected from unauthorized access. All confidential data shall be protected at all times. The Contractor shall utilize best practices to prevent unauthorized access, modification, theft or other loss of the Authority data but, in no event, less than the same care and processes that it utilizes to protect its own information of a similar nature. In the event of any non-authorized access, modification, disclosure, theft or other loss,

or inability to account for any Authority data, the Contractor shall provide immediate notification to the Authority's Contract Manager. In addition, the Contractor shall be liable for all damages or expense to the Authority resulting from any such non-authorized access, modification, disclosure, theft or other loss, or inability to account for any Authority data including the cost of recovery of lost or modified data, staff time in dealing with the ramifications of the disclosure of private information and corrective procedures and actions undertaken.

2. Secure Access to the Software Applications

In order to maintain confidentiality of sensitive information, security provisions must be employed in the Software. These include data access limitation by password and permission, ITS asset monitoring and control by password, user role, and other permission schema, maintenance of audit controls, and security violation reporting. Only the assigned Authority user may have control of the assignment, removal or reinstatement of a user. Any changes shall be audited. Database access for the Contractor shall be removed once the Contractor has completed their work. All passwords shall be encrypted and any traffic going over the air or across a network must be encrypted. Passwords shall be changed at set expiration times and account lockout of accounts for three or more tries must be enforced. All other security-related requirements included in this and any other Attachment to this RFP must be met.

3. Escrow

The Contractor shall maintain an escrow account with a Port Authority approved and independent third party company in the business of providing escrow services, unless informed otherwise. The Contractor shall deposit the latest source code along with all necessary documentation, test programs, specifications, instructions for maintaining or modifying the licensed software and notify the Port Authority of the deposit date. The deposit shall contain all libraries and the platform operating system to allow the application to be recreated if so needed.

Note: The Port Authority may require the Contractor to have the independent third party perform testing services on the escrow deposit.

H. Quality Assurance (QA)

The Contractor shall establish and maintain a quality assurance program that the Contractor shall utilize to assure that all work is performed in accord with the terms of this Contract, including compliance with this Attachment E and its Appendices, and at a level consistent with acceptable industry practices. The Contractor shall employ procedures to assure the timely and effective execution of all tasks required by this Contract. The QA Program shall include a measurement program that tracks the quality and productivity of services provided by the Contractor. The Contractor shall issue reports regarding this Quality Assurance activity each quarter.

I. Contractor's Personnel

The Contractor shall be responsible for maintaining the appropriate knowledge, skills and abilities of its staff assigned to this account by providing a regular ongoing training program appropriate to the needs of the staff assigned.

1. Contractor Employee Minimum Skill Requirement

Staff assigned must be experienced in the configuration of the Contractor's Software offering. The Contractor shall propose the staffing to be provided to meet the services required and identify minimum experience level for each staffing position. This shall identify minimum ATMS Application experience and minimum experience with the Contractor's product (the Software). The Contractor shall similarly specify minimum technical experience of staff, related to support of System Interface Development. The proposed staffing shall be depicted in an organizational chart format with each position's experience level clearly designated.

2. Key Staff and Key Staff Replacement

All non-administrative staff that is proposed to be assigned to this project will be considered to be Key Staff and they shall be listed in the organization chart referenced in the immediately preceding Subsection I.1. Should the need arise for the Proposer to replace Key Staff before or at any time during the term of the Contract, replacement staff shall be assigned to the project only with the prior approval of the Authority. The Proposer shall notify the Authority of the need to replace key staff and submit qualifications for all proposed candidates. The Authority shall review the submitted materials and advise the Proposer which, if any, of the candidates would be an acceptable replacement. All such replacements shall possess equal or better skills and shall be provided for the same or lesser cost to the Authority. The Authority will then interview acceptable candidates and notify the Proposer of the results of the Authority's assessments. Any candidate deemed to be acceptable by the Authority may then be assigned to the project.

3. Reporting of Accidents

The Contractor shall promptly report in writing to the Contract Manager and to the Manager, Claims Administration, the Port Authority of New York and New Jersey, all accidents whatsoever arising out of or in the connection with the performance of the Contract which result in injuries or property damage, giving full details and statements of witnesses. In addition, if death or serious injuries or damages are caused the same shall be reported immediately by telephone to both of the said Authority representatives.

J. Maintenance of Application Metrics

The Contractor shall provide services to periodically assess and continuously improve metrics on the quality and performance of the Authority's applications and systems impacted by this project.

K. Customer Budget Planning and Billing

The Contractor shall assist Authority staff with the development of annual customer plans, in accordance with deadlines established by the Authority. These plans are to be used to establish the level of anticipated enhancements and support (in estimated and actual dollars) for the application and System Interfaces. The customer plans are used during the Authority's annual budget process for establishing both the Authority's corporate support budget and the user expense budgets. The Contractor shall also provide monthly accounting of services and expenses.

L. Location Where Service Will be Provided

The Authority requires that key team members, including the Project Manager perform all their work on Authority premises [generally available Monday through Friday, 8:00AM to 5:00PM] at the location designated by the Authority, except where specifically noted herein or in the Contractor's proposal, and agreed to by the Authority. These key team members are full time staff requiring direct interaction with Authority personnel to perform their duties. The locations may be changed at the Authority's sole discretion to facilitate work at the facilities. The Proposer shall propose which services will be provided off site to reduce cost or gain some other potential advantage. The Proposer may propose various alternatives with associated costs for consideration.

The Authority will provide work space for the Contractor's personnel, which includes space, utilities, current work station equipment, and reasonable telephone usage. If the Contractor requires additional site resources and/or relocation to an alternate site, and/or workstation equipment upgrades, the Authority will not assume any costs for space, workstation equipment or related networking and telecommunications equipment, software and/or expense. All expenses for off-site services shall be specified in the proposal.

The Contractor shall provide its own data processing equipment for staff working remotely, excluding that set forth above, and reimburse the Authority for its usage of telephone and fax services for personal reasons.

The final determination of which services are to be provided off-site will be made by the Authority to assure an appropriate level of application and system responsiveness and support.

M. Contract Completion

At the end of the term of this Contract, the Contractor shall work with the Authority and any other contractors to transition support within an agreed upon timeframe. The transition period shall not exceed three (3) months and shall conclude on the date upon which this Contract expires. The Contractor shall perform all services as requested by the Authority to ensure successful transition and the Authority will separately compensate the Contractor for this "Net Cost Work."

N. Return of Data

Upon the termination or expiration of the Contract, all Authority data stored on electronic media or otherwise, shall be returned to the Authority without cost. Any copies held by the Contractor shall

be purged from the Contractor's files, and the Contractor shall send the Authority a notarized statement confirming such purging and destruction.

O. Right to Use Contractor Tools

Upon termination of the Contract, the Contractor may have implemented specific Contractor owned or proprietary tools for the management, operation or reporting on the application maintenance environment within the Authority. To avoid disruption of operations, the Authority or its designee will require use of, or access to, any and all Contractor specific tools or services until such time as they can be replaced. Additionally, maintenance, training, support and documentation may be required.

P. Right to Acquire Contractor Tools

Upon expiration or termination of the Contract, the Contractor shall provide the Authority or its designee with the right to license or purchase, at the price currently in effect for its most favored customers, those materials, tools and equipment owned by the Contractor that allowed for the support and operation of the Authority application maintenance and system infrastructure. However, if termination is due to the Contractor's failure to perform, this will be at no cost to the Authority.

It should be noted that if Contractor-owned or proprietary tools are necessary for the continued operation and maintenance of the applications, the Contractor is required to use tools which can be transferred to the Authority such that the ongoing support of the application is not in jeopardy at the termination of the contract.

VI. REQUIRED SERVICES

A. Implementation Sequence and Schedule

The Contractor shall furnish, install, configure, maintain, and support an ATMS software package (the Software) that will become the Authority's Agency-wide TMC Core Software solution. Separate instances of the Software shall be installed on workstations at each Authority facility to monitor and/or control ITS assets. It is anticipated that a total of twenty-one (21) installations of the Software will be deployed within the Implementation Phase. The primary application/database software shall be installed on redundant central servers (provided by the Authority) at the NOCs. The NOC will serve as the data repository and information hub for the Authority. Facility instances of the Software shall continually transmit data regarding traffic volumes, incidents, etc. to the NOC for purposes of data archiving and calculation of facility-specific performance metrics.

The PA-AOC shall have the capability to monitor and control assets at any Authority facility when required. The PA-AOC shall also provide Agency-wide regional situational awareness via automated communications with the facilities. Exact replicas of the PA-AOC instance shall be located at the Backup PA-AOC, TEC, and an undisclosed Disaster Recovery Site.

The Contractor shall furnish, install, configure, maintain, and support "lightweight" web-based interfaces for use by PATH, PABT, GWBBS, Ferry Transportation Unit, Stewart International Airport, Teterboro Airport, and Public Affairs. Using standard browsers and Agency authentication, the Software shall provide users access to traffic and incident information that could potentially impact their operations. The applications shall also permit authorized users to input information regarding incidents at or near their facilities, which may impact other Authority facility operations. As part of the System Interface Development-related efforts, the Contractor shall meet with representatives from the above entities to identify the exact information to be exchanged.

All inter-facility communications shall utilize the Port Authority Wide Area Network (PAWANET). Detailed system requirements are presented in Appendix 1 of this Attachment E.

The Contractor shall provide the Authority with hardware recommendations for each workstation and server upon which the Software will be installed. This information shall be included in a separate report that will be part of the Project Management Plan pursuant to Requirement PM-1. The Authority will acquire and install all servers and operator workstations. Workstations will include monitor, keyboard and mouse. In addition, the Authority will install and configure server and workstation operating systems, databases, security software, and all other software required per the Port Authority Standards and Guidelines for Port Authority Technology (see Attachment N). This does not include the installation and configuration of the TMS, which is the sole responsibility of the Contractor.

Figure 1 below presents an implementation sequence and high-level schedule proposed by the Authority. Proposers must either explicitly state that they will accept the Authority's proposed schedule or specify an alternative one including detailed rationale for deviating from the Authority's proposed schedule as part of their Technical Approach. Any such Project Schedule must be approved by the Authority before work on this project commences.

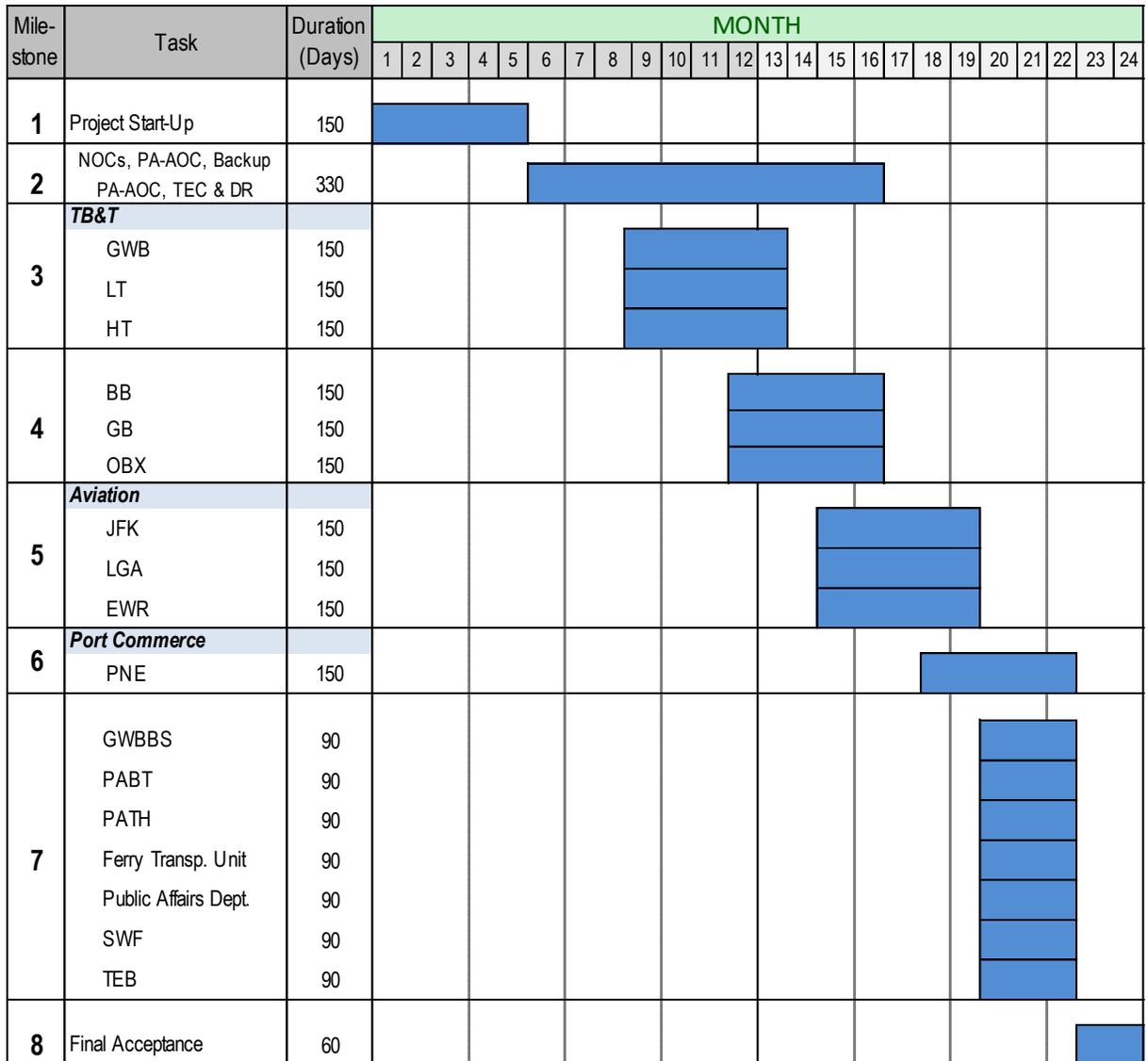


Figure 1- Implementation Sequence and High-Level Schedule

B. Implementation Phase (Years 1 and 2)

During the Implementation Phase, the Contractor shall install, configure, maintain, and support the Software at the NOCs and at each of the sites depicted in Figure 2; develop, test, implement, support, and maintain system interfaces (SI) to establish communications between the Software and the local legacy ITS assets; and develop, test, implement, support, and maintain the Traffic Management Data Dictionary TMDD Standard version 3.03 (or higher) conformant interfaces to enable communications between the facilities and the PA-AOC as well as between the PA-AOC and all external entities. To accomplish the objectives of this project, three types of SIs shall be developed by the Contractor during the Implementation Phase:

- a) Center-to-Field (C2F) interfaces to allow the Software to monitor and control legacy assets, and National Transportation Communications for ITS Protocol (NTCIP)-conformant SIs between facility Software instances and new ITS assets projected to be installed during the Implementation Phase (see Appendix 3);
- b) SIs to interface with subsystems such as TACTICS, eAlerts, and Nextiva; and
- c) TMDD Standard version 3.03 (or higher)-conformant Center-to-Center (C2C) interfaces to automate communications between facilities and the PA-AOC and between the PA-AOC and OpenReach via a two-way interface. C2C User Needs that must be met by these SIs are included in the document referenced in Appendix 2.

The Contractor shall identify the total number of unique SIs, develop, test and document each, and deploy them at each facility as appropriate. The Contractor shall be responsible for maintenance of the SIs for the duration of the Contract. The Contractor shall ensure that the SIs are "plug-and-play" such that an SI developed for assets at one facility can be used at all other Authority facilities that deploy that asset type at no additional cost to the Authority. The Contractor shall be responsible for maintenance and support of their solution for the duration of the Contract.

The Contractor shall conduct work sessions at each facility to document operational scenarios and to develop appropriate corresponding response plans. The response sequences shall subsequently be approved by the Authority and then incorporated into the facility and PA-AOC software instances. Implementation of the Response Plans must be accomplished via software configuration rather than through changes to the Software code.

The Contractor shall be responsible for preparation of all training materials and the delivery of training to the end users at each facility. Separate sessions shall be held for System Administrators and Facility Operators. Train the Trainer is not an acceptable solution for the Authority. The Contractor shall conduct a minimum of three 4-hour sessions for 8-12 Authority staff at each facility each year for the duration of the Contract (See Section VI. B. 5. Training). The Contractor shall be prepared to provide training sessions during all shifts.

The Contractor shall assign a full-time Project Manager (to be approved by the Authority) to the project. The Project Manager shall, at a minimum, be responsible for coordinating the Contractor's efforts, scheduling meetings, documenting key findings, representing the Contractor at all meetings, and reporting to the Authority as required.

The Contractor must fully adhere to the Authority's ITS Design Guidelines (See Attachment O), pertinent sections of Division 16 of Specifications, (<http://www.panynj.gov/business-opportunities/pdf/discipline-guidelines/traffic.pdf>), and Standards and Guidelines for Port Authority Technology (See Attachment N). C2F System Interface testing must be conducted in accordance with NTCIP 9012, Testing Guide for NTCIP Center-to-Field Communications (<http://www.ntcip.org/library/standards/default.asp?standard=9012>). The Contractor shall be responsible for preparing all Test Plans, which must be approved by the Authority prior to implementation (See Section VI. B. 3. Testing).



Figure 2 - System Context Diagram

The Authority will provide all computer hardware, Operating Systems, and Database Licenses. Hardware recommendations shall be provided by the Contractor pursuant to Requirement PM-1. Upon approval of the Project Management Plan by the Authority, the Contractor shall provide written notice to the Authority of the dates when the servers are required. The written notice shall allow a minimum of 8 weeks for servers to be available. The Operating Systems will be installed on the servers by the Authority along with the Database software. The Contractor shall be responsible for creation of the required database schemas and installation of all instances of the Software.

The schedule in Figure 1 is based upon completion of Software installation, configuration, and testing one Line Department at a time. Work at each facility at which an instance of the Software is to be installed will require approximately 150 calendar days for interface development, software installation, testing, and training. The NOC and PA-AOC instances have been allocated 330 calendar days for completion of those tasks aligned with the requirements

2/8/16

related to Center-to-Center (C2C) communications. Implementation of the NOC and PA-AOC instances will proceed concurrently with implementation at the GWB, HT, and LT and shall include all C2C Interfaces. The intent is to bring the PA-AOC instance online as soon as practicable to begin to collect facility-based data and to provide regional awareness. The "lightweight" applications/interfaces have been scheduled to be built, installed, and tested in ninety (90) calendar days.

As shown in the Schedule, work will first be performed at the NOCs and PA-AOC and will commence when the Project Management Plan and System Documentation have been submitted by the Contractor and reviewed for completeness and approved by the Authority. System C2C Interface Development for the PA-AOC instance (Milestone #2) will include deployment at the Backup PA-AOC, TEC, and the Disaster Recovery (DR) site. Once the NOC implementation is completed, concurrent installation and configuration of instances at George Washington Bridge, Lincoln Tunnel, and Holland Tunnel (Milestone #3) will begin. When integration of the PA-AOC with GWB, LT, and HT has been completed, data from those three major facilities will begin to be stored at the NOC. Project work at all facilities has been broken into the following four deliverables:

- System Interface (SI) Development;
- Software Configuration;
- Testing; and
- Training.

Implementation at the Bayonne Bridge, Goethals Bridge, and the Outerbridge Crossing will be performed concurrently (Milestone #4). System Interface development will include C2C Interfaces with the PA-AOC.

Implementation at Aviation facilities will be performed concurrently at JFK, LGA, and EWR (Milestone #5). System Interface development will include C2C Interfaces with the PA-AOC.

Interface Development for Port Commerce (Milestone #6) shall include SIs to control local assets as well as the C2C Interface with the PA-AOC that shall be developed and tested.

Upon completion of Software Configuration for Port Commerce, the seven "lightweight" applications shall be developed, implemented, and tested at GWBBS, PABT, PATH, Ferry Transportation Unit, SWF, TEB, and Public Affairs (Milestone #7). Each of these instances is to receive data and information from the PA-AOC via C2C Interfaces and have the capability to input information regarding locally occurring incidents into the system.

Subsequent to successful completion of the 30-day Operational Testing of the "lightweight" applications at the above locations, the final round of System Acceptance Testing will commence. Final Acceptance (Milestone #8) will be reached at the conclusion of the final 30-day Operational Testing period.

1. Submittal and Documentation Requirements -- Unless specifically stated otherwise, the Contractor shall submit, to the Authority's Contract Manager, project management, design, testing, operational documentation and plan submittals as follows:
 - a. General Submittal Requirements
 - i. The review period for Contractor's submittals shall be a minimum of 10 business days. The Contractor is responsible for maintaining the approved schedule even if multiple review cycles are required for each submittal.
 - ii. The Contractor shall submit all narrative text or tabular list-based submittals as follows:
 1. Bind all 8.5" x 11" documentation, except standard spiral bound materials, in logical groupings in 3-ring loose-leaf binders. Each bound grouping of documentation shall be appropriately labeled. No documentation shall be on paper smaller than 8.5" x 11". Document pages shall be numbered sequentially. Revised documentation shall be identified with a version number and revision date on the cover and on each page.
 2. Six sets of all hardcopy documents shall be provided by the Contractor.
 3. One set in machine readable format which shall be viewable and easily modifiable with Authority approved version of Microsoft Office suite of tools.
 - iii. Within twenty (20) calendar days after receipt by the Contractor of Contract Award, the Contractor shall submit a Project Plan and Schedule to the Authority's Contract Manager in accordance with Project Management Requirements PM-1 through PM-9. The degree of detail to be included in the project schedule shall be sufficient to identify at a minimum:
 1. All activities, tasks and stages of Software installation, milestones and deliverables as specified both within the Contractor's system development and installation methodology and those specifically identified herein.
 2. All activities and tasks associated with the development, installation, integration, configuration and preparation of the Software, System Interfaces, subsystem components, submittals, testing, and training.
 3. Interfaces and dependencies with preceding, concurrent, and succeeding work effort.
 4. Authority resources needed at the task level.
 - iv. The Contractor shall prepare and submit updated progress schedules to the Authority's Contract Manager every week, with a complete outline of all tasks and activities required for the execution of this project.

- v. The Contractor shall schedule and conduct regular status meetings on strategic, tactical and operational issues a minimum of once per week. The Contractor, the Authority, and other service providers necessary for resolution of agenda items shall be in attendance. Meeting frequency may be modified at the sole discretion of the Authority. The purposes of these meetings shall be, but not limited to:
 - 1. Tracking the status of work activities
 - 2. Reporting on the operational status of the services, infrastructure and communications links essential to the success of this project.
 - 3. Reporting on progress achieved with Software configuration and System Interface development and testing since the last meeting.
 - 4. Reviewing and reporting on project risks and issues.
 - 5. Reviewing schedule performance versus baseline.
 - 6. Identifying and discussing Deliverables acceptance criteria.
 - 7. Discussing/resolving minor disputes.

The Contractor shall prepare and deliver to the Authority, a minimum of 48 hours prior to each scheduled meeting, an agenda that includes a status report listing strategic, tactical and operational items and issues and the status of each. The report shall, at a minimum, provide a status update for the reporting period. Also included should be progress made on work to correct deficiencies (if any exist), work completed since the last report, work planned for the next reporting period, schedule status, important risks and issues, and list of decisions required from the Authority.

- 2. System Documentation – Within thirty (30) calendar days after Contract Award, the Contractor shall submit, to the Authority’s Contract Manager for review and approval, a detailed description of the System to be furnished under this Contract. System documentation shall include comprehensive and detailed technical descriptions of the Software, required hardware, System Interfaces to be developed during the Implementation Phase, communications architecture, and any other information that the Contractor deems to be essential to the overall system. At a minimum, the following information shall be provided:
 - a. A summary of materials provided in the System Documentation including an overview of the Software describing all major components, and special features of the System which address performance, expansion, system security, ease of use, and maintainability.
 - b. A Design Overview which shall describe the overall implementation design. This shall include the advantages and disadvantages of the design (e.g., modularity, flexibility, expandability, redundancy), and an explanation of why the design is the best implementation to meet the Authority’s requirements.

- c. A detailed Functional Description that includes both a detailed description of the overall system as well as a functional description of the major components and describes their operation.
- d. A graphical representation and accompanying narrative of the System Architecture which shall depict logical components, system interfaces, and interconnections between facility Software instances.
- e. A Failure Handling and Recovery matrix showing types of failures, process for reporting them (whether manual or automatic) and accompanying narrative describing system diagnostics used to detect and isolate failures.
- f. A set of narratives shall be prepared, which shall describe all user functions to enable the System to operate as specified. The narratives shall also place special emphasis on the requirements for operation and system administration, with an explanation including graphic descriptions that illustrate the proposed user interface and shall describe the following:
 - i. Operating features
 - ii. Reports and their formats
 - iii. Screen Layouts illustrating all user interface screens, graphical maps, pop-up windows, pull down menus, etc.
 - iv. Matrix that defines the access restrictions to all applications, business user and workstation location.
 - v. A description of all System Security features designed into the system to control and monitor access to the System and its components (i.e., hardware, software, and data).
 - vi. A description of the expected Data Loading that identifies the type, amount, and frequency of data transmission between ITS assets at each facility and the facility instance of the Software (C2F communications) as well as the type, amount, and frequency of data to be transmitted between facility Software instances and the NOC instance. These analyses shall include estimates of bandwidth requirements for each communications path in the system.
 - vii. Any other material, documentation or drawings which the Contractor deems appropriate.
- g. A detailed description of the database including the following:
 - i. A description of the database schema including overall organization of the files and tables to be used for the NOC Software. This description shall include an identification of all data files, tables, and fields, and the relationships between fields and tables. This description shall also include but not be limited to full details regarding any third party database products including version, release,

functional characteristics, operational requirements and any other relevant characteristics of the product.

- ii. A Data Dictionary listing all System data elements, including the size, definition, validation rules and other information pertaining to the data elements.
 - iii. A Data Storage Analysis shall be prepared and shall include a description of the techniques employed to estimate the size of the NOC VMware hosts that shall have virtual database servers for each facility.
 - iv. A Data Flow Diagram shall be prepared to graphically depict the logical processes that comprise the System and an illustration that depicts the data flows as the data moves between processes and/or facilities. The documentation shall include data flow diagrams and other necessary documentation to understand how the data is handled and stored.
 - v. An Entity-Relationship Diagram shall be prepared and transmitted in both hardcopy and electronic form to the Authority. This description shall identify all significant System entities and show the nature of all significant interactions from the data's inception to storage.
- h.** The Software shall operate on computer hardware to be provided by the Authority in accordance with hardware specifications provided by the Contractor pursuant to Requirement PM-1. The Contractor shall document the hardware requirements for each Software instance (including redundant components) that will ensure satisfaction of the functional and performance requirements of the Contract. The Contractor's report shall state all computer hardware considerations and include, at a minimum, the computer architecture, number of processors, processor speeds, memory, secondary storage, and peripheral considerations.

Subsequent to submission of the Contractor's hardware requirements, the Contractor shall meet with the Technology Department (TD) to review them, formulate system architecture, and finalize the computer architecture that will be used to run the Software.

The System will be connected to PAWANET, which may be expanded by the Authority to meet the requirements identified by the Contractor. The Contractor shall provide detailed requirements of what will be needed from PAWANET in order to satisfy the functional and performance requirements of the Contract.

The Contractor shall provide a complete list of COTS products furnished as part of the Contract. Include the name, manufacturer, part number and material specifications as applicable.

3. Testing – Prior to Final Acceptance, all Software Instances and System Interfaces must successfully complete Acceptance Testing and 30-day Operational Testing as follows:

- a. Field Acceptance Testing – After Contract Award, the Contractor shall configure the Software and develop System Interfaces as necessary to meet the contract requirements specified herein and in Appendix 1 hereto. Prior to implementation of the Software or any SI in the Production Environment, the system shall be tested in its entirety using the Authority Test Lab Environment. The Authority Test Lab Environment consists of a centralized fault tolerant server environment located in the datacenters. The Lab environment can be accessed from any Authority facility connected to PAWANET.

The Authority's Contract Manager has the right to include additional Authority representatives with technical and operational expertise to assist in witnessing the tests. The Contractor shall maintain a test bed of transactions and known results to verify the integrity of new versions of the Software, including a retest of the current system after modifications are made. The test bed shall be updated to include test data for all new conditions arising out of maintenance, enhancement or upgrade of the system.

A Test Plan shall be submitted to the Authority's Contract Manager for approval not less than 30 days prior to the proposed start of the testing. Upon receipt of the Test Plan, the Authority will promptly (within 10 business days) review and comment upon the Plan's contents. The Contractor shall respond to all comments and resubmit the Test Plan for final review and approval. The Test Plan shall include, at a minimum, the following details:

- i. A summary statement of the purpose and goal of each portion of the Test Plan(s);
- ii. The testing method. A description of the overall test environment including block diagrams showing the total test environment, relevant equipment interconnection and test equipment hookup.
- iii. A list of all hardware, software, and System Interfaces to be included in the testing.
- iv. Detailed Test Cases that demonstrate every feature and function to be provided in the furnished Software and/or System Interfaces.

For each Test Case, the following, at a minimum, shall be provided:

- i. The steps for each Test Case
- ii. Test Purpose
- iii. Conditions which exist at the start of each test procedure
- iv. Expected Results
- v. The specific requirement to be addressed by the test.

Requests to conduct tests shall be submitted to the Authority's Contract Manager for approval, not less than 30 calendar days prior to the proposed start of the test. The request shall include the estimated length of time required to conduct the tests, and shall

include an agenda that identifies when each of the tests are scheduled to be conducted. The Contractor shall also submit draft copies of all user manuals to enable test participants to familiarize themselves with the System's operations.

If, in the opinion of the Authority's Contract Manager, there are an excessive number of failed tests, the Test Phase shall be halted and the Contractor shall repeat all or part of the tests, at the discretion of the Authority's Contract Manager, at a later date at no additional cost to the Authority.

Neither witnessing of a test by the Authority, nor the waiving of a right to witness a test, shall relieve the Contractor of the responsibility of furnishing the System that is in compliance with the Contract requirements.

Test Reports shall be submitted to the Authority after the completion of the testing phase. The reports shall state the testing results and indicate the nature of any failures, the reasons for them, what corrective actions were taken and a list of outstanding items.

Prior to deployment, Acceptance Testing shall be conducted to demonstrate that every feature and function of the Software and/or System Interfaces is fully integrated and is in conformance with the Contract documents. Testing shall demonstrate end-to-end processes and full functionality of all system components. The Contractor shall maintain a Requirements Traceability Matrix and shall report thereon the precise test and step that demonstrates that each requirement has been met.

At the conclusion of Acceptance Testing, the Contractor shall submit to the Authority a Field Acceptance Test Report for the purpose of verifying and validating that the installed system meets or exceeds the Requirements in Appendix 1 to Attachment E herein.

b. 30-day Operational Test_– Upon approval of the Field Acceptance Test Report, an Operational Test Phase shall begin. Authority staff, with advice and assistance from the Contractor, shall perform the Operational Test during a 30 consecutive day period. During this period, Authority operating staff will operate the system using the latest version of all applicable manuals, printed guides, and procedures.

i. Failures During Operational Test

If there is a major system, SI, or component failure during the 30-day Operational Test, the Contractor shall correct any such malfunctions as they occur. After the Contractor corrects the malfunction, the 30-day Operational Test shall restart, at day one, and shall continue until the system has operated without interruption or malfunction for 30 days, and the results are satisfactory, as evidenced by the written approval of the Authority's Contract Manager.

ii. Performance Period

The performance period for operational testing shall begin on the date operational testing commences. It shall end when the System has met the 30

consecutive days of operation in conformance with the Contract requirements at the required availability level stated herein.

- iii. At the conclusion of testing, the Contractor shall submit to the Authority a Test Report for purposes of verifying and validating the accuracy and integrity of the System and System Interfaces as installed. The Authority's Contract Manager will review the report and respond; indicating approval or noting required changes in either performance of the work or in the report. The Contractor shall make all changes and perform such necessary work as the Authority may direct in order to complete the 30-day Operational Test.
- iv. Separate 30-day Operational Tests shall be performed at each facility and for the PA-AOC instance of the Software.

Manuals -- No less than 30 calendar days before the date when Acceptance Testing is to begin, the Contractor shall prepare and submit for approval six (6) sets of complete separate manuals for Facility Operations Staff and administrators that will use the System. Separate manuals shall be developed for each site at which the Software is installed. All manuals shall be site-specific and shall document specifics related to configuration, operations and maintenance.

a. System Operations Manuals

A set of Operations Manuals shall be provided that clearly describes all User operations. The manuals shall explain all features and functions of the System for day-to-day operations and how to use the system to manage more complex situations and scenarios. A section for problems and/or exception conditions shall be included to enable the User to quickly resolve common operating problems.

The Operations Manual shall contain detailed descriptions of system operations and procedures on how to perform all user functions, including but not limited to adding/modifying operational scenarios and response plans, overriding suggested response plans to account for equipment that might be temporarily out of service or for any other reason, implementing any special system features, and error and alarm handling procedures including recovery from failures.

The Operations Manual shall be written for beginner computer users who are not familiar with detailed computer operations and terms. It shall contain step-by-step procedures with examples containing screenshots, explanations of the user interfaces, and graphics to illustrate the overall concepts. The manual shall be for instruction, study, and refresher use.

b. Application Administration Manual

The Application Administration Manual shall include but not be limited to all sections covering administration of the application, configuration functions, including but not limited to:

- i. Detailed instructions and procedures for the installation and configuration of the Software.
- ii. Detailed description and procedures for configuration of user access privileges and access levels to use of all application functions.
- iii. Detailed description and procedures for the configuration and management of the application and database.
- iv. Detailed description and procedures for installing, backing up, and restoring the application Software.
- v. Detailed description and of and procedures for conducting system health checks.
- vi. Detailed procedure that describes all of the steps to manually switch over operation from the primary application server (active) to the backup application server (passive) and to switch back to the former primary application server once the operation of the former primary application server is restored.

c. System Administrator's Manual

A System Administrator's Manual shall be provided which contains graphical depictions, written detailed descriptions and procedures of all functions required for the proper monitoring, maintenance, and administration of the system, including but not limited to, the following topics:

- i. Detailed procedure that describes all of the steps to manually switch over operation from the primary application server (active) to the backup application server (passive) and to switch back to the former primary application server once the operation of the former primary application server is restored.
- ii. Archiving data and restoring archived data to the database.
- iii. Backing-up and restoring the database.
- iv. Installation and configuration of the Software.
- v. Backing up and restoring the current version of the Software and System Interfaces.
- vi. Performance analysis.

- vii. Scheduled maintenance.
- viii. Audit and control.
- ix. Report production.
- x. Configuration control.
- xi. System diagnostics.
- xii. Database integrity checks.

A separate, removable section of the System Administrator's Manual shall contain information on the proper administration and control of the security features built into the System, including but not limited to: maintenance of user identifiers, password control, and security policy review.

d. Site Configuration Manual

A Site-specific Configuration Manual shall be provided for each facility and for the PA-AOC. This manual shall include all scenarios and pre-programmed response plans, site-specific configuration parameters and threshold levels; default parameters, actions, and descriptors. Interface details, operation, and configuration shall be presented.

e. Operations Run Book

This document shall contain a set of defined procedures developed by the Contractor for any recurring activities required for maintaining the day-to-day operations of the Software, as well as addressing out-of-the-ordinary operations. A run book shall be prepared for each facility and for the PA-AOC and shall include all the information the User would need to perform daily operations and information on dealing with problems that might arise during usage. Procedures defined in the run book shall include, but not be limited to: procedures for starting and stopping the Software, instructions for handling System Interface operations and testing, and procedures for special operations such as backing up the data, archiving the data, etc.

4. Final Versions of the Documentation and Applications Software – Prior to certification by the Authority that the Contractor has completed all work associated with the provision of a fully functional Software system at all facilities and the PA-AOC, the Contractor shall submit all design documentation, manuals, and/or drawings which have been developed or revised to accurately depict as-built conditions. System documentation shall be provided in both a bound copy and an electronic version that is Microsoft Office (including Visio) compatible. All CAD drawings must be AutoCAD compatible.

Final versions of the configured Software for each facility and the PA-AOC as well as all documentation shall be delivered to the Authority's Contract Manager.

5. Training

The Contractor shall conduct training for facility operators and system administrators prior to Software Go Live at each facility and when application system enhancements warrant such training to ensure that users are properly trained in the appropriate procedures associated with the system and can function effectively after training, prior to Go Live and/or implementation of the enhancement. Furthermore, the Contractor shall provide onsite training for each shift at each facility at least once per year for new users of the Software. The Contractor shall be required to conduct facility training during time periods when the appropriate staff is available. The Contractor shall collaborate with management at each facility to determine the dates and times of all training. **Training the Trainer will not be an acceptable method.**

Training Plans for each facility must be submitted to, and approved by, the Authority. Instructional videos shall be prepared and provided to the Authority for review and approval. The videos shall be facility-specific and shall provide step-by-step instructions on use of the software and SIs including all Graphical User Interfaces, Menus and Sub-Menus, Scenarios and Automated Responses, as well as System Troubleshooting. Facility-specific Training Manuals (including relevant screenshots) shall be prepared by the Contractor for Authority review and approval. All training materials (including manuals, tutorials and videos) shall be submitted to the Authority not less than 30 calendar days prior to the scheduled training. The Training Plan must be approved before the Authority will commence the review of Training Materials.

The Contractor shall be required to provide refresher training if the time period between the end of training and Go-Live exceeds one week.

C. Maintenance Phase (Years 3 and 4)

Software and System Interface maintenance and support shall include (but not be limited to) correction of all software "bugs;" provision of onsite annual training to Authority staff; installation, configuration, testing and validation of software upgrades; and the provision of Help Desk Services to answer facility operator questions regarding the software. These services are more fully described below in **Section a. Application Management, Maintenance, and Support Services.**

Additionally, at its sole discretion, the Authority may request, negotiate, and direct the Contractor to perform Net Cost work for, software enhancements, development of SIs to enable the Software to monitor and control newly acquired ITS assets, or any other task deemed necessary to modify and/or enhance the capabilities or performance of the Software. All such work shall be performed in accordance with this Contract and its terms related to Net Cost Work. Proposers shall furnish a list of Key Staff and the fully burdened hourly rates for each in their Cost Proposal. Those classifications and rates shall be used by the Contractor to develop

costs for the requested deliverables. The prices in the Cost Proposal that are accepted by the Authority will be the prices paid for any such additional Net Cost Maintenance Work.

a. Application Management, Maintenance and Support Services

The Contractor shall be responsible for providing management, maintenance and support services for the term of the Contract including option years and extensions.

The services to be provided include:

1. Support Functions: – The Contractor shall maintain, support and synchronize Production, Development, Quality Assurance, Training, and Staging environments for the Software. The lower tiers shall be used for development and testing of enhancements, configuration changes, System Interfaces, and new releases of the Software. It is anticipated that single instances of the Development, Quality Assurance, Training, and Staging environments will be required for the Contractor’s use.
2. Troubleshooting and Problem Management and Resolution – The Contractor shall be responsible for logging, documenting, tracking and resolving production-related issues while ensuring ongoing data integrity and any and all interfaces and/or systems interfacing the Software. This may include:
 - a. Correction of all production problems that require application code and/or configuration modification, or operational changes
 - b. Implementation of “hot-fixes” to the Software code
 - c. Provision of narrative documents describing the problem and resolution. This documentation must be stored in a central repository.

The Contractor shall:

- i. Provide full technical, workflow and security support. (See Section VIII. Service Levels). The Contractor shall be responsible for troubleshooting and maintenance, provide technical support to Authority staff as required, and conduct onsite training of Authority personnel on the application supplied by the Contractor.
- ii. Provide Tier 2 and 3 Help Desk Support. The Authority will provide Tier 1 support which will consist of script-based telephone assistance to users who are experiencing problems which can be easily resolved. If the Authority’s Tier 1 representative cannot resolve the issue, it will be referred to the Contractor for Tier 2 (software-related issues) or Tier 3 (network, database, server-related issues). The Contractor shall provide a fully staffed support group that will respond to incident reports in accordance with the Service Levels specified in Section VIII.

- iii. Provide break/fix support as necessary.
 - iv. Support Authority with reports and analysis of the Software's functionality.
 - v. Serve as a resource for Authority staff as related to application system functionality. This shall include, but not be limited to:
 - 1. Providing technical support to Authority staff and/or vendors relative to applications support
 - 2. Researching and taking corrective action on reported software malfunctions
 - 3. Participating in internal and external audits, to ensure that security and procedures are in accordance with best business practice as directed by the Authority's Contract Manager.
 - 4. Providing training materials as necessary.
 - vi. Provide twenty-four (24) hour on call and support availability for resolution of problems in accordance with the Service Level Agreements set forth in Section VIII.
3. Disaster Recovery Support – The Contractor shall assist the Authority in any disaster recovery test or in the enactment of a real disaster recovery operation. This includes fail over to the backup server as well as fail over to an alternative instance of the Software (at the PA-AOC, the Backup PA-AOC, and/or the Disaster Recovery Site). This item of work shall also include establishment of the PA-AOC instance with all functionality in an environment established at an Authority selected Disaster Recovery Site. The Contractor shall collaborate with the Authority's Contract Manager to define the scope of periodic disaster recovery tests, coordinate with other Authority staff and third parties to ensure all required tasks are executed, and conduct and evaluate the results of the Software tests. The Contractor shall maintain up-to-date Disaster Recovery Plans, including projected and actual timelines for the various recovery steps. The Contractor shall perform basic validation and ongoing tuning to ensure the resulting processes are always kept current. In the event of a real disaster, the Contractor's staff may be required to work from an external recovery location.
- Specifically, Disaster Recovery Support includes, but is not limited to:
- 1. Perform Yearly Functional Tests;
 - 2. Perform Yearly Technical Tests;
 - 3. Maintain Disaster Recovery Documentation;
 - 4. Maintain Currency of Disaster Recovery media at an off-site location.
4. Administration of the Software – Working with the Authority's Contract Manager, the Contractor shall establish and maintain user accounts, user roles, and user security profiles which shall control access to specific instances and features of the Software. Since the

Contractor shall be providing 24 hour support, it shall be responsible for creating system User IDs and Original passwords and rectifying Lockout issues for all Software instances.

Audit logs and user accounts are required to be reviewed for end user account activity. Automatic reporting capabilities shall be provided by the Contractor.

The Contractor shall configure and maintain the Software application security, via Authority Audit Department approvals, pursuant to Attachment M. Additionally, the Contractor shall:

- a. Setup Roles and Permission Lists;
- b. Maintain Security Roles as directed by Facility Managers;
- c. Recommend and Support Security processes; and
- d. Assign Roles to Users upon request.

The Contractor shall be responsible for maintaining and testing all SIs incorporated into the Software. Such testing shall include confirmation that individual interfaces operate as specified and that they are properly integrated into the overall solution.

5. Updates to the Software and/or System Interfaces – It is anticipated that over the life of the Contract, the Contractor shall make substantive revisions, modifications, and/or enhancements to its Software as a part of its business activities. The Contractor shall, upon approval of the Authority’s Contract Manager, be responsible for the deployment of new versions of the Software. When the Contractor releases major enhancements to the Software, it shall prepare and present to the Authority a risk-benefit assessment with recommendations and a proposed schedule for deployment of that upgrade. If so directed by the Authority, the Contractor shall test and deploy those Software upgrades at all facilities as part of the Annual Maintenance and Support Services.

It is further understood that from time-to-time, pertinent ITS Standards may be modified or new ones issued. If so directed by the Authority, the Contractor shall modify and/or develop the requisite SIs and incorporate them into the Software instances as appropriate, which work will be performed as Net Cost Work.

6. Maintenance of the Software and System Interfaces– System maintenance shall consist of the following:

- a. Maintenance Components

- i. Maintain operational availability of the Software through Scheduled Preventive and Remedial Maintenance.
- ii. Perform Error Correction.
- iii. Maintain a staffed, local maintenance office within 50 miles of the PA-AOC site.
- iv. Provide, install, and configure Software Updates.

- v. Maintain software compatibility with installed versions of installed Third Party software including all connected system software until the Authority notifies the Contractor of its intent to patch or update such Third Party software.
- vi. Ensure the Software works with third-party releases and patches.
- vii. Provide Supplemental Training Classes at least once per year at each facility.
- viii. Update Manuals and Documentation to document any changes to the system or system operation.
- ix. Provide staffed On-Call Tier 2 and Tier 3 Support 24 hours per day, seven (7) days per week, 365 days per year.

b. Maintenance Requirements

Upon certification by the Authority that the System has satisfactorily passed the 30-Day Operational Test and that the Contractor has completed all work as specified in the Detailed Project Plan for a facility, the Contractor shall then provide the maintenance required for the System to perform in accordance with, but not limited to, the following specifications and the Service Levels specified in Section VIII:

i. Maintenance

The following maintenance & support tasks must be performed for the systems upon successful completion of the 30-Day Operational Test at each facility; then under the Maintenance Phase.

- ii. Maintenance and support tasks include all expenses (labor, tools, software, licenses, travel costs, etc.), without additional cost to the Authority, required to perform the following, at a minimum:
 - 1. On-call remedial and scheduled preventive maintenance in order to meet the 99.9 % availability requirements stated herein.
 - 2. Correct defects in the Software, System Interfaces, or any components and configuration within 48 hours of notification.
 - 3. Validate and correct (when necessary) the Software and/or System Interfaces furnished by the Contractor to ensure that they perform in accordance with the specifications of the Contract within ten (10) days after Microsoft and other software providers release patches and updates to the operating system, database and other third-party software that is furnished or used in the System.
 - 4. Certify, validate, correct, update, and make available (when necessary) the Software and/or System Interfaces furnished by the Contractor to ensure that they perform in accordance with the specifications of the Contract within ninety (90) days after third party System software providers (such as Video Management, Vehicle Detection System, etc.) connected to the Software release patches and updates to their system software. Update the

Software within thirty (30) days of the Authority's notification of its intent to install such Third Party system software patches or updates.

5. Maintain a current version of the Software in the Authority Test Lab Environment. All software and System Interface updates shall be installed and tested in the Authority Test Lab Environment prior to installation in the production environment.
6. Provide updated copies of the Software and installation instructions whenever the furnished Software is updated, patched or new versions of the Software are installed, and shall include update to the System in its escrow program, by the Contractor.
7. Provide supplemental training classes as part of the on-going maintenance contract, a minimum of at least once a year at each facility, or when requested by the Authority.
8. Provide staffed On-Call Tiers 2 and 3 Support by telephone during twenty-four (24) hours per day, seven (7) days per week, 365 days per year.

iii. Access to the Software

The Contractor will be permitted access to the Software in the production systems in order to perform its obligations in accordance with the requirements stated herein. If it becomes necessary to obtain physical access to the integration and test or production systems, arrangements will be made through the Technology Department for the Contractor to access the production system under the Authority's supervision. The Contractor may also be permitted limited access to the Software in the production system through the Authority's Remote Access Solution.

iv. Operational Availability

As referenced in Section VIII, the system shall meet the percentages stipulated below, each calendar month for the term of this Contract:

The Software, Databases, and System Interfaces on the servers and workstations:
99.9%

As used in this numbered Clause, "Operational Availability" means the time during any calendar month period the System is Available to Users at all facilities. "Available" means that during any calendar month period, the furnished and installed Software applications and any Contractor furnished equipment perform according to the manufacturers' specifications.

In the event that Operational Availability fails to meet the percentage stipulated herein, damage amounts for unavailability for operation are as specified in Section VIII Service Levels.

v. Maintenance Work

1. The Contractor shall perform any and all maintenance work so that the System meets the Operational Availability requirement of 99.9% and may be operated twenty four (24) hours a day, seven (7) days a week, 365 days per year.
2. The maintenance program shall be performed with all reasonable care to keep the System in a proper, safe, and efficient operating condition capable of correct operation and reporting.
3. The Contractor shall furnish all labor, travel, materials, supplies, parts, equipment, warning signs, other safety devices, and all other things necessary or proper for, or incidental to, such maintenance.
4. The Contractor, at its option, shall repair or replace, within the time(s) stipulated in Section VIII Service Levels, Software, System Interface, or firmware of the System, which become unsuitable for continued use.
5. The maintenance performed by the Contractor shall include, but not be limited to, scheduled Preventive Maintenance, on-call Remedial Maintenance, error correction, Software and System Interface diagnostics and corrections, validation that the Software continues to work (in accordance with the Contract requirements) with manufacturer released patches to third-party software and engineering updates of the System as described below.
6. The Contractor shall submit, to the Authority's Contract Manager for review, a schedule of preventive maintenance activities and a description of preventive maintenance procedures for each software instance within 30 days of the Maintenance Phase Start Date and each anniversary thereof. The Authority's Contract Manager will review the submission, and make comments, within ten (10) working days.
7. In order to meet the Service Level agreements stipulated in this Scope of Work in this Contract, the Contractor shall maintain an adequate number of qualified staff to provide the required technical support.
8. The Contractor's personnel shall report to the Facility Manager or his/her designated representative at the start and completion of each maintenance visit, and said service personnel shall keep the Facility Manager informed of the work performed by them by furnishing him/her with a completed "Service Maintenance Form". Said form shall include, in addition to any

other pertinent data, such data as times of arrival, departure, Software or System Interface downtime duration, and the workers names, and shall notify the Authority's Contract Manager of additional activities which may have to be scheduled for maintenance.

vi. Maintenance Description

The results from all inspections, tests, diagnostics, and corrective actions shall be reported to the Authority's Contract Manager on Authority approved forms.

The maintenance performed by the Contractor shall include, but not be limited to, scheduled Preventive Maintenance, on-call Remedial Maintenance, error correction, and Software and System Interface diagnostics and corrections, validation that the Software continues to work (in accordance with the Contract requirements) with manufacturer released patches to third-party software and engineering updates of the System as described herein.

1. Scheduled Preventive Maintenance

Scheduled Preventive Maintenance shall consist of all actions necessary to inspect, test, diagnose, repair failures, correct System malfunctions and restore System operation to perform in accordance with the manufacturer's stated specification, performance and tolerances.

Scheduled Preventive Maintenance shall include, but not be limited to, all actions necessary to prevent System failures and extend the System's useful life, verify adequate empty disk space available for program usage (e.g., temporary files, logs, etc.), verify log files are saved to removable media and log files are purged on a regular basis, review reports on communications throughput and errors and perform communications end-to-end diagnostics on each communications channel to identify equipment or cabling problems.

2. On-call Remedial Maintenance

On-call Remedial Maintenance shall consist of all unscheduled actions necessary to obtain the Operational Availability, diagnose and correct all System malfunctions and failures and restore the System in accordance with the manufacturers' stated specification, performance and tolerances and the System to perform in accordance with the Contract requirements. The Contractor shall provide a specified telephone number, FAX number and email address at no additional cost to the Authority, which is to be staffed twenty-four (24) hours per day, seven (7) days per week, 365 days per year, to enable the Authority to report errors and malfunctions to the System.

a. In response to on call remedial maintenance where failover has failed and the Software system is unavailable to the user community, the

Contractor shall contact the Facility Manager or his/her designee within 30 minutes of initial notification in order to coordinate the repair work. Then, the Contractor shall send its personnel who are fully familiar with the System and its maintenance requirements, to the Authority property where System components are located in response to notification of a System malfunction or error, and said personnel shall arrive at the premises after receipt of the telephone call and report in to the Facility Manager or his/her authorized representatives, repair the malfunction and restore System operation within the time(s) stipulated in Section VIII Service Levels.

- b. In response to on-call remedial maintenance where failover was successful and the Software system is available to the user community, the Contractor shall contact the Facility Manager or designee and correct the situation in accordance with Section VIII Service Levels.
- c. Within twenty-four (24) hours of each site visit for a reported on-call Remedial Maintenance problem, the Contractor shall provide written documentation of the reported problem and all actions performed related to the maintenance call in a computer-readable format to the Facility Manager.

c. Correction

The Authority will notify the Contractor via the 24-hour telephone or fax number or email, described above, when the System does not perform in accordance with the Specifications stipulated in the Contract due to error in the Software, System Interfaces, or any modifications thereto. The Contractor shall correct any such error as identified by the Authority or through the Contractor's investigation of the reported error(s). Errors shall include but not be limited to flaws in operations and errors due to flaws in the design and coding of the System and/or Interfaces.

The Contractor shall dispatch trained personnel to diagnose, debug, and correct all malfunctions required for the System to perform in accordance with the Specifications within the time(s) stipulated herein. The Contractor shall provide documentation in machine-readable format, if any, relating to the error correction. The Contractor in an off-line test environment shall test the corrected Software. The Contractor shall then prepare a test report and submit it to the Authority for review and approval before the corrected Software is installed into the System. Such corrections to the Software and/or System Interfaces shall be provided at no additional cost to the Authority.

The Contractor shall dispatch Trained Personnel and complete such testing, validation and correction to ensure that the Software performs in accordance with the

Specifications stipulated in the Contract, with the released patches and updates that Microsoft and other software providers used in the System release patches and updates to fix software defects or security vulnerabilities to the operating system, database and other third-party software that is furnished or used in the System.

The Contractor shall, at no additional cost to the Authority, certify, validate, correct, and update (when necessary) the Software furnished by the Contractor to ensure that it performs in accordance with the Specifications of the Contract when System software providers (such as Video Management, etc.) connected to the Software release patches and updates to their systems, and the Authority has notified the Contractor of its intent to install such patches or updates.

d. Upgrades and Enhancements

The Contractor shall notify the Authority's Contract Manager whenever upgrades and/or enhancements to the Software and/or System Interfaces provided under the Contract or third party software becomes available. The Contractor shall also provide the Authority's Contract Manager with an analysis of the potential effects of such upgrades/enhancements on the System. This analysis shall include at a minimum the following:

- i. Compatibility of the Software with the new operating system or third-party software.
- ii. Potential increases or decreases in operating System performance.
- iii. The availability of product support for the current (older) version of the operating system or third party software.
- iv. The testing required ensuring that the upgrade will perform as expected
- v. The cost of the software upgrade, including any tasks which may be associated with the upgrade, shall be at no additional cost to the Authority.

The Authority's Contract Manager will then determine whether or not to approve the upgrade. If the Authority's Contract Manager selects the upgrade, the Contractor shall perform the recommended testing, prepare the test report, and perform the upgrade on the System, at no additional cost to the Authority .

e. Location Conditions and Procedures

- i. Maintenance shall be performed by qualified personnel, who shall be responsible to keep the Software in proper operating condition. Any employee of the Contractor, or its subcontractors, deemed by the Authority's Contract Manager or Facility Manager not qualified to perform the work hereunder shall be immediately removed from the location and replaced by the Contractor upon request by the Authority.

- ii. The Authority's Facility Manager will, whenever possible, provide such cooperation as may be necessary to permit entry into locked areas. The Contractor shall give a minimum of forty-eight (48) hours notice of its intention to perform work (other than On-call Remedial Maintenance) under this Contract to the Authority's Facility Manager or his designated representative in order that any necessary arrangements may be made by the Authority. This notice shall include the Contractor's expected hours of arrival and departure, areas to be serviced, and the number of workers that will be working.
- iii. The Authority will not furnish any free facility use passes or parking spaces for the Contractor. In addition, parking at any location may not be available and the Authority makes no guarantee that parking at the location will be provided to the Contractor.
- iv. Vehicles of the Contractor, employees of the Contractor, subcontractors, materialmen, or others over whom the Contractor has control shall be subject to the following:
 - 1. Vehicles shall not be permitted to park in or on Authority property, except for the area of Work during the times when the Work is being performed, subject to the conditions stated below and elsewhere herein.
 - 2. All vehicles entering the Work site shall be required to display a Placard issued by the Authority. Submit all Placard applications, including vehicle registration documentation, to the Facility Manager a minimum of five business days in advance of any vehicle entering the Work site. Placards must be renewed by the Contractor on a quarterly basis.
 - 3. All vehicles entering the Work site shall be registered commercial vehicles with commercial license plates and shall have permanently affixed company identification on the exterior of the vehicle.
 - 4. There shall be no parking of personal vehicles, nor parking of non-Placarded Contractor vehicles, anywhere on Authority property. The Contractor shall arrange for any necessary transportation for all personnel to the Work site. Vehicles used for transportation shall not be parked on Authority property.
 - 5. All vehicles shall be required to pay the appropriate tolls for each passage or crossing of Authority facilities, or parking at Authority lots.
- v. At the time the Contractor is carrying out its operations, there may be other persons working in the vicinity. The Contractor shall so conduct its operations as to work in harmony and not endanger, interfere with or delay the operations of others, all to the best interests of the Authority and others, as may be directed by the Facility Manager.

- vi. The Contractor shall provide qualified employees with identification badges approved by the Facility Manager. Such badges shall be worn in a conspicuous and clearly visible position by all employees of the Contractor whenever engaged at the location. All Contractor personnel shall be approved by the Facility Manager.
- vii. The Contractor shall observe and obey (and compel its subcontractors, officers and employees and those doing business with it to observe and obey) the rules and regulations of the Authority and such further rules and regulations which may from time-to-time during the effective term of this Contract be promulgated by the Authority or other authorities, commissions, or jurisdictions for reasons of safety, health, preservation of property or maintenance of a good and orderly appearance of the work areas and property of the location.

f. Maintenance Reporting

The Contractor shall utilize a maintenance management system which tracks preventive and corrective maintenance on all system components. The system shall provide periodic reports for preventive and corrective maintenance activity. The system shall report on the preventive maintenance schedule of system components, preventive maintenance activity that has been performed over prior period(s), a schedule of upcoming activity, and any deviations from the established preventive maintenance program. Reports on corrective maintenance activity shall include a summary of each call including: reason for the call, date and time received, time responded at the facility, total time to correct the problem and return the components to service, corrective measures taken, etc. The system shall also identify and produce reports of trends such as failures of particular components, failures at specific locations, etc.

g. Supplemental Training

The Contractor shall provide supplemental training to the Authority staff in the form of one Software Administrator Level training class once a year during each maintenance year. The time and place of the training class shall be coordinated in advance with the Authority's Contract Manager. The training material shall be updated to reflect the then currently installed Software.

7. Application Capacity Management and Performance Monitoring

The Contractor shall be responsible for monitoring the application capacity and performance to ensure that performance and response meet the operational needs of the users. The Contractor shall take all necessary measures to ensure the continued effective operation of the application through accepted prudent industry capacity management and performance monitoring procedures, including recommending corrective actions to correct capacity and performance inadequacies. Such recommendations shall be made only after consultation with TD representatives.

The scope of the application capacity management and performance monitoring shall include, but not be limited to, the activities identified in this Section. Monthly reporting on these areas shall be provided to the Authority's Contract Manager.

a. Capacity Management

- i. **Maintaining Records:** The Contractor shall maintain records on application performance and resource usage, user response time, etc. adequate to project needed upgrades to hardware and software based on current performance and expected growth.
- ii. **Forecasting Upgrade Needs:** The Contractor shall maintain communication with the Authority's Contract Manager in regard to the Authority's plans for system expansion or modification, which will impact on system capacity or performance.
- iii. **Tracking Resource Usage:** The Contractor shall track such items as database/file sizes, and concurrent users to ensure adequate resources shall be available for the foreseeable future, and to take preventative action to minimize application failure due to insufficient resource levels.

b. Performance Monitoring

- i. **Troubleshooting:** The Contractor shall investigate and diagnose system problems that result in application system performance degradation and take steps to remedy the problem.
- ii. **Maintaining Proper Allocation of Resources:** The Contractor shall monitor CPU, memory, application and database servers, file distribution on direct access storage devices, network performance, and, as warranted, make recommendations to ensure adequate system performance.
- iii. **Maintaining Data Structures:** The Contractor shall defragment files and perform database "tuning" on a scheduled and/or as-needed basis.

8. System Change Management

The Contractor shall be responsible for ensuring that all changes to the application and/or System Interfaces are accomplished in a controlled manner. The Contractor shall keep the Authority's Contract Manager apprised of the changes requested. The Authority's Contract Manager shall be the sole authorized approver of changes into Production. All such changes shall be reviewed with the Authority's Contract Manager at a regularly scheduled change prioritization meeting. The Contractor shall be responsible for ensuring that all application changes are properly authorized, tested, and documented prior to implementation in the production environment, using a structured Application Management Methodology acceptable to the Authority. The Contractor shall adhere to the Change Management processes and controls that are currently in place. Appropriate backout/reversal procedures shall be in place and successfully tested prior to migration to production.

2/8/16

All changes to the application, whether initiated at the request of the Authority or delivered by Contractors, must be logged, tracked, documented and approved by the Authority's Contract Manager.

Narrative documents describing the change and the business reason for the change must be prepared and stored in a central repository.

Test plans shall be prepared by the Contractor. The test results must be approved by the Authority's IT support team and then by the customer, prior to implementation of any change.

The scope of the Change Management portion of the Work shall include, but not be limited to the activities identified below:

- a. Verification and Control of Software:** The Contractor shall submit evidence that no unauthorized software has been introduced onto the system. The submission will be reviewed by the Authority and verified that no unauthorized changes have been made. The Authority's Change Control procedures shall be used as dictated by the Authority's Standards and Guidelines (please refer to "Attachment N –Standards and Guidelines for Port Authority Technology").
- b. Inform Management of New Software Options for Third Party Software:** The Contractor shall maintain contact with the third party software vendor(s) (e.g., Microsoft, etc.) to stay aware of software upgrades and fixes and hot packs, and deliver to the Authority a plan and schedule for recommended implementation of these upgrades and fixes and hot packs.
- c. Establish and Maintain a Segregated Test and Quality Assurance Environment:** The Contractor shall maintain a segregated Test and Quality Assurance environment(s) isolated from the production environment for testing of all changes to the Software prior to introduction to the production environment.
- d. Establish and Maintain a Training Environment:** The Contractor shall maintain a segregated training environment and manage the refresh strategy as needed.
- e. Controlling Software Migrations:** The Contractor shall maintain and enforce procedures to ensure only approved and non-conflicting changes are implemented by ensuring that:
 - i. modification request forms have been received for all changes to be made;
 - ii. multiple changes to the same module are coordinated;
 - iii. there is synchronization of changes to all modules affected by a modification to a data element or other factors that are changed simultaneously;
 - iv. migration of modules is controlled through the test and implementation cycle;
 - v. new application versions are thoroughly tested prior to use on production system;
 - vi. new application versions are thoroughly documented, in accordance with, at a minimum, Authority standards; and

- vii. all changes are coordinated with any and all business owners and/or third party software/hardware vendors as required.
- f. Scheduling: The Contractor's implementation of changes shall be scheduled to minimize downtime and avoid the Monday to Friday time period, utilizing scheduled weekend and night maintenance windows accordingly.
- g. Maintaining Prior Versions of Software: The Contractor shall exercise control over Software versions, ensuring the proper version of Software is migrated and that prior versions are available for roll back in the event of an emergency. The Software must be downwardly compatible to the last major version.
- h. Testing: The Contractor shall maintain a test bed of known results to verify the integrity of new Software versions, including a retest of the current system after modifications are made.
- i. The Contractor shall be required to participate in TD weekly Change Management Meetings.

9. Software Documentation

The Contractor shall maintain a documentation library containing all hardcopy and computer readable documentation for software/interfaces developed during ongoing maintenance. Similar documentation is required to be maintained for operating system, database and hardware related efforts. The Contractor shall be responsible for ensuring that all documentation needed for the continued operation and management of the system is accurate and available and is in compliance with, at a minimum, a structured Application Management Methodology agreeable to the Authority.

- All documentation remains the property of the Authority.
- All physical documentation must be maintained on site at the Authority.

The scope of the system documentation shall include, but not be limited to, the activities identified below:

- a. Maintain a Documentation Library/Repository: The Contractor shall maintain a Document Library/Repository (at a network location specified by the Authority) containing all documentation material (technical and functional) for software, standards and procedure manuals and obtaining or producing any needed documentation. All material in, or obtained for, the library shall be the property of the Authority. The Contractor shall ensure that the documentation meets the standards as set in the Contractor's structured Application Management Methodology acceptable to the Authority. Access to electronic versions of documentation shall be controlled at the user ID and file structure level. Documentation is to be kept current and be checked and approved by the Authority before a case is closed or a change implemented
- b. Maintain Application System Documentation: The Contractor shall maintain a run book for Authority's Computer Operations Division that highlights and tracks all information required

for scheduling, interfaces, jobs, etc., as well as, a functional specifications document describing the business purpose of the system and a high level description of the processes and report; a design specifications document detailing the technical solution to the business function described in the functional design document described above; and maintain program documentation including narrative descriptions, specifications, code listings, data layouts, IPO (Input, Processing, Output) charges, flow charts etc.

- c. **Maintain Test Plans:** The Contractor shall maintain test plans and procedures for retesting the system after modifications to the Software. The Contractor shall also maintain a file of all test results in accordance with the documentation standards referenced above and evaluations of results along with any recommendations arising out of that testing. All test plans and related files and data shall be the property of the Authority. Test plan documentation shall include:
- i. **Unit Testing –** Perform, create and maintain unit test plans to verify the functioning of the new system component and that it satisfies the requirements. These should be available for use by the Authority in Operational testing.
 - ii. **System/Integration Testing –** Perform, create and maintain test plans to test the entire system with the new component installed to verify the integrity of the system as a whole and to determine that the intended purpose of the new component is achieved. These shall be available for use by the Authority in Operational testing.
 - iii. **Operational Testing –** Create and maintain test plans to verify the functioning of the new component in the production environment for a specified period prior to the final acceptance tests.

10. Business Continuity Support

The Contractor shall work with the Authority's Contract Manager and appropriate user departments to participate in activities associated with the Authority's Business Continuity Plan. The Contractor shall be primarily responsible for the portion of the plan concerned with providing continuing support for the application. The Contractor will participate in any test of the Business Continuity Plan scheduled by the Authority, typically, quarterly. The Contractor shall be responsible for installation of the Software and all requisite SIs at the Disaster Recovery Center.

11. Security

The Audit Security Checklist is made up of the following two (2) documents:

- Controls Requirement Contract Checklist
- Disaster Recovery Plan Checklist

Please refer to "Attachment M" for details.

Physical security is the responsibility of Authority staff. The Contractor, however, shall help ensure that the checklist items are being followed and assist Authority staff in improving and complying with these items. This also includes notification to the Authority's Contract Manager of related issues.

The Disaster Recovery Plan Checklist shall also be followed by the Contractor. It should be noted, however, that a Disaster Recovery Plan will be developed for the system. See "Disaster Recovery Support" above. The Contractor shall update and provide guidance for updating and improving the plan. In addition, Contractor staff shall assist in testing the plan, maintaining currency and documenting test results.

The Contractor shall maintain the system to conform to the Authority Audit Department's Control Guidelines included in Attachment M and satisfy the checklists therein.

b. Infrastructure Support Services

Infrastructure Support Services is the grouping of the non-application based system support components, such as:

- Hardware Components
- Database Components
- Operating System Components

1. Support Functions

a. Infrastructure Hardware and Software

- i. Database Support and Administration
- ii. System Software/Hardware Support

b. The Contractor shall be responsible for developing scripts to incorporate any required desktop changes as a result of a release or installation upgrade and testing of this software before deployment to the user community. The Contractor also shall be responsible for coordination with the Authority's Systems Administrator to ensure that the Software functionality remains during upgrades in OS, security patches, and standard image and Secure Login.

2. Troubleshooting and Problem Management and Resolution

The Contractor will be responsible for logging, documenting, tracking and resolving production problems while ensuring ongoing data integrity with any and all interfaces and/or systems interfacing and/or interacting with the Software.

The Contractor shall perform correction of all production problems related to the application's Database and/or Operating System environments. The Contractor shall investigate and diagnose system problems resulting in unsatisfactory application system performance and take appropriate Authority approved steps to remedy the problem.

Narrative documents describing the problem and resolution must be prepared and stored in the Document Repository referenced above.

The Contractor shall support the Authority with reports and analysis of Software and interface functionality.

The Contractor shall provide break/fix Software support as necessary.

The Contractor shall be responsible for correction of all production problems related to the deployment of the Software.

The Contractor shall serve as a resource for Authority staff as related to application system functionality. This shall include, but not be limited to:

- a. Providing technical support to Authority staff and/or vendors relative to the applications support
- b. Researching and taking corrective action on reported software malfunctions
- c. Participating in internal and external audits as directed by the Authority's Contract Manager
- d. Assisting in the development of training materials, as necessary.

Twenty-four (24) hour on call and support availability for resolution of problems in accordance with the Service Level Agreements set forth in Section VIII is required.

3. Tuning

The Contractor shall be responsible for all functions related to the monitoring and tuning of the database and/or Operating System environments, standard queries, indexing and similar tasks to ensure an efficient and effective system for the users.

4. Releases

The Contractor shall perform any/all adjustments, installations, configurations and implementations required for new releases of Database and/or Operating System environments, system software and/or hardware equipment end of life cycles. All modifications shall be performed in lower tiers and migrated to production. The Contractor shall monitor, evaluate and apply all security or other related patches in a manner consistent with Authority procedures. Security alerts shall be given a high priority.

5. System Monitoring

The Contractor shall provide system monitoring, security and reporting in accordance with industry best practices of Database and/or Operating System environments.

6. System Logs

The Contractor shall regularly review the Database and/or Operating System environment logs and take corrective action as necessary. The process and follow-ups must be auditable by the Authority.

7. Systems Capacity Management and Performance Monitoring

The Contractor shall be responsible for monitoring the system's capacity and performance to ensure that performance and response meet the operational needs of the users. The Contractor shall take all necessary measures to ensure the continued effective operation of the application through prudent industry capacity management and performance monitoring procedures, including recommending corrective actions to correct capacity and performance inadequacies.

The scope of the system's capacity management and performance monitoring shall include, but not be limited to, the activities identified in this section. Monthly reporting on these areas shall be provided to the Authority's Contract Manager.

a. Capacity Management

- i. **Maintaining Records:** The Contractor shall maintain records on systems' performance and resource usage, user response time, etc., adequate to project need upgrades to hardware and software based on current performance and expected growth.
- ii. **Forecasting Upgrade Needs:** The Contractor shall maintain communication with the Authority's Contract Manager in regard to the Authority's plans for system expansion or modification, which will impact on system capacity or performance.
- iii. **Tracking Resource Usage:** The Contractor shall track such items as database/file sizes, and concurrent users to ensure adequate resources shall be available for the foreseeable future, and to take preventative action to minimize application failure due to insufficient resource levels.

b. Performance Monitoring

- i. **Troubleshooting:** The Contractor shall investigate and diagnose system problems that result in application system performance degradation and take steps to remedy the problem.
- ii. **Maintaining Proper Allocation of Resources:** The Contractor shall monitor CPU, memory, application and database servers, file distribution on direct access storage devices and, as warranted, make recommendations and, after securing the Authority's concurrence, implement these recommendations to maintain adequate system performance.

- iii. **Maintaining Data Structures:** The Contractor shall defragment files and purge/reorganize databases on a scheduled and/or as needed basis.

8. Systems Change Management

The Contractor shall be responsible for ensuring that all changes to the database and/or server hardware or operating system platforms occur in a controlled manner. The Contractor shall keep the Authority's Contract Manager apprised of the changes requested. The Authority's Contract Manager will be the only authorized approver of changes into production. All such changes shall be reviewed with the Business Owners and the Authority's Contract Manager at regularly scheduled change prioritization meetings. The Contractor shall be responsible for determining that all system changes are properly authorized, tested and documented prior to implementation in the production environment, using a structured Application Management Methodology acceptable to the Authority. The Contractor shall adhere to the Change Management processes and controls that are currently in place. Appropriate backout/reversal procedures shall be in place and successfully tested prior to migration to production.

The scope of the Change Management portion shall include, but not be limited to the activities identified below:

- a. **Verification and Control of Software:** The Contractor shall verify that no unauthorized software has been introduced. The versions of the Authority authorized software shall be checked to verify that no unauthorized changes have been made. The Authority's Change Control procedures shall be used as dictated by the Authority's Standards and Guidelines (please refer to "Attachment N –Standards and Guidelines for Port Authority Technology").
- b. **Inform Management of New Hardware and/or Software Options for Third Party Software:** The Contractor shall maintain contact with the third party hardware and software vendor(s) to stay aware of upgrades, fixes and hot packs, and deliver to the Authority a plan and schedule for recommended implementation of these upgrades and fixes and hot packs.
- c. **Establish and Maintain a Segregated Test and Quality Assurance Environment:** The Contractor shall maintain a segregated Test and Quality Assurance environment(s) isolated from the production environment for testing of all changes to the Software prior to introduction to the production environment. These environments shall have accessibility to the Hardware Testing Laboratory where ITS devices will be tested.
- d. **Establish and Maintain a Training Environment:** The Contractor shall maintain a segregated training environment and manage the master client, training IDs and the client refresh strategy as needed.
- e. **Controlling Migrations:** The Contractor shall maintain and enforce procedures to ensure only approved and non-conflicting changes are implemented by ensuring that:

- i. modification request forms have been received for all changes to be made;
 - ii. migration is controlled through the test and implementation cycle;
 - iii. new application versions are thoroughly tested prior to use on production system;
 - iv. new application versions are thoroughly documented, in accordance with, at a minimum, Authority standards; and
 - v. all changes are coordinated with any and all business owners and/or third party software/hardware vendors as required.
- f.** Scheduling: The Contractor’s implementation of changes shall be scheduled to minimize downtime and avoid the Monday to Friday time period, utilizing scheduled night and weekend maintenance windows accordingly.
- g.** Maintaining Prior Versions of Software: The Contractor shall exercise control over versions of the Software, ensuring the proper version of the Software is migrated and that prior versions are available for roll back in the event of an emergency.
- h.** Testing: The Contractor shall maintain a test bed of transactions and known results to verify the integrity of new versions of the Software, including a retest of the current system after modifications are made. The test bed shall be updated to include test data for all new conditions arising out of maintenance or enhancement of the system.

9. Business Continuity Support

The Contractor shall work with the Authority's Contract Manager and appropriate user departments to participate in activities associated with the Authority’s Business Continuity Plan. The Contractor shall be primarily responsible for the portion of the plan concerned with providing continuing support for the application. The Contractor will participate in any test of the Business Continuity Plan scheduled by the Authority, typically, quarterly.

c. Miscellaneous

The Contractor shall be expected to make recommendations for optimizing the Software with changes to business processes, expanded use of Software functionality and configuration changes, and/or other industry best practices. This may also include “bolt-on” third party products complementary to the Software for functions such as data mining and reporting.

D. Option Periods (Years 5 and 6)

During the two one-year Option Periods, the Contractor shall be responsible for maintenance, support, and upgrading of the installed instances of the Software and the System Interfaces for a fixed annual fee. The Authority may, at its sole discretion, direct the Contractor to perform Net Cost Work for enhancements to the Software, development of SIs to enable the Software to monitor and control newly acquired ITS assets, or any other task deemed necessary to modify or enhance the capabilities of the Software.

The Contractor will be requested to provide all services required to develop and test SIs to facilitate communications between instances of the Software and newly deployed ITS assets for which SIs have not already been developed. SIs shall conform to the Authority's *ITS Design Guidelines* (See Attachment O), pertinent requirements in Appendix 1, and any new requirements that may be issued by the Authority. All new equipment deployed by the Authority during the Option Periods will adhere to the Authority's *Intelligent Transportation Systems (ITS), General Requirements* and other applicable Authority Requirements for specific ITS components which stipulate conformance with National Transportation Communications for ITS Protocol (NTCIP) Standards (see www.ntcip.org). This will facilitate the use of identical SIs (to be developed by the Contractor) at all Authority installations where the same equipment is deployed. Consequently, one set of SIs shall be developed for a particular ITS asset type and used at all Authority facilities. The Contractor will be compensated for the development of each unique SI. That interface shall then be incorporated into other facility instances of the Software as appropriate at no additional cost to the Authority. The SIs shall become an integral part of the Software for which the Contractor shall grant the Authority a perpetual use license.

For Net Cost Work throughout the term of this Contract, the Authority will issue a Statement of Work to the Contractor that will describe the requested services and deliverables. The Contractor shall respond within the time period noted in the Statement of Work with its technical approach (if requested), a completion schedule, and a firm fixed-price proposal for the deliverables. The price proposal shall include a breakdown of estimated hours (and costs) for each sub-task. Applicable hourly rates shall be those included in the Proposer's Cost Proposal for this Contract and shall be adjusted in accordance with the Contract for the year in which the work is performed. It is important to note that all personnel assigned to such work shall be assigned to one of the Key Staff classifications provided by the Contractor in its response to this RFP. Key Staff identified to work under a Net Cost Work Proposal who are not qualified to be included in one of the classifications provided in the Proposer's response to this RFP will not be eligible to perform the work.

The Authority may then, at its sole discretion, direct the Contractor to perform the Net Cost Work. The Authority will identify the specific deliverables that shall be furnished by the Contractor for the agreed-upon lump sum amount(s) as determined above and specified therein.

VII. ENHANCEMENTS

The core tasks discussed above are designed to keep the Authority's System free from bugs, operational, and up to date with all Software, System Interface, and OS patches and upgrades. However, it is envisioned that the Authority may require, at any point during the Contract, additional services (sometimes known as enhancements or Optional Project Work) to expand the functionality of the Software.

Specific enhancements have not as yet been identified but could include, for example:

- Development of new Center-to-Field System Interfaces for the first time deployment of a particular ITS asset;
- Enhancements to the Software to increase its functionality and value to the Authority;
- Development of new Center-to-Center System Interfaces to either modify the data exchanged between Centers or to add new regional partners;
- Development of analytical tools to assist the Authority with the automatic computation of Performance Metrics;
- Development of System Interfaces to exchange data with other systems that the Authority may acquire during the term of this Contract.

Any enhancements will be considered Net Cost Work, which will be centrally managed through the Authority's Contract Manager and will follow a Contractor supplied tracking process that has been approved by the Authority. The essence of this process shall be the following:

- a. An enhancement request is documented by the Authority. The Authority's Contract Manager will review and forward to the Contractor for scoping, estimating and scheduling. Unless otherwise agreed, the Contractor shall provide a written estimate of the results of their analysis for discussion and approval by the Authority within ten (10) business days. The Contractor shall use as the basis for costing the rates provided in the Cost Proposal accepted by the Authority and which is a part of the Contract. While the Contractor is encouraged to provide more competitive rates to take advantage of economies of scale, under no circumstances can the hourly rate be higher than that quoted in accepted the Cost Proposal.
- b. Unless otherwise specified by the Authority, approved cost proposals for enhancements are to be considered fixed price deliverables-based and payment will be made in accordance with project-specific deliverables. In special circumstances, the Authority may negotiate interim deliverable-based payment milestones.
- c. The Authority will review and, when satisfied, formally approve the cost estimate for the enhancement, as well as the scope of work. At that time, unless otherwise agreed, the Contractor will have fifteen (15) business days to secure the resources quoted and begin work, in accordance with the agreed-upon scope of work.
- d. The Contractor is strongly advised to remain competitive in cost, quality and schedule throughout the course of the Contract when providing enhancement estimates.

VIII. SERVICE LEVELS

The Contractor shall respond to all reported problems associated with the Software and System Interfaces in a timely fashion. The Contractor shall be responsible for meeting the service levels stated below.

- A. Notification to the Contractor may take the form of an e-mail, telephone call, Short Message Service (SMS or text messages) or any other mutually agreeable form of communication. When the communication is initiated by the Authority, the time in which a response or resolution is required is considered to have started.

- B. Authority staff and Contractor staff will attempt to agree to the severity classification when a problem arises, but the Authority's Contract Manager will have the authority to make the final determination regarding the severity classification when a mutual agreement cannot be reached by staff, or when the priority needs to be escalated.

Problem Severities and Time to Respond/Resolve

Problem Severity	Example (not all inclusive)	Required Response Time from Notification	Required Resolution Time from Notification
High: Traffic Management at a Facility is not possible.	Both the facility and PA-AOC instances either fail or are not properly operating.	30 Minutes	4 Hours (Inclusive of 30-minute notification requirement)
Medium: The problem is not time-critical, but it adversely impacts Facility Operations	Either the Facility Software instance is inoperable or System Interfaces are not working properly	2 Hours	24 hours (Inclusive of 2- hour notification requirement)
Low: The problem is non-critical and does not adversely impact Facility Operations	Most reporting issues and some Center-to-Center communications issues	24 hours	Five (5) Business Days (Inclusive of 24- hour notification requirement)

Availability

The Application must be fully and accurately functioning 24 x 7 x 365, except for scheduled maintenance windows. Maintenance windows will be established by the Authority after consultation with the Contractor. When necessary, exceptions may be required in which the Contractor shall work with the Authority to accommodate such contingencies.

All instances of the application must provide 99.9% availability, excluding the maintenance window. The service level specified will be monitored by the Authority.

The System must be fully and accurately functioning during scheduled hours of operations, (as such may periodically be revised by the Authority). This includes but is not limited to:

- Monitoring and controlling Legacy ITS assets by facility instances of the Software;
- Monitoring and controlling newly installed ITS assets by facility instances of the Software;

2/8/16

- Full monitoring and control of facility ITS subsystems, where appropriate;
- Full monitoring and control of all facility ITS assets and subsystems from the PA-AOC instance;
- Continuously recording and archiving all pertinent data at the NOC;
- Providing automated information regarding facility conditions to the PA-AOC, other Authority facilities, and regional transportation partners as originally configured;
- Receiving, processing, and synthesizing strategic information from regional partners' ATMS systems;
- Executing appropriate facility Response Plans by facility Software instances when corresponding Scenarios occur;
- Executing appropriate facility Response Plans by PA-AOC Software instance when corresponding Scenarios occur at any facility;
- Switching monitoring and control functions for any facility to the PA-AOC when protocols warrant;
- Automatically accumulating data from each facility at the NOC for development and computation of performance metrics as required;
- Replication of the NOC Database to an offsite Reporting Database instance.

The Contractor's obligations are to perform all work at the service levels specified in this Contract. The Contractor guarantees that it can and will complete performance under this Contract at the levels stipulated. Inasmuch as the damage and loss to the Authority which will result from the Contractor's failure to perform at these levels will include items of loss whose amount will be incapable or very difficult to accurately determine, the damages to the Authority for Contractor's non-performance will be liquidated according to the following table.

Service	Service Level	Resulting Liquidated Damages for Non-Performance
Monitoring and Control of ITS assets at each facility	99.9% The Contractor is not responsible for system outages attributable to hardware failures beyond its control.	\$5,000 per day after the allowable 48 hour repair time window (see VI.C.6.b. Maintenance Requirements).
On-line availability of the production server at the NOC, measured monthly.	99.9% The Contractor is not responsible for system outages attributable to hardware failure beyond their control.	\$100 per hour for each hour below the percentage target.
Inability to Communicate between Centers in accordance with the Requirements	Continuously	\$1,000 on the first day of outage and \$2,000/day each day thereafter
Problem response and resolution	<p>High – 30-minute response with 4-hour resolution (or workaround acceptable to the Authority)</p> <p>Medium – 2-hour response with 24-hour resolution (or workaround acceptable to the Authority)</p> <p>Low – 24-hour response with five (5) business day resolution (or workaround acceptable to the Authority)</p>	<p>\$500 per incident for each hour or part thereof over the specified resolution time</p> <p>\$3,000 per incident for each 24 hours over the specified resolution time</p> <p>\$1,000 per incident for each 24 hours over the specified resolution time</p>
Patch management	<p>All critical patches (Operating System, Database) as defined in advance by the Authority and the applicable Contractor must be tested and applied through the standard migration path to production environment within ten (10) business days from either release or, where applicable, certification by the Application Contractor.</p> <p>All other non-application patches must be tested and applied through the standard migration paths thirty days from either release or where applicable, certification by the Application Contractor</p>	<p>\$500 per day per patch for the first five (5) business days implementation is delayed; \$1,000 per day per patch thereafter.</p> <p>\$500 per day per patch for each day in excess of thirty days.</p>

Appendix 1 - Requirements

Requirements are categorized as: Fundamental, Project Management, Performance, Data and Database, Interface, Human-Machine Interface, and Functional Requirements. Functional Requirements are further broken down into the following sub-categories: General, Dynamic Message Signs (DMS), Closed Circuit TV (CCTV), Vehicle Detection Systems (VDS), Incident Management and Response, and ITS Asset Monitoring and Management. Each requirement is designated as: Mandatory (M) or Necessary (N) as follows:

1. **Mandatory** – The project requirements defined in this RFP, denoted as "Mandatory," are the requirements that must be met by each Proposer in order to be initially deemed technically responsive to the RFP during the evaluation phase. The Proposer **must** meet these requirements. Mandatory requirements are evaluated as either pass or fail (depending upon the Proposer supplied response). If the Proposer indicates that the requirement cannot be met, the Proposal will be deemed non-responsive and afforded no further consideration.
2. **Necessary** – the requirement is essential to fulfilling the Contract. The Authority will evaluate and document the degree of responsiveness of the Proposer's response to requirements labeled within this RFP as "Necessary." The Proposer shall indicate whether the requirements will be met out-of-the-box, via configuration, or via customization, defined as follows:
 - a. Out-of-the-Box (Commercial Off The Shelf or COTS) – The software fulfills the requirement with no need for configuration or customization.
 - b. Configuration – The requirement will be met via configurations which will be stored in the database and implemented through the application's Graphical User Interface. This response indicates that no programming code changes will be required to fulfill the requirement.
 - c. Customization – The requirement can only be met via changes to the programming code.

Since the Authority is seeking a COTS solution, it will favor solutions that have minimal software customization needs.

The Contractor shall complete the spreadsheet which accompanies this RFP by placing an "X" in the appropriate column(s) for each Requirement. For Fundamental and Project Management Requirements, a "Y" or "N" shall be placed in the appropriate column (yes or no) to indicate ability to comply with those Mandatory Requirements. For all other Requirements, the Contractor shall indicate whether the requirements will be met (Y or N) and, if so, how: out-of-the-box, via configuration, or via customization and shall so indicate with an "X" in the appropriate column. If the Proposer does not provide a response for a Necessary Requirement, it will be assumed that the Requirement cannot be met. If the Proposer indicates that the requirement will be met but does not indicate the compliance method, it will be assumed that software customization is required.

Fundamental Requirements

Fundamental Requirements are the technical requirements that the Software **must** meet. Thus, they are all designated as mandatory requirements (M). For these requirements, the Proposer shall mark a "Y" or "N" in the appropriate column in the spreadsheet provided by the Authority, which must be submitted as part of the response.

ID	Title	Fundamental Requirement Description	Need Mandatory	Complies Yes or No
F-1	High Availability	Each instance of the Software shall be available 24 x 7 x 365 and facilitate automatic failover.	M	
F-2	Redundancy	There shall be redundant central servers for the Software with automatic failover. The servers will be supplied by TD. TD will make the determination as to whether they will be physical or virtual servers. The Contractor shall recommend to the Authority the manner in which redundancy is to be achieved in the documentation of Hardware Recommendations for Servers (see PM-1).	M	
F-3	Secure Access	The Software shall utilize active directory credentials to provide secure access for all approved users.	M	
F-4	Browser-based Access	The Software shall be accessible via the standard browser as stipulated in the Standards and Guidelines for Port Authority Technology.	M	
F-5	Control of Legacy Assets	The Software shall have the capability to monitor and control legacy assets at all facilities.	M	
F6	Database	The Software shall utilize a Microsoft SQL Server Database pursuant to Standards and Guidelines for Port Authority Technology. <i>Proprietary Databases are unacceptable.</i>	M	
F-7	National Transportation Communications for ITS Protocol (NTCIP) Center-to-Field (C2F) Conformance	The Software shall be conformant with the latest NTCIP C2F Standards for each equipment type as shown in the Inventory List (Attachment E, Appendix 3).	M	
F-8	Traffic Management Data Dictionary (TMDD) Standard version 3.03 Center-to-Center (C2C) Conformance	The Software shall be conformant with version 3.03 (or most current version as of the award date) of the TMDD Standard. User Needs to be incorporated in the SI are referenced in Attachment E, Appendix 2. The PA-AOC shall provide real-time situational awareness to all Authority facilities.	M	
F-9	Compliance with Agency Standards and Guidelines	The Software shall fully comply with current Standards and Guidelines for Port Authority Technology.	M	
F-10	Scalable	The Software shall be able to monitor and control up to 2000 Dynamic Message Signs (DMS), 3000 Vehicle Detection Stations (VDS), 500 Lane Use Control Signals (LUCS), 500 Variable Speed Limit Signs (VSLs), 200 Travel Time stations, and 2000 CCTV Cameras.	M	

ID	Title	Fundamental Requirement Description	Need Mandatory	Complies Yes or No
F-11	Real-time	The Software shall be able to collect, parse, filter, calculate and analyze real-time data from field devices and other sources and display on DMS.	M	
F-12	Interoperability	The PA-AOC installation shall be able to monitor and control assets at any facility if conditions warrant. In a worst case situation, all field assets shall be able to be controlled from the primary or backup PA-AOC.	M	
F-13	Intra-Agency (Inter-Facility) Coordination	The PA-AOC installation shall automatically provide situational awareness to the facilities to apprise them of incidents and/or conditions at other Authority facilities that can impact operations on them.	M	
F-14	Regional Coordination	The Software shall automatically provide incident and/or travel time data to TRANSCOM's OpenReach. Additionally, TMDD v 3.03 or the most current version available as of the award date shall be implemented as noted in the User Needs to enable C2C communications between the PA-AOC and regional transportation agencies.	M	
F-15	Data Mining and Analysis	The Software shall include tools that will enable development of Performance Metrics. At a minimum, the Contractor shall provide the Authority with a data dictionary and entity-relationship diagrams for the tables in the database to facilitate the use of 3rd party data analysis tools.	M	
F-16	Account Administration	The Software shall provide the ability for Authority staff to administer user accounts, roles, and permissions.	M	
F-17	Configuration Management	The Contractor shall utilize a stringent Configuration Management process to manage, control, and document software configuration. Separate documentation shall be prepared for each facility and the PA-AOC and shall include specific configuration information, documentation of all SIs, and detailed recovery procedures and processes.	M	
F-18	Incident Detection	The Software shall utilize real-time VDS data and information from legacy subsystems to automatically alert operators of potential incidents. The Software shall automatically provide access to a CCTV camera feed (if available) to help verify the existence of the incident. At a minimum, alerts should be visual and audible.	M	
F-19	Planned Responses	The Software shall recommend pre-planned responses to incidents either automatically detected or manually entered. This will enable the Authority to manage incidents from detection through resolution.	M	

ID	Title	Fundamental Requirement Description	Need Mandatory	Complies Yes or No
F-20	Data Archiving	The Software shall automatically record in the centralized database all incident-related information, including at a minimum, time of detection, responses, response time, time to clear, and detailed location information.	M	
F-21	GUI	The Software shall have a map-based GUI that shows the locations of ITS assets (using different icons for each type) and their conditions. A GIS-based map is preferred.	M	
F-22	Enterprise License	The Contractor shall provide the Authority with a perpetual Enterprise License which entitles the Authority to an unlimited number of seats and to deploy as many instances of the Software as desired at no additional cost. The Contractor shall also, as part of Application Management, Maintenance, and Support, deploy software upgrades (if deemed by the Authority to be advantageous) at no additional cost to the Authority for the term of the Contract.	M	
F-23	Software Intellectual Property Ownership	The Contractor shall own all Intellectual Property Rights for the Software and have the rights to configure and make changes to the Software as required to meet the needs of the Authority.	M	
F-24	Video Wall Compatibility	The Software shall not have any compatibility or dependency requirement or issue relative to any video wall solution that the Authority might implement.	M	
F-25	NIST 800-27 Conformance	The Contractor’s Development Methodology and Software shall conform with “Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A” (NIST Special Publication 800-27, Revision A) which can be found at: http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf .	M	

MandatoryThe Proposal must meet the requirement in order to be initially deemed technically responsive to the RFP.

Project Management Requirements

The following Project Management-related requirements are also mandatory and shall be specifically addressed in all RFP responses. The Proposer must complete the accompanying spreadsheet and indicate with a "Y" or "N" whether the Proposer will or will not comply with the requirement.

ID	Title	Project Management Requirement Description	Need Mandatory	Complies Yes or No
PM-1	Project Management Plan	The Contractor's Proposal shall include a project management plan (PMP) specific to this project. The Plan shall include: Hardware Recommendations for Workstations and Servers, Work Breakdown Structure (WBS), Project Schedule, Staffing Plan, Risk Management Plan, Change Management Plan, Acceptance Management Plan, Issue Management Plan, Communications Plan, Training Plan, QA/QC Plan, and Implementation/Transition Plan including Migration Plans. This PMP shall be a "living document" and the Contractor shall be responsible for making all updates.	M	
PM-2	Project Schedule	The schedule shall be developed and maintained in Microsoft Project 2007 or greater and include a timeline, all major milestones, WBS, and a list of technical assumptions.	M	
PM-3	Schedule Details	The schedule shall define the sequencing of project tasks and activities including durations and activity dependencies.	M	
PM-4	Staffing Plan	The Contractor shall provide a staffing plan that identifies Key Staff and how they will be used to meet the RFP requirements. The staffing plan shall include an estimate of total effort hours contributed by each key staff member to each task and an estimate of total effort hours for each task.	M	
PM-5	Key Staff Replacement	Personnel identified as key staff shall be replaced only by personnel with equal or better qualifications and for the same or less cost. All key staff replacements shall be approved by the Authority.	M	
PM-6	Content of Plans	All plans identified in PM-1 above shall be developed in accordance with the Project Management Body of Knowledge (PMBOK) version 4 or 5.	M	
PM-7	Project Manager Presence and Certification	The Contractor shall assign a full-time Project Manager who will be onsite a minimum of 60% of the time for the duration of the project. The Project Manager shall be a certified PMP.	M	
PM-8	Project Management Plan Approval	All Plans identified above shall be approved by the Authority prior to implementation.	M	
PM-9	Project Management Meetings	The Project Manager shall participate in and report at all Status and Change Management Meetings for the duration of the Contract.	M	

MandatoryThe Proposal must meet the requirement in order to be initially deemed technically responsive to the RFP.

Performance Requirements

The Performance Requirements included in the following table are applicable to all instances of the Software to be installed at the facilities and the NOC and the PA-AOC. The Proposer shall, in the provided spreadsheet, indicate with a "Y" or "N" whether the Proposer will or will not comply with the requirement, and indicate whether its solution can meet each requirement out-of-the-box, with configuration (i.e., settings stored in the database), or via customization (i.e., changes to program code). Please note that if no response is provided, it will be assumed that the requirement can only be met via customization.

ID	Title	Performance Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
P-1	Real-Time	Real-time is defined such that data is no more than two (2) seconds old from the time a field device transmits the data to the time that the Software receives the data. All data shall be displayed by the Software in real-time.	N				
P-2	Polling for Device Status	The Software shall continuously poll ITS assets to determine the then current status of the equipment. Each device shall be polled at least one time per minute. DMS, VSLS, and LUCS may be polled at longer intervals to preserve bandwidth, but not at the sacrifice of function. The elapsed time from the request for information to displaying the polling results shall be less than 5 seconds.	N				
P-3	Data Veracity	The Software shall analyze all data transmitted from field devices. Should data fall outside of pre-configured limits, an alert shall be automatically issued, the operator notified, and the event logged.	N				
P-4	Receipt of Failure Notification	The Software shall be able to receive, interpret, log, and notify the operator of failure notifications received from ITS assets.	N				
P-5	Continuous Operation	The Software shall be designed and configured to operate 24 x 7 x 365. There shall be no scheduled downtime. Updates and patches shall run as hot fixes.	N				
P-6	High-Demand Performance	The Software at the PA-AOC shall perform at the level described above while monitoring and controlling up to 2000 Dynamic Message Signs (DMS), 3000 Vehicle Detection Stations (VDS), 500 Lane Use Control Signals (LUCS), 500 Variable Speed Limit Signs (VSLS), 200 Travel Time stations, and 2000 CCTV Cameras.	N				

ID	Title	Performance Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
P-7	Real-Time Analysis and Information Dissemination	The Software shall have the capability to receive, process and analyze VDS data in real-time and post travel time, report delays, or provide other traveler information to DMS in real-time.	N				

Necessary The Authority will evaluate the degree of responsiveness of the Proposal to the requirement.

Out-of-the-Box The software fulfills the requirement with no need for configuration or customization.

Configuration The requirement will be met via configurations that will be stored in the database and implemented through the application’s Graphical User Interface with no programming code changes.

Customization The requirement can only be met via changes to the programming code.

Data and Database Requirements

Requirements related to the database and data requirements are included in the following table. Proposer shall, in the provided spreadsheet, indicate with a "Y" or "N" whether the Proposer will or will not comply with the requirement, and indicate whether its solution can meet each requirement out-of-the-box, with configuration (i.e., settings stored in the database), or via customization (i.e., changes to program code). Please note that if no response is provided, it will be assumed that the requirement can only be met via customization.

ID	Title	Performance Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
DD-1	Relational Database	The Software shall utilize a Microsoft SQL Server database to store all data and software configuration information. A specific waiver from the Authority is required if any other database is to be utilized. Proprietary databases are unacceptable.	N				
DD-2	Activation from Map or Grid View	The Software shall display the image from a CCTV camera or data from other ITS field assets when that camera/device is selected either by clicking the icon representing the camera/device on the map view or by selecting the camera/device from the grid or list view.	N				
DD-3	Password Information	Password information shall not be stored in the database. The Software shall authenticate users by submitting credentials to the Lightweight Directory Access Protocol (LDAP) server for authentication.	N				
DD-4	Record of System Activity	All activity that is monitored and/or controlled by the Software shall be recorded and stored in the central database at the NOC.	N				
DD-5	Automatic Replication	The Software shall include automatic replication of the NOC databases to help ensure 24 x 7 x 365 availability.	N				
DD-6	Business Continuity	For purposes of business continuity, the NOC database at the primary data center shall automatically replicate to the secondary data center.	N				
DD-7	Reporting Capabilities	The Software shall have the capability to produce ad-hoc and predefined reports as needed. The Software shall have the capability to export report data in XML, CSV, HTML, and Excel Formats.	N				
DD-8	Login Record	The Software shall log all failed login attempts and unauthorized attempts to access information.	N				

ID	Title	Performance Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
DD-9	Activity Log	The Software shall track actions and record operator information for each operator action taken during the disposition of an incident.	N				
DD-10	VSL Log	The Software shall maintain a time-stamped log of postings on all Variable Speed Limit Signs.	N				
DD-11	Error Logs	All error messages generated by the Software shall be logged in the database in ASCII format. A complete dictionary of terms used in the error logs shall be provided.	N				
DD-12	User Creation	The Software shall provide the capability for an Authority System Administrator to add or delete users and to assign privileges as desired. This shall be accomplished by front-end configuration and all such information shall be recorded and maintained in the database.	N				
DD-13	Groups and Roles	The Software shall assign access privileges to the functionality of the Software based upon the user's assigned Group and Role. Functionality associated with each shall be configurable by an Authority System Administrator.	N				
DD-14	Equipment Logs	The Software shall date, timestamp, and store all information relative to equipment activation, communications, failures, and other actions. This information shall be transmitted to the NOC database for archival purposes. Each equipment log shall have a priority ranking field to allow filtering of critical alarms versus non-critical.	N				

NecessaryThe Authority will evaluate the degree of responsiveness of the Proposal to the requirement.

Out-of-the-BoxThe software fulfills the requirement with no need for configuration or customization.

ConfigurationThe requirement will be met via configurations that will be stored in the database and implemented through the application’s Graphical User Interface with no programming code changes.

CustomizationThe requirement can only be met via changes to the programming code.

Interface Requirements

The following table lists the Interface Requirements. Included therein are (among other things) references to Attachment E, Appendices 3 and 4 that contain inventories of legacy ITS assets for which interfaces are to be developed, lists of ITS equipment planned to be installed at the facilities, User Needs related to Traffic Management Data Dictionary TMDD Standard v3.03 requirements, and operational scenarios. Proposer shall, in the provided spreadsheet, indicate with a "Y" or "N" whether the Proposer will or will not comply with the requirement, and indicate whether its solution can meet each requirement out-of-the-box, with configuration (i.e., settings stored in the database), or via customization (i.e., changes to program code). Please note that if no response is provided, it will be assumed that the requirement can only be met via customization."

ID	Title	Interface Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
I-1	Center-to-Field (C2F) Interfaces between Facility instances of the Software and Legacy ITS Equipment	The facility-based Software instances shall monitor and control all of the legacy assets at that facility as listed in the ITS Equipment Inventory. Special SIs may need to be developed for some legacy equipment. To the extent feasible, all such SIs shall be National Transportation Communications for ITS Protocol (NTCIP) v2 (or higher) compliant.	N				
I-2	C2F Interfaces between Facility instances of the Software and New ITS Equipment	The facility-based Software instances shall monitor and control newly acquired assets. The equipment (to be provided by others) will be as stipulated in the Authority's ITS Design Guidelines and SIs shall conform to the Standards and Guidelines for Port Authority Technology.	N				
I-3	C2F Interfaces between PA-AOC instance and Legacy ITS Equipment	The PA-AOC instance of the Software shall be capable of real-time control of existing ITS equipment at all facilities. This instance shall incorporate all SIs developed for the individual facilities.	N				
I-4	Center-to-Center (C2C) Interfaces for all instances of the Software.	All Software instances shall incorporate SIs that conform to TMDD v 3.03 or later. The User Needs for this project are referenced in Attachment E, Appendix 2. All Software instances shall include the resultant TMDD SI to foster automatic communications between facilities.	N				

ID	Title	Interface Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
I-5	OpenReach Interface	The Software shall include an automatic two-way interface between TRANSCOM's OpenReach and the PA-AOC Software instance. It is envisioned that communications external to the Authority will be via the PA-AOC Software instance only, although the derived information may come from the various facilities.	N				
I-6	TRANSMIT Interface	An SI to receive TRANSMIT data from TRANSCOM shall be incorporated into the PA-AOC Software instance. The Software shall store and distribute to all facilities the travel time information made available from TRANSCOM. The Software shall have the capability to post TRANSCOM-provided travel time information to appropriate DMS automatically in real-time.	N				
I-7	Nextiva Interface	The Software shall interface with the Authority's Nextiva Video Management System (VMS), manufactured by Verint, Inc. to facilitate access to traffic surveillance cameras only, for simultaneous live viewing by multiple users. The Contractor shall coordinate with Verint to develop an SI based on the manufacturer's software development kit (SDK), the Verint VMS Client SDK, and acquire up to ten (10) Media Gateway licenses.	N				
I-8	Real-Time Analysis and Information Dissemination	The Software shall have the capability to receive, process and analyze VDS data in real-time and post travel time and delay information to DMS in real-time.	N				
I-9	Response Plans	At facilities for which there are no ITS Master Plans, operational scenarios shall be developed by the Contractor, using the Bayonne Bridge example in Attachment E, Appendix 3. The facility Software instances shall incorporate response plans to address each scenario. The Response Plans will be approved by the Authority prior to implementation. The PA-AOC instance shall have the capability to remotely implement and/or override appropriate facility response plans if necessary.	N				
I-10	Equipment Deployment	The Software shall enable an Authority System Administrator to configure the application to support new equipment for which an SI exists.	N				

ID	Title	Interface Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
I-11	INRIX Interface	The PA-AOC and TEC instances of the Software shall be capable of interfacing with third-party data providers (such as INRIX) to obtain near real-time traffic information for locations on and near the Authority facilities.	N				
I-12	TACTICS Interface	The PA-AOC and TEC instances of the Software shall include a TMDD-conformant interface to the Authority's instance of Siemens' TACTICS, traffic signal central control server. The Contractor shall be responsible for coordinating with Siemens to facilitate seamless communications between these systems. Pre-emptive traffic signal timing changes shall be a part of the facility response plans.	N				
I-13	PATH	The Port Authority Trans-Hudson (PATH) transit service is a rail transit system that runs between NJ and NY. PATH provides for electronic PATH-alerts (text/email) to subscribing customers using the eAlerts commercial system. The purpose of this interface is to provide 2-way exchange of intermodal transportation information with the PA-AOC instance of the Software such as PATH delays, disruption of service, and other critical information which may cause impact to Bridges, Tunnels, and Ferry transportation operations. Likewise, regional traffic information may be shared with PATH. This interface shall consist of a lightweight web-based application configured to satisfy the communications specified herein.	N				

ID	Title	Interface Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
I-14	Ferry Interface	Ferry Service from Manhattan to New Jersey, Staten Island, Brooklyn, and Queens presently employs a system which tracks its Ferry boats via GPS and provides real-time communications of CCTV, Terminal DMS boards, and boat kiosk screens. The purpose of this interface is to provide 2-way exchange of intermodal transportation information with the PA-AOC instance of the Software such as Ferry delays, disruption of service, and other critical information which may cause impact to Bridges, Tunnels, and the Ferry. Likewise, regional traffic information shall be shared with Ferry service such that it can accommodate a sudden increase in demand due to PATH delays, tunnel or bridge closures. This interface shall consist of a lightweight web-based application configured to satisfy the communications specified herein.	N				
I-15	Public Affairs Interface	The PA-AOC instance of the Software shall interface with Public Affairs Department to furnish regional traffic information for general use and for dissemination to the public. This interface shall consist of a lightweight web-based application configured to satisfy the communications specified herein. In particular, the interface shall include a dashboard that presents an event log that displays incident information ranked by severity at Public Affairs.	N				
I-16	PABT Interface	The Port Authority Bus Terminal (PABT) located in midtown Manhattan hosts bus service throughout the region. The PA-AOC instance of the Software shall interface with the PABT to furnish regional traffic information for general use. Likewise, delays or disruption of bus services shall be exchanged with the Software for real-time awareness. This interface shall consist of a lightweight web-based application configured to satisfy the communications specified herein.	N				

ID	Title	Interface Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
I-17	GWBBS Interface	The George Washington Bridge Bus Station (GWBBS) located in Washington Heights section of Manhattan hosts bus service throughout the region. The PA-AOC instance of the Software shall interface with the GWBBS to furnish regional traffic information for general use. Likewise, delays or disruption of bus services shall be exchanged with the Software for real-time awareness. This interface shall consist of a lightweight web-based application configured to satisfy the communications specified herein.	N				
I-18	SWR and TEB Interfaces	The PA-AOC instance of the Software shall interface with the Stewart International Airport and Teterboro Airport instances to furnish regional traffic information for general use. Likewise incidents in the area in and around those airports shall be exchanged with the PA-AOC for real-time awareness. This interface shall consist of a lightweight web-based application configured to satisfy the communications specified herein.	N				
I-19	WebEOC Interface	The PA-AOC instance of the Software shall interface directly to the WebEOC database and automatically update WebEOC with all information required for it to function in accordance with Authority needs. The intent is to have the ATMS software serve as the single point of input for Incident data.	N				

NecessaryThe Authority will evaluate the degree of responsiveness of the Proposal to the requirement.

Out-of-the-BoxThe software fulfills the requirement with no need for configuration or customization.

ConfigurationThe requirement will be met via configurations that will be stored in the database and implemented through the application’s Graphical User Interface with no programming code changes.

CustomizationThe requirement can only be met via changes to the programming code.

Human-Machine Interface (HMI) Requirements

The HMI Requirements are listed in the following table. Proposer shall, in the provided spreadsheet, indicate with a "Y" or "N" whether the Proposer will or will not comply with the requirement, and indicate whether its solution can meet each requirement out-of-the-box, with configuration (i.e., settings stored in the database), or via customization (i.e., changes to program code). Please note that if no response is provided, it will be assumed that the requirement can only be met via customization.

ID	Title	HMI Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
HMI-1	Map Interfaces for Facility-based instances of the Software	Facility-based Software instances shall have map interfaces that display the existing roadway network in the vicinity of each facility. A separate schematic representation of the facility shall be displayed adjacent to the map to show multi-level facilities and tunnels. The map and schematics shall show (on separate layers that can be toggled on or off) icons representing all ITS assets on the approaches to the facilities. The schematics shall show (on separate layers that can be toggled on or off) icons depicting the relative locations of the ITS assets on the facilities.	N				
HMI-2	Map Interfaces for PA-AOC instance of the Software	The PA-AOC instance of the Software shall display a map interface showing the Metropolitan New York area with Authority facilities prominently noted. The overview map shall have the capability to display link travel times either computed by the Software and/or provided by third-parties. The operator shall have the capability to "drill-down" to the facility level by clicking on a facility of interest. The resultant view will be identical to that displayed by the facility-based Software instance.	N				
HMI-3	Display of ITS Assets	All Software map and schematic displays shall have icons positioned to show field device locations. Each device type shall have a special icon (approved by PA) to represent it. The icons shall be automatically color coded to represent the following four statuses: <ol style="list-style-type: none"> 1. Blue shall be used to indicate that the device is functioning but not currently in service (Standby); 2. Green shall be used to indicate that the device is operating normally (Active); 	N				

ID	Title	HMI Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
		<p>3. Yellow shall indicate that the device is usable but has limited functionality. Field repairs will be required to return the device to Active status (Warning); and</p> <p>4. Red shall indicate that the device is not functioning (Disabled). Alternative color designations may be proposed.</p>					
HMI-4	Display of DMS Messages from Map Interface	The Software shall display the current sign message when a DMS icon is selected on the map.	N				
HMI-5	Display of CCTV videos from Map Interface	When an icon representing a CCTV camera is selected on the map, the video from that camera shall be displayed in a separate pop-up window on the display screen.	N				
HMI-6	Device Activation from Map	The Software shall allow an operator to activate a device from the Map Interface. All available information regarding the device shall be displayed when the device is selected.	N				
HMI-7	Tabular Display of Device Information	Facility-based Software instances shall have the capability to display a tabular list of ITS assets assigned to the facility. The data shall be presented in a grid that permits the operator to select and sort the devices based upon type or status. The PA-AOC instance shall have the capability to display a tabular list of ITS assets for all facilities which shall be displayed in a grid that permits sorting and filtering by type, status, and facility.	N				
HMI-8	Display of DMS Messages from Grid View	The Software shall display the current sign message when a DMS is selected from the grid or list.	N				
HMI-9	Display of CCTV videos from Grid View	When a CCTV camera is selected from the Grid View, the Software shall display the feed from that camera in a separate pop-up window.	N				
HMI-10	Device Activation from Tabular View	The Software shall allow an operator to activate a device from the Tabular/Grid View. All available information regarding the device shall be displayed when the device is selected in the Grid View.	N				

ID	Title	HMI Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
HMI-11	Display of Incident Locations on Maps	The Software shall display an icon representing an incident at the correct relative location on the Map and Schematic. The symbology shall be configurable by the operator. The description and status of the incident shall be displayed in a pop-up window on mouse-over.	N				
HMI-12	Tabular Display of Incident Information	Facility-based instances of the Software shall have the capability to display a tabular list of active incidents at the facility. The data shall be presented in a grid that permits the operator to select and sort active incidents based upon type or status. The PA-AOC instance shall have the capability to display a tabular list of active incidents for all facilities which shall be displayed in a grid that permits sorting and filtering by type, status, and facility.	N				
HMI-13	Dynamic Scaling of Map	The Software shall dynamically scale all objects (icon, symbols, text, menus, etc.) based on screen resolution.	N				
HMI-14	System Administration	The Software shall provide front-end configuration capabilities. Authority System Administrators shall have the capability to add/delete/modify Users, User-Groups, and ITS devices (when SIs already exist). System Administrators shall also have the ability to configure C2C communications with regional partners.	N				
HMI-15	External System Access from Map.	The Software shall provide access to other systems (e.g., TACTICS) by clicking on an icon displayed on the map (e.g., a traffic signal) to open a window or instance to view communications status.	N				

NecessaryThe Authority will evaluate the degree of responsiveness of the Proposal to the requirement.

Out-of-the-BoxThe software fulfills the requirement with no need for configuration or customization.

ConfigurationThe requirement will be met via configurations that will be stored in the database and implemented through the application’s Graphical User Interface with no programming code changes.

CustomizationThe requirement can only be met via changes to the programming code.

Functional Requirements - General

The following table lists a set of functional requirements that address general capabilities that the Software must meet. Proposer shall, in the provided spreadsheet, indicate with a "Y" or "N" whether the Proposer will or will not comply with the requirement, and indicate whether its solution can meet each requirement out-of-the-box, with configuration (i.e., settings stored in the database), or via customization (i.e., changes to program code). Please note that if no response is provided, it will be assumed that the requirement can only be met via customization.

ID	Title	General Functional Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
FG-1	High Availability	The Software shall achieve 99.9% availability.	N				
FG-2	Automatic Failover	The Software (including database) shall be installed on two mirrored central servers and both the Software and database shall automatically fail over when necessary, without downtime.	N				
FG-3	Hardware Scalability	The Software shall automatically utilize the total number of CPUs available on the servers.	N				
FG-4	Virtualization	The Software shall have the ability to operate in a virtualized environment in accordance with the <i>Standards and Guidelines for Port Authority Technology</i> .	N				
FG-5	Seamless Updates	The Software shall provide the ability to deploy new functionality and or new SIs with minimal downtime (in accordance with the Service Level Agreement for the contract).	N				
FG-6	Software Migration Plan	The selected Contractor shall collaborate with the Authority to develop a Migration Plan to fully test the application in non-production tiers prior to "go-live."	N				
FG-7	Software Architecture	The Software shall be a server-based application that utilizes an industry standard Relational Database. Users will access the application via web-browsers. The Software shall be accessible via a secure connection to the Authority's network.	N				
FG-8	Hardware and Operating System	The Software shall run in the environments specified in the <i>Standards and Guidelines for Port Authority Technology</i> .	N				

ID	Title	General Functional Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
FG-9	Central Database for Archiving	The Software shall use and maintain a central repository for configuration information and all historical data at the NOC. All such data from each facility shall be automatically transmitted to and stored in the central database.	N				
FG-10	Performance Metrics	The PA-AOC instance shall have the ability to calculate performance metrics (to be determined by the Authority) for each facility. The database at the NOC shall be made available to select third party tools for data mining and reporting purposes.	N				
FG-11	Tabular Display of Incident Information	Facility-based Software instances shall have the capability to display a tabular list of active incidents at the facility. The data shall be presented in a grid that permits the operator to select and sort active incidents based upon type or status. The PA-AOC instance shall have the capability to display a tabular list of active incidents for all facilities which shall be displayed in a grid that permits sorting and filtering by type, status, and facility.	N				
FG-12	Permissions for Asset Monitoring and Control	The Software shall restrict access to ITS assets based upon assigned user roles. Facility operators shall have the ability to monitor and control only those assets under their purview. The PA-AOC instance shall have the ability to monitor and control all Authority assets.	N				

NecessaryThe Authority will evaluate the degree of responsiveness of the Proposal to the requirement.

Out-of-the-BoxThe software fulfills the requirement with no need for configuration or customization.

ConfigurationThe requirement will be met via configurations that will be stored in the database and implemented through the application’s Graphical User Interface with no programming code changes.

CustomizationThe requirement can only be met via changes to the programming code.

DMS Functional Requirements

The proposed Software must meet the following requirements related to DMS. Proposer shall, in the provided spreadsheet, indicate with a "Y" or "N" whether the Proposer will or will not comply with the requirement, and indicate whether its solution can meet each requirement out-of-the-box, with configuration (i.e., settings stored in the database), or via customization (i.e., changes to program code). Please note that if no response is provided, it will be assumed that the requirement can only be met via customization.

ID	Title	DMS Functional Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
FDMS-1	WYSIWYG Capabilities	The Software shall provide the operator with WYSIWYG sign monitoring if the field device is capable of so doing (National Transportation Communications for ITS Protocol (NTCIP) v2 or better compliance). That is, the solution shall depict the DMS sign on the operators' displays exactly as it appears in the field when the icon representing the DMS is clicked or on mouseover.	N				
FDMS-2	Manual Message Creation	The Software shall provide the operator with the capability to create ad-hoc sign messages on the fly.	N				
FDMS-3	Message Library	Each facility instance of the software shall have a message library containing predefined messages that are to be displayed pursuant to a response plan. The sign message library for the PA-AOC instance of the Software shall include all facility message libraries. Each message shall be uniquely identified in accordance with nomenclature that will indicate the facility/sign for which the message has been created.	N				
FDMS-4	Message Editing and Deletion	The Software shall provide the operator with the capability to edit and/or delete messages. The solution shall also contain a list of forbidden words and terms that can be edited only by system administrators. Messages containing forbidden words shall be prevented from being displayed.	N				
FDMS-5	Pre-programmed Messages	The Software shall automatically display pre-defined messages in accordance with a response plan and/or operator action.	N				
FDMS-6	Updating/Editing Sign Messages in Response Plans	The operator shall have the ability to create or modify messages that are part of a pre-programmed response plan.	N				

ID	Title	DMS Functional Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
FDMS-7	Display of Message on Multiple DMS	The Software shall enable the operator to select multiple DMS upon which a message shall be displayed. This functionality shall be available both from the map view and the grid view.	N				
FDMS-8	Blank Out Sign	The Software shall provide the capability for the operator to blank out all messages on a DMS.	N				
FDMS-9	DMS Verification	Operators shall have the capability to verify DMS integrity using the Software.	N				
FDMS-10	Display Control	The Software shall provide the ability for the operator to manually control display brightness and color intensity, to the extent possible by the DMS.	N				
FDMS-11	Message Scheduling	The Software shall provide the capability to schedule messages for display on DMS as desired.	N				
FDMS-12	Automatic Updating of Messages	The Authority may wish to post travel times on their DMS. The Software shall have the ability to automatically update travel time information at operator-configured intervals on operator-selected DMS.	N				
FDMS-13	VMS Message Hierarchy	The Contractor shall, in close collaboration with the Authority, define a hierarchy of DMS messages displayed by the facilities and the PA-AOC. The Software shall include a mechanism to prevent highly important messages from being inadvertently overwritten by those of lesser import. This functionality shall be available in the Software along with the capability to override it if appropriate.	N				
FDMS-14	Failure Alarms	The Software shall automatically trigger an alarm to notify the operator of a DMS malfunction. The icon representing the malfunctioning DMS in the map view shall flash red and an audible alarm shall be triggered.	N				
FDMS-15	DMS Logging	The Software shall automatically log in the NOC database a full history of messages displayed at each DMS. Each message and change thereto shall be logged and time-stamped. The username of the operator invoking the change shall also be recorded. Automated travel time messages shall also be logged in the database and archived.	N				

NecessaryThe Authority will evaluate the degree of responsiveness of the Proposal to the requirement.

Out-of-the-BoxThe software fulfills the requirement with no need for configuration or customization.

ConfigurationThe requirement will be met via configurations that will be stored in the database and implemented through the application’s Graphical User Interface with no programming code changes.

CustomizationThe requirement can only be met via changes to the programming code.

CCTV Functional Requirements

The following functional requirements for CCTV camera integration must be met. Proposer shall, in the provided spreadsheet, indicate with a "Y" or "N" whether the Proposer will or will not comply with the requirement, and indicate whether its solution can meet each requirement out-of-the-box, with configuration (i.e., settings stored in the database), or via customization (i.e., changes to program code). Please note that if no response is provided, it will be assumed that the requirement can only be met via customization.

ID	Title	CCTV Functional Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
FCCTV-1	Pre-Set Capabilities	The Software shall provide the capability for operators to save preset camera positions including pan angle, zoom setting, tilt angle, focus setting, and an appropriate description that shall be superimposed on the image.	N				
FCCTV-2	Activation from Map or Grid View	The Software shall display the image from a CCTV camera when that camera is selected either by clicking the icon representing the camera on the map view or by selecting the camera from the grid view.	N				
FCCTV-3	Camera Control	The Software shall provide the capability for an operator to control the Pan, Tilt, and Zoom settings for any selected camera using virtual joystick. The Software shall have the capability to save the resultant settings, have them activated at a later time by referencing the name assigned by the operator, and shall allow the operator to designate the resultant settings as the new default for the camera.	N				
FCCTV-4	Minimum Number of Presets	The Software shall allow for a minimum of 30 preset PTZ combinations to be saved for each camera.	N				
FCCTV-5	Video Tours	The Software shall allow the operator to create and edit video tours consisting of sequential feeds from selected cameras. Preset (default) PTZ settings shall be automatically used for each camera in the series. The operator shall have the capability to temporarily stop the tour on any selected camera view and control PTZ for that camera as desired.	N				

ID	Title	CCTV Functional Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
FCCTV-6	Automatic Selection of Camera on Alarm	When the Software detects a potential incident, the nearest CCTV camera shall be automatically activated (e.g., in a pop-up window) and aimed in the direction of the detected anomaly.	N				
FCCTV-7	Group Control	Similar to camera control, under group control, multiple cameras may be automatically positioned to a preset position based on automatic detection of an incident on a facility. This is based on derived scenario response plans for each facility.	N				

NecessaryThe Authority will evaluate the degree of responsiveness of the Proposal to the requirement.

Out-of-the-BoxThe software fulfills the requirement with no need for configuration or customization.

ConfigurationThe requirement will be met via configurations that will be stored in the database and implemented through the application’s Graphical User Interface with no programming code changes.

CustomizationThe requirement can only be met via changes to the programming code.

Vehicle Detection System Functional Requirements

The following requirements related to VDS must be met by the Software. Proposer shall, in the provided spreadsheet, indicate with a "Y" or "N" whether the Proposer will or will not comply with the requirement, and indicate whether its solution can meet each requirement out-of-the-box, with configuration (i.e., settings stored in the database), or via customization (i.e., changes to program code). Please note that if no response is provided, it will be assumed that the requirement can only be met via customization.

ID	Title	VDS Functional Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
FVDS-1	Map and Grid Display	The Software shall display each VDS station on the map and in the grid view. The VDS stations shall be polled at a minimum rate of two (2) times per minute. The status of each station shall be determined and displayed. Information on the map shall be displayed on mouseover. Information in the grid view shall be automatically updated as appropriate.	N				
FVDS-2	Activation from Map or Grid View	The Software shall display the latest data from the VDS when it is selected either by clicking the icon representing the VDS on the map view or by selecting the VDS from the grid view. The latest received values for Volume, Occupancy, and Speed for each lane shall be displayed. Depending on the VDS, vehicle length (classification) should also be displayed.	N				
FVDS-3	Speed Displays	The Software shall receive and process data from the VDS stations at regular intervals and shall compute and display the then-current travel times between VDS on the map and in a grid view.	N				
FVDS-4	Anomaly Detection	The Software shall utilize an algorithm (approved by the Authority) to detect potential incidents. When potential incidents are detected, the Software shall display alarms on the map and in the grid view. An audible alarm shall also sound at the workstation.	N				
FVDS-5	Incident Verification	The Software shall place potential incidents in a list available to the operator. The operator shall, upon analyzing all available data, be able to make a determination as to the existence of an incident.	N				

ID	Title	VDS Functional Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
FVDS-6	Incident Data Archiving	The facility instance of the Software shall transmit to the NOC instance all information regarding an incident that has been verified by the facility operator. Each response step shall be automatically archived in the NOC database.	N				
FVDS-7	Data Archiving	The facility instance of the Software shall transmit to the NOC database volume, occupancy, classification, and speed data. The facility instance shall aggregate the VDS data to 15 minute averages and transmit those values to the NOC for archiving, analysis, and computation of performance metrics.	N				

NecessaryThe Authority will evaluate the degree of responsiveness of the Proposal to the requirement.

Out-of-the-BoxThe software fulfills the requirement with no need for configuration or customization.

ConfigurationThe requirement will be met via configurations that will be stored in the database and implemented through the application’s Graphical User Interface with no programming code changes.

CustomizationThe requirement can only be met via changes to the programming code.

Incident Management and Response Functional Requirements

A primary function of the Authority's facility operators is to manage the response to incidents and to clear them as quickly as possible. Specific requirements that the Software must meet are included in the following table. Proposer shall, in the provided spreadsheet, indicate with a "Y" or "N" whether the Proposer will or will not comply with the requirement, and indicate whether its solution can meet each requirement out-of-the-box, with configuration (i.e., settings stored in the database), or via customization (i.e., changes to program code). Please note that if no response is provided, it will be assumed that the requirement can only be met via customization.

ID	Title	Incident Management/Response Functional Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config-uration	Requires Custom-ization
FIMR-1	Response Actions	Actions available for use in a response plan shall include: providing suggested actions to an operator; providing information to an operator regarding emergency contacts; activation of roadside devices (e.g., automatically posting, upon user confirmation, a pre-defined message to one or more DMS); automatically providing information to TRANSCOM's OpenReach; and automatically notifying (via SMS text message, email, or page) a predefined list of entities.	N				
FIMR-2	Pre-defined Response Plans	Operational Scenarios and response plans are to be developed under this project for each facility. A sample scenario/response plan developed for the Bayonne Bridge is shown in Attachment E, Appendix 3. Pre-defined response plans shall be developed in the same manner. The Software shall store and utilize the Pre-defined Response Plans for each scenario when so indicated by the operator. Response Plans shall consist of a set of recommended actions to be confirmed by the operator prior to execution.	N				
FIMR-3	Ad-Hoc Responses	The Software shall facilitate the specification and deployment of incident responses specified by the operator. These responses may override Pre-defined Responses at the operators' discretion.	N				
FIMR-4	PA-AOC Responses	All facility Response Plans shall be included in the PA-AOC instance of the Software. When necessary, the incident response shall be able to be managed from the PA-AOC.	N				

ID	Title	Incident Management/Response Functional Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
FIMR-5	Automatic Responses	Individual steps for each Response Plan shall be recommended by the Software. Steps may include specific DMS messages displayed on one or more signs, activation of specific CCTV cameras, etc. Such actions though programmed, shall not be executed prior to operator approval. At the operator's discretion, steps in the plans shall be able to be skipped.	N				
FIMR-6	Response Plan Creation	The Software shall allow operators to create, edit, and modify response plans. Information shall include (at a minimum) location, severity, devices to be activated/controlled, action/message for each.	N				
FIMR-7	Notification of Need to Override	The ATMS solution shall automatically notify a facility when circumstances exist that warrant operation of facility assets from the PA-AOC. All such notifications shall be recorded, logged, and archived.	N				
FIMR-8	Data Archiving	The facility instances on the Software shall transmit to the NOC database all incident related data including (but not limited to): time of detection, time of verification, incident type and location, time each response step was executed, individuals contacted, and time incident was cleared.	N				
FIMR-9	Contact List	The Software shall allow operators to create, manage, and revise contact lists and schedules. The solutions shall allow for lists which vary in accordance with time of day and shall automatically display the appropriate contact list.	N				
FIMR-10	Cancellation	The Software shall cancel equipment activation associated with a response plan only upon confirmation by the operator.	N				
FIMR-11	System Restore	The Software shall permit the operator to revert to normal operations via a single-click operation.	N				
FIMR-12	Operator Configuration	The Software shall provide a means (via a GUI) for the operators to add, edit or delete parameters related to an incident including the thresholds for reporting a potential incident.	N				

NecessaryThe Authority will evaluate the degree of responsiveness of the Proposal to the requirement.

Out-of-the-BoxThe software fulfills the requirement with no need for configuration or customization.

ConfigurationThe requirement will be met via configurations that will be stored in the database and implemented through the application’s Graphical User Interface with no programming code changes.

CustomizationThe requirement can only be met via changes to the programming code.

ITS Asset Monitoring and Management Functional Requirements

The Authority has specific needs relative to the monitoring and management of legacy and new ITS devices. Those needs are embodied in the following requirements. Proposer shall, in the provided spreadsheet, indicate with a "Y" or "N" whether the Proposer will or will not comply with the requirement, and indicate whether its solution can meet each requirement out-of-the-box, with configuration (i.e., settings stored in the database), or via customization (i.e., changes to program code). Please note that if no response is provided, it will be assumed that the requirement can only be met via customization.

ID	Title	Asset Monitoring and Management Functional Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config-uration	Requires Custom-ization
FAMM-1	Condition Monitoring	The Software shall allow all operators to generate an equipment list with current status for the ITS assets under their purview.	N				
FAMM-2	Condition Reporting	Facility based instances shall have the capability to generate reports on the historical condition of all assets for any given date range.	N				
FAMM-3	Inventory Information	An interface to the Authority's Roadway Devices Management System (RDMS) Maximo implementation shall be developed. This shall be a two-way interface. Information for each ITS field device shall be stored in the database and shall include at a minimum; device manufacturer, model number, and firmware number, install date, location, communications protocol, and service history.	N				
FAMM-4	Remote Diagnostics	The Software shall automatically monitor the health of all ITS assets, detect failures, issue problem reports, and track the repair or replacement of the equipment.	N				
FAMM-5	Device Additions	The Software shall allow operators to add new field devices (for which SIs have been developed) via the user interface. Operators shall also have the capability to edit, delete and/or modify information regarding individual assets.	N				
FAMM-6	Maintenance Information	The Software shall provide operators with the means to maintain up-to-date maintenance information for assets and allow ad-hoc reports to be developed to summarize that data.	N				

ID	Title	Asset Monitoring and Management Functional Requirement Description	Need Necessary	Complies Yes No	Out of Box	Config- uration	Requires Custom- ization
FAMM-7	Administration GUI	The Software shall include a GUI which will allow complete Administration of the equipment, data, maintenance records, etc. This GUI shall include online and context sensitive help.	N				

NecessaryThe Authority will evaluate the degree of responsiveness of the Proposal to the requirement.

Out-of-the-BoxThe software fulfills the requirement with no need for configuration or customization.

ConfigurationThe requirement will be met via configurations that will be stored in the database and implemented through the application’s Graphical User Interface with no programming code changes.

CustomizationThe requirement can only be met via changes to the programming code.

2/8/16

Appendix 2 - User Needs (TMDD Standard v3.03c)

User Needs for Traffic Management Data Dictionary (TMDD) Standard v3.03c are Section 2.3 of Concept of Operations Document and Requirements for TMDD Standard v3.03c dated July 16, 2014. A PDF of that document can be found at:

<http://www.ite.org/standards/tmdd/3.03/TMDDv3.03c-Vol1.pdf>

Appendix 3 - Concept of Operations and Inventories

Operational Scenarios for each facility are unique to that facility and the response plans are dependent upon the field assets available to that facility at the time of implementation. Upon award of this Contract, it will be the Contractor's responsibility to work with Facility Operations and Traffic Engineering staff to determine the necessary scenarios to employ and their respective response plans. The ITS Master Plans help define which DMS, VLS, Cameras, LUCS, Traffic Signal timings, etc. are impacted by either Operational or Incident-driven scenarios. ITS Master Plans will be made available to the Contractor. Operational scenarios are incurred when deemed necessary by the Facility Manager for planned or anticipated events. These would be for example, planned lane closures, bridge closures, high wind, ice or snow. Incident scenarios are unanticipated events and their respective response plans are determined in accordance with the location of one or more incidents on or near the facility. A sample ITS layout, scenario and response plan is provided below for the Bayonne Bridge under the Staten Island Bridges discussion.

Overview

The purpose of this project is to optimize transportation system network operations, reduce incident response times, and share information with neighboring agencies, and ultimately provide real-time regional situational awareness among all Port Authority (PA) Facilities. The existing PA facilities were observed based on how they operate, assets available, and existing operation center floor plan arrangements. The findings are discussed and presented below. Most of the facilities observed have limited ITS assets and/or assets that will be updated and/or replaced in the near future. System interfaces will have to be developed by the Contractor for some facilities that will require maintaining operations of legacy devices until such time those new assets are installed.

There will be four centers, including the proposed Primary Port Authority Agency Operations Center (PA-AOC); backup PA-AOC, disaster recovery site; and Traffic Engineering Center. Each of the centers will have a separate instance of the Agency-wide Transportation Management Software (TMS) and each will have the ability to monitor and/or control one or more facilities.

In addition to the four (4) centers, there will be 17 instances of the TMS, one (1) each at ten (10) PA facilities to monitor and/or control nearby ITS assets, and "lightweight" applications at seven (7) locations (see Figure 1). The NOC will serve as the data repository and the information hub for the PA. Facility TMS instances will continuously transmit data regarding traffic volumes, incidents, etc. to the NOC instance for purposes of data archiving and calculation of facility-specific performance metrics. The PA-AOC will have the capability to monitor and control assets at any PA facility when required and will also provide Agency-wide regional situational awareness. All inter-facility communications will utilize the Port Authority Wide-Area Network (PAWANET). Legacy assets that do not have National Transportation Communications for ITS Protocol (NTCIP) compatibility will require the Contractor to develop custom system interfaces to monitor and control these field assets.

Supervisory Control and Data Acquisition (SCADA) systems are not included in this project. Although many facility management and other SCADA systems do exist at most of the PA facilities, these are not to be included in this project and will be left separated to operate independently by a SCADA central control system.



Figure 1 - System Context Diagram

George Washington Bridge (GWB)



The GWB is a suspension bridge that spans the Hudson River connecting Washington Heights neighborhood in the borough of Manhattan, NYC to Fort Lee, New Jersey. Interstate 95 crosses the bridge. The GWB has an upper level that carries four lanes of traffic in each direction while the lower level carries three lanes of traffic in each direction for a total of 14 lanes. There are paths located on each side of the upper level of the bridge for pedestrian and bicycle traffic.

The GWB is operated under the Transdyn DYNAC system for both ITS and SCADA; however, the TMS selected under this project will replace the ITS function. SCADA will remain on the DYNAC system.

The bridge CommDesk consists of the police operators workstation where most of the radio communications and equipment are located, a small monitor workstation is used for bridge ITS and SCADA, and a video wall on the right side of the room which is no longer functional. The video wall used to serve in providing a status overview of the facility and the vehicle detection sensors. The bridge tour manager's office is located in another room on the same floor. Communications between the police workstation and the tour manager's office is through intercom only.

DYNAC ES presently controls both ITS and SCADA functions. After the TMS implementation, DYNAC ES will remain in place for the SCADA function only.

The Authority intends to implement Sensys Networks' wireless detection sensors embedded in the roadway on the approaches to the facility, details of which will be provided after contract award.

Under the TMS, incidents are to be detected in real-time from changing traffic conditions, stopped or slowed traffic as seen by the vehicle detection system. In turn, this would trigger an alarm in the TMS and offer suggestions to a relevant scenario and response plan for the operator to authorize initiation. The interface requirement for this software action is listed in Appendix 1 - Requirements.

SCADA systems for bridge aesthetic lighting, network health, ventilation and pump control systems will remain under the operation and monitoring of the DYNAC ES software. Ideally, there should be multiple (larger) monitors setup for this ITS workstation where several of the most common functional screens are visible at all times without having to toggle through menus for access. Refer to the GWB floor plan for proposed location of new ITS Workstation, which is adjacent to the existing DYNAC workstation. In addition to the proposed workstation in the OCC, access to the TMS should also be possible from the facility tour manager's office using the existing PC in that location.

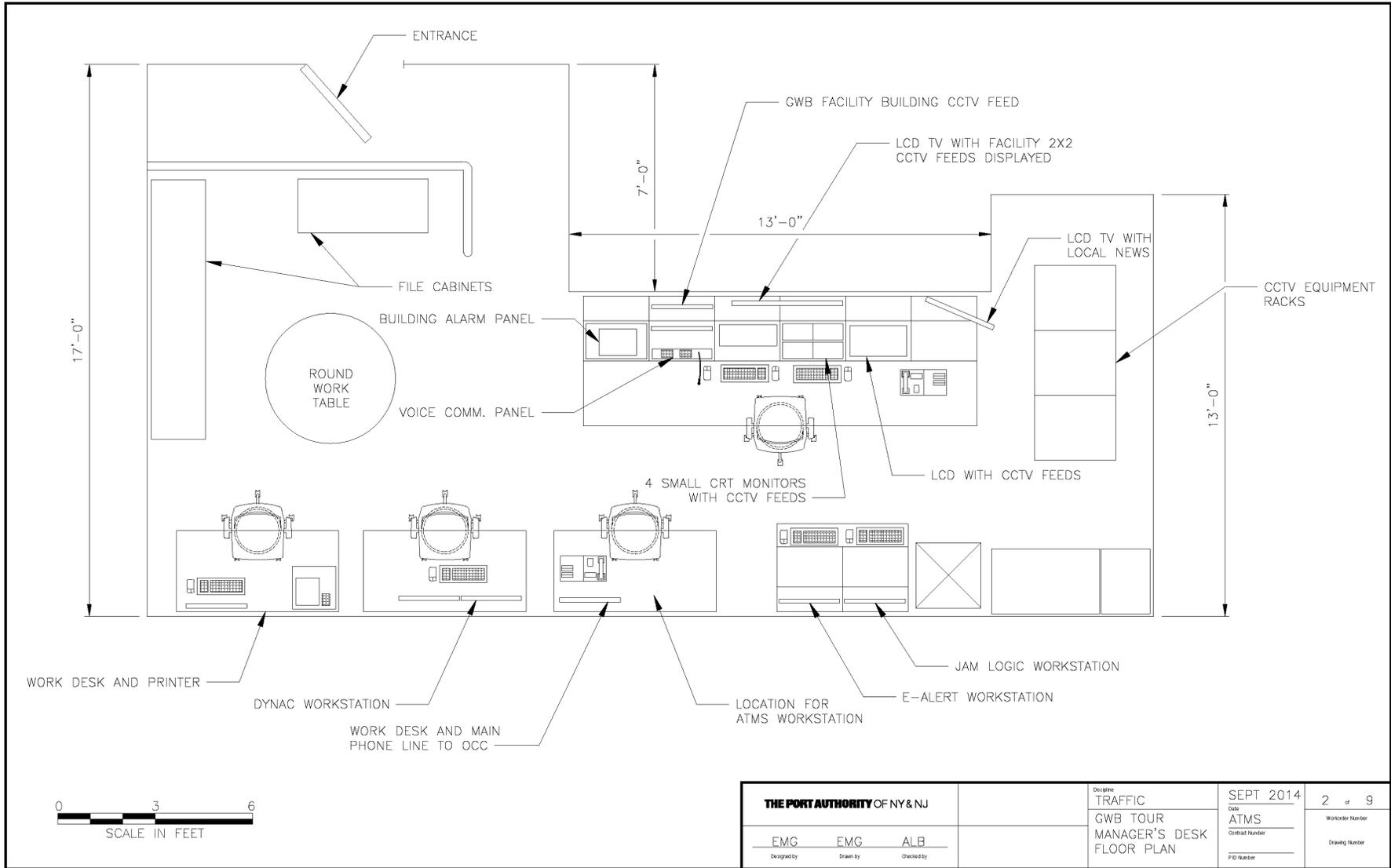
There are four (4) main screens that need to be visible at all times, including DMS control/messages, alert log screen, graphical layout of vehicle detection on the bridge, and a 4th screen solely dedicated for CCTV. The large video monitors to the right side of the room should be a solid large video wall with an overall graphic of the bridge in plan-view showing the status of all vehicle detection stations and RWIS. Alarms triggered on that wall can be acted upon at the police or ITS workstations. While it is not in the scope of this project for the Contractor to furnish and install a new video wall, the provisions for communicating with this future video wall need to be accounted for in the TMS.

2/8/16

Visibility of the bridge roadway and levels from the OCC is very limited and there is almost complete dependency on the CCTV system to see all areas of the bridge. The existing CCTV system includes analog cameras routed through an American Dynamics video switch. However, TD is presently implementing an Enterprise CCTV solution using the Verint Nextiva system, but the exact schedule of full transference onto the enterprise solution is unknown.

The GWB uses an "E-Alert" system by which they log incidents and events electronically. All future events will be logged into the TMS, which in-turn will be required to populate the E-Alert system as well as OpenReach. Incidents that may be automatically detected by the TMS should bring up the nearest field camera to that incident.

The GWB currently has ten new Daktronics full color matrix DMS and six legacy Vultron DMS. Twenty-seven new LED DMS are scheduled to be installed within the next year on the approaches or at the GWB itself. All of these new signs are anticipated to be by Daktronics and of the latest version of NTCIP for full matrix, full color, 20mm pitch DMS. The following is a complete inventory list of the required devices (both legacy and new), for which the Contractor will need to provide System Interfaces (SIs) at GWB.



0 3 6
SCALE IN FEET

THE PORT AUTHORITY OF NY & NJ			Discipline TRAFFIC	SEPT 2014	2 of 9
			GWB TOUR MANAGER'S DESK FLOOR PLAN	Date ATMS	Worksheet Number
EMG	EMG	ALB		Contract Number	Drawing Number
<small>Designed by</small>	<small>Drawn by</small>	<small>Checked by</small>		PID Number	

INVENTORY AT GWBDynamic Message Signs (DMS)

Communication interfaces are a mix of serial hardwired and fiber optic cable. DMS protocol is predominantly NTCIP.

Manufacturer	Sign Model / Matrix	Qty	Controller Model	Vintage	Protocol	Interface
Vultron	Model B090-2L (14x104) Firm v1.272	2	-	Legacy	NTCIP	RS-232/IP
Vultron	Model B090-2L (14x88) Firm v1.272	1	-	Legacy	NTCIP	RS-232/IP
Vultron	Model B090-2L (14x144) Firm v1.272	1	-	Legacy	NTCIP	RS-232/IP
Vultron	Model B090-2L (14x264) Firm 1.272	1	-	Legacy	NTCIP	RS-232/IP
Vultron	Full Matrix (42x184)	1	-	Legacy	NTCIP	RS-232/IP
Daktronics	VF-2320-64x224-20-RGB	1	VFC-3000	New	NTCIP	IP
Daktronics	VF-2320-64x288-20-RGB	7	VFC-3000	New	NTCIP	IP
Daktronics	VF-2320-96x384-20-RGB	2	VFC-3000	New	NTCIP	IP
Daktronics	VF-2329-96x336-20-RGB	1	VFC-3000	New	NTCIP	IP
Daktronics	VF-2329-64x288-20-RGB	4	VFC-3000	New	NTCIP	IP

Closed Circuit TV System (CCTV)

Manufacturer	Model Description	Qty	Controller Model	Vintage	Protocol	Interface
Verint	Nextiva Video Management Server	1	Nextiva	Version 6	IP	Verint SDK
American Dynamics	Analog Video Switch	1	-	Legacy	-	RS-232
COHU	Camera 1322-1000	39	-	Analog-Encoder	-	IP

Lane-Use Control Signals (LUCS)

Existing LUCS are legacy X-arrow signals by National Sign and Signal Company. There are 12 sets of signals serving the facility and are controlled by Transdyn's DYNAC Software as a SCADA system. These will be replaced with NTCIP-compliant units and integrated with the TMS in the future.

2/8/16

TRANSMIT (Travel Time System)

TRANSMIT is a TRANSCOM system that utilizes Kapsch Janus Multi-protocol readers. The TMS is to communicate with TRANSMIT through the use of TRANSCOM's Bridge API, which can be obtained at no cost from TRANSCOM. All TRANSMIT Servers are Windows based and located at the GWB Administration Building. DYNAC utilizes an application on a separate server to interface with TRANSCOM to post travel times on DMS. This function/application must be replicated in the TMS.

ID	Site	# of Reader Cabinets	# of Antennas	XMIT Server	Interface
GW01	GWB @ Amsterdam Ave	1	8	GWB	Cell Modem
GW02	GWB @ Henry Hudson Pky	1	4	GWB	Cell Modem
GW03	GWB @ Palisades	1	4	GWB	Cell Modem
GW04	GWB @ Central Road	1	2	GWB	Cell Modem
GW05	I-95 @ Fletcher Avenue	1	4	GWB	Cell Modem
GW06	I-95 @ Jones Road	1	4	GWB	Cell Modem
GW07	PIP North of Exit 1	1	2	GWB	Cell Modem
GW08	Route 4 West of I-95	1	3	GWB	Cell Modem
GW09	Route 46 @ Oakdene Avenue	1	3	GWB	Cell Modem
GW10	I-80 @ Garden State Parkway	1	2	GWB	Cell Modem
PA01	Rt 46 Approach	1	2	GWB	Cell Modem
PA02	1.5 mi North of PIP	1	2	GWB	Cell Modem
PA03	I95 South of I-80	1	3	GWB	Cell Modem

Lincoln Tunnel (LT)



The LT is a 1.5-mile-long vehicular tunnel under the Hudson River, connecting Weehawken, New Jersey and Manhattan, New York City, New York (midtown). The LT has three tubes that carry a total of six travel lanes. During the weekday morning peak period, one travel lane in the center tube is used solely for buses as part of the Exclusive Bus Lane (XBL) operation. Each of the travel lanes in the tunnel's center tube is reversible. In the mornings, both lanes are Manhattan-bound while in the evenings during rush hour both lanes are New Jersey-bound. In other time periods, one lane is provided in each direction. This XBL function is presently handled by a SCADA system with a Human-Machine Interface (HMI) by HSQ. Operations for XBL Lane Use Signal control and related variable message signs will remain on HSQ. In the future, when the Lane Use Signal System is upgraded to an NTCIP-compliant system, the XBL function will be added to the TMS.

The Lincoln Tunnel has a fairly large OCC occupied by the tour manager, police and other operators. Direct communication within the room is possible without the need for an intercom. (See LT OCC Floor Plan below).

There is a large video wall with two rows of ten monitors each configured for four feeds per monitor. This video wall is used strictly for CCTV surveillance. Each row provides full video coverage of one of the three tunnels, and a fourth row provides video coverage of the tunnel approaches, ramps for both NY and NJ. Video is provided through a Verint Nextiva server and is switched using a video switcher keyboard directly controlling an American Dynamics analog video switch located in a back room. The tour manager seemed to have memorized all of the camera numbers by location. Video selection, therefore, is not done graphically by location off of a map.

There are several workstations located along two rows of long curve-shaped desks configured and arranged for visibility of the video wall. The leftmost workstation is a general-use PC mostly used for Web-EOC (E-log) for logging of events and incidents. The tour manager will make all of his/her entry logs in E-log. OpenReach is not yet installed at this facility, but it is coming and will be on yet a separate workstation. One of the difficulties for the tour manager is the need to enter the same information several times. Logging of an event or incident requires the tour manager to log this into E-Log and OpenReach. It is the intent of this project to allow the user to only enter this information into the TMS, and the TMS to populate E-Log and OpenReach with this information, thus only requiring the tour manager to enter it once. The proposed TMS workstation is to replace the existing DYNAC once all TMS functions are duplicated and transferred over. In addition to the proposed workstation at the CommDesk, access to the TMS should also be possible from the facility tour manager's office using the existing PC in that location.

The second workstation at the desk is running HSQ and has a 28-inch widescreen monitor. HSQ is a program that operates legacy Lane Use Control Signals, Changeable Speed Limit Signs, and some DMS that serve the XBL. Since these are older non-NTCIP devices, they are operated from relay cabinets controlled by a SCADA system. The SCADA system is controlled by the HSQ software. The process in the morning of reversing the westbound lane to eastbound for the buses is complex and requires field crews to manually place markers along the lane line. The HSQ terminal does not have any video functions nor

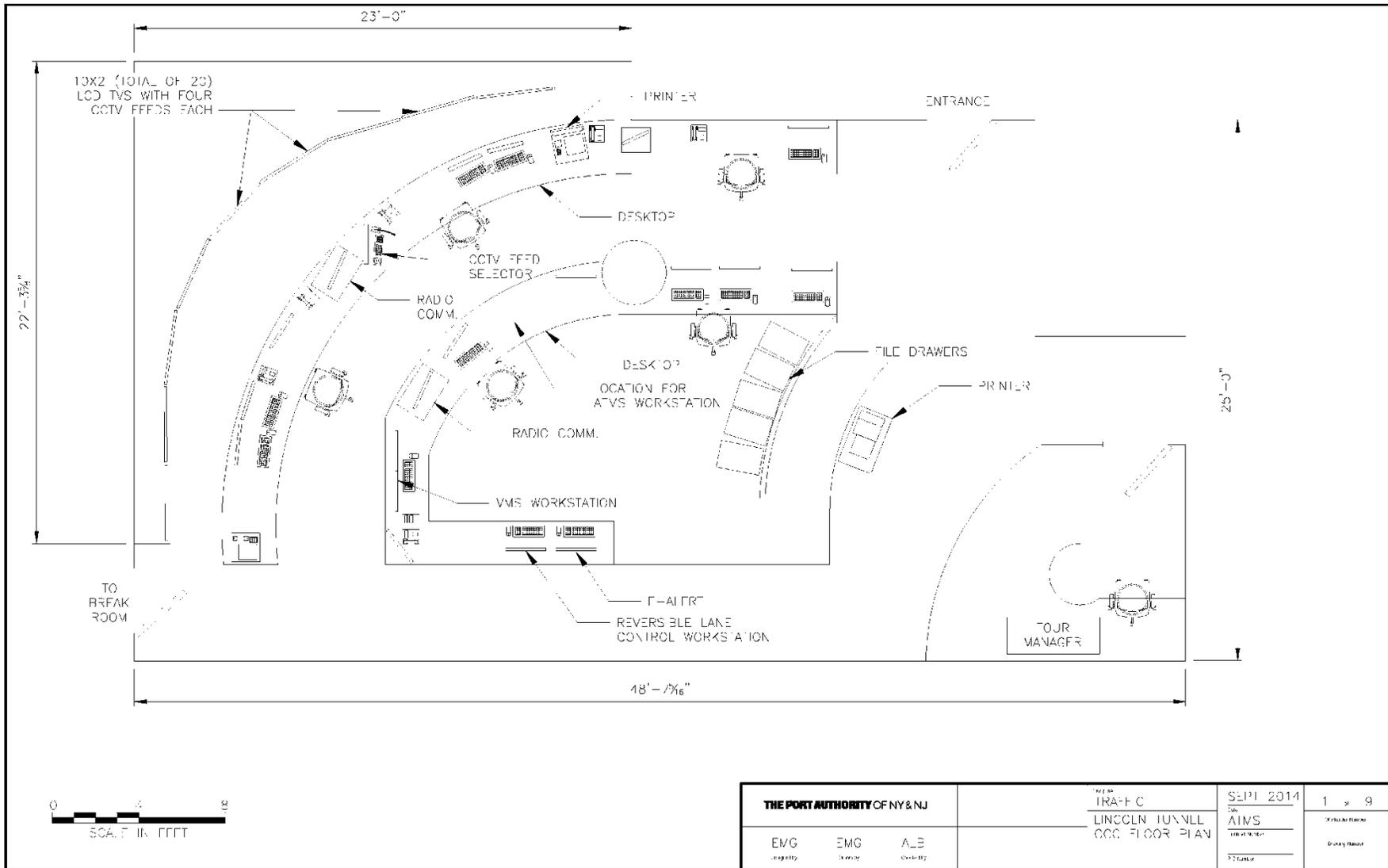
2/8/16

is it interfaced to the AD switch for video switching. The HSQ does not interface with any vehicle detection equipment and does not provide for automated operation from detected traffic conditions.

The next workstation over is the DYNAC DMS workstation. It is very different from HSQ, where HSQ focuses on the approach traffic to and from the tunnel, the DYNAC software focuses on the traffic within the tunnel and on arterial roadways outside of the facility in NY and NJ. A Video-based Stopped Vehicle Detection System does exist in the tunnel through the employment of Citilog. This is to notify the tunnel operators of an immediate occurrence of a stopped vehicle in the tunnel. Video switching is not controlled from DYNAC at this facility and the tour manager uses the video switch board and Nextiva directly. Through the combination of the detection system and the CCTV images on the video wall, the operators can monitor traffic strictly from the video on the wall and then change the DMS, VSLS and LUCS accordingly. The TMS will need to interface to the tunnel Citilog system and provide the necessary alerts in the event of a detected incident. The proper camera of where the incident occurs should be brought up on the operator's main screen.

Travel time data from the TRANSMIT system is fed into the DYNAC software.

Similarly to GWB recommendations, the TMS workstation should have several screens for the four mostly used functions. The array of linear workstations can be consolidated into a single universal workstation or the tour manager with at least four main screens showing the most commonly used functions. Existing DMS are about ten (10) years old except for two (2) full color matrix DMS that were installed in 2013. The following is a complete inventory list of the required devices (both legacy and new), for which the contractor will need to provide System Interfaces (SIs) at LT.



INVENTORY AT LTDynamic Message Signs (DMS)

Manufacturer	Sign Model / Matrix	Qty	Controller Model	Vintage	Protocol	Interface
Daktronics	VF-1320-48x112-6	8	VFC-3000	November 2004	NTCIP	IP
Daktronics	VF-1320-2-16x264-9	1	VFC-3000	September 2004	NTCIP	IP
Daktronics	VF-1320-2-16x336-9	1	VFC-3000	September 2004	NTCIP	IP
Daktronics	VF-2320-64x480-20-RGB	1	VFC-3000	2013	NTCIP	IP
Daktronics	VF-2320-128x128-20-RGB	1	VFC-3000	2013	NTCIP	IP

Vehicle Detection System (VDS)

Manufacturer	Model Description	Qty	Controller Model	Vintage	Protocol	Interface
Citilog	Citilog Video Detection System	18	Video Analyzer	Legacy	-	-
COHU	3930 DSP	72	Camera	Legacy	-	-

Closed Circuit TV System (CCTV)

Manufacturer	Model Description	Qty	Controller Model	Vintage	Protocol	Interface
Verint	Nextiva Video Management Server	1	Nextiva	Version 6	-	Verint SDK
American Dynamics	Analog Video Switch	1	-	Legacy	-	RS-232
COHU	1300 Series	17	-	Legacy	-	-

Lane-Use Control Signals (LUCS)

Existing LUCS on Route 495 approaching the LT facility are used for Exclusive Bus Lane (XBL) Operations during rush hour traffic. The LUCS are operated separately under a SCADA system called HSQ and will remain in operation until such time that the LUCS system is replaced in the future with an NTCIP-compliant system. No TMS interface to the LUCS is anticipated under this project.

2/8/16

TRANSMIT (Travel Time System)

TRANSMIT is a TRANSCOM system that utilizes Kapsch Janus Multi-protocol readers. The TMS is to communicate with TRANSMIT through the use of TRANSCOM's Bridge API, which can be obtained at no cost from TRANSCOM. All TRANSMIT Servers are Windows based and located at the GWB Administration Building. DYNAC utilizes an application on a separate server to interface with TRANSCOM to post travel times on DMS. This function/application must be replicated in the TMS.

ID	Site	# of Reader Cabinets	# of Antennas	XMIT Server	Interface
MH01	Dyer Plaza NY Side	1	8	GWB	Cell Modem
MH02	Galvin Plaza	1	1	GWB	Cell Modem
NJ05	Rte 495 @ Kennedy Blvd	1	5	GWB	Cell Modem
NJ06	495 Helix@ Pleasant Ave	1	6	GWB	Cell Modem
NJ10	Bldv East @ 495 Helix	1	3	GWB	Cell Modem
NJ11	NJ Plaza	1	4	GWB	Cell Modem
PA10	NJ Turnpike before LT	1	2	GWB	Cell Modem
PA11	Route 3 before LT	1	3	GWB	Cell Modem
PA12	Dyer Avenue and 34 th Street	1	3	GWB	Cell Modem
Fut81	10th Avenue & 41st Street	-	-	GWB	-
Fut82	10th Avenue & 30th Street	-	-	GWB	-
Fut83	11th Avenue & 40th Street	-	-	GWB	-

Holland Tunnel (HT)



The Holland Tunnel spans Manhattan, NYC and Jersey City, NJ under the Hudson River using Interstate 78. There is a pair of tubes, each providing two lanes in a 20-foot roadway width. Both tubes are approximately 1.5 miles long.

The Holland Tunnel has a fairly large CommDesk occupied by operators, with the facility tour manager's office just off to the side (but visible) from the CommDesk. Direct communication between rooms is possible without the need for an intercom. The tour manager has a 55-inch large LCD flat panel TV monitor in his office with DYNAC running on the main display. The most commonly used screen from the software displayed is the DMS screen with a windowed section of logged alarms in the lower portion of the screen. According to the tour manager, these are the most important screens he needs to see.

Similar to LT, there is a Video-based Stopped Vehicle Detection system employed in the tunnel through the use of Citilog and the CCTV cameras in the tunnel. The TMS is to interface with the existing CCTV cameras and Citilog system. Detected incidents or events are to automatically bring up an alert and the appropriate CCTV camera image on the large LCD display. For normal camera viewing, the manager prefers to use the separate workstation located behind him with a smaller screen running Verint Nextiva and a keyboard switch for the American Dynamics switch control to access CCTV images. Use of general camera surveillance in the regard is to remain with the Nextiva workstation. A new workstation dedicated for the TMS is to be installed at the CommDesk. In addition to the proposed workstation at the CommDesk, access to the TMS should also be possible from the facility tour manager's office using the existing PC in that location.

The TMS shall also provide complete control over all DMS at the facility based on the scenarios and response plans developed and programmed by the Contractor.

HT operations uses Web-EOC (E-log) for events but stated that multiple entries for the same event is cumbersome and needs to be streamlined into a single entry system. OpenReach has been installed in a separate office on another workstation. It is recommended that OpenReach be installed at the CommDesk. The TMS should be the single system of entry for incidents and events and, in turn, the TMS should populate E-log and OpenReach. This should be typical for all facilities.

Many of the DMS at the facility are about 10 years old and should have the ability to show the actual WYSIWYG message of the signs in the TMS.

The tour managers at this facility prefer to each have their own customized setup within the TMS, or rather profiles, which can be saved and retrieved during their shift.

Travel time data from the TRANSMIT system is presently fed into the DYNAC software. This TRANSMIT interface is to be transferred over to the TMS for travel times.

All traffic signals are operated by Siemens TACTICS as a central traffic management system. The TMS is to interface to the Siemens TACTICS software to allow for pre-emptive triggers based on certain scenarios. Such triggers may be based on an evacuation scenario where extended green signals may be

necessary, or other requested change in traffic signal timings. These are to be specifically determined by the facility when working to develop the scenario/response plans. Iteris video detection is used for intersection control. The TMS is also to interface to the Iteris software to allow for video to be displayed on the video wall.

Similarly to GWB recommendations, the TMS workstation should have several screens for the four mostly used functions. Nextiva CCTV should be in front of the tour manager as part of the same screen array and not behind him. Nextiva does not need to be on the same workstation, but visibly appear to be the same as part of the workstation displays. The intent is to improve efficiency and workflow. The following is a complete inventory list of the required devices (both legacy and new) for which the contractor will need to provide System Interfaces (SIs) at HT.

The existing HT Supervisory Control System (SCS), scheduled to be replaced with a new SCADA system, will be integrated with the Automatic Control System (ACS) software that controls the ventilation and other systems. A common Human Machine Interface (HMI) is slated to operate both systems. The TMS will remain independent of these systems, but some alerts and critical alarms may need to be communicated between SCADA and TMS, as will be determined during the scenario/response plan development phase. However, under the SCADA improvements project a new video wall system is to be furnished and installed, which is intended to replace the legacy mimic board. The new dynamic video wall will display information from SCADA and ACS as well as CCTV video feeds.

The video wall system will consist of LED-based 50-inch diagonal Digital Light Projection (DLP) cubes capable of full HD (1,920 x 1,080) resolution. The video wall will be approximately 36 ft wide by 8 ft high (two rows of cubes by seven across) and controlled by a standard PC being provided under the SCADA project. The TMS is to interface and share the use of this wall to bring up a CCTV camera in response to an event or incident. Additionally, the TMS should be capable of displaying an overview graphic of the tunnel, its VIDS cameras and the status (condition) of traffic within each tunnel. Use of the wall with the TMS should be user-configurable.

INVENTORY AT HT

Dynamic Message Signs (DMS)

Manufacturer	Sign Model / Matrix	Qty	Controller Model	Vintage	Protocol	Interface
Daktronics	VF-13X0-2-16x240-6	9	VFC-3000	October 2004	NTCIP	IP
Daktronics	VF-13X0-2-16x264-9	2	VFC-3000	September 2004	NTCIP	IP

Vehicle Detection System (VDS)

Manufacturer	Model Description	Qty	Controller Model	Vintage	Protocol	Interface
Citilog	Video Detection System	12	Video Analyzer	Legacy	-	-
COHU	3930 DSP	46	Cameras	Legacy	-	-

Closed Circuit TV System (CCTV)

Manufacturer	Model Description	Qty	Controller Model	Vintage	Protocol	Interface
Verint	Nextiva Video Management Server	1	Nextiva	Version 6	-	Verint SDK
American Dynamics	Analog Video Switch	1	-	Legacy	-	RS-232
COHU	Analog Camera	19	-	Legacy	-	-

TRANSMIT (Travel Time System)

TRANSMIT is a TRANSCOM system that utilizes Kapsch Janus Multi-protocol readers. The TMS is to communicate with TRANSMIT through the use of TRANSCOM's Bridge API, which can be obtained at no cost from TRANSCOM. All TRANSMIT Servers are Windows based and located at the GWB Administration Building. DYNAC utilizes an application on a separate server to interface with TRANSCOM to post travel times on DMS. This function/application must be replicated in the TMS.

ID	Site	# of Reader Cabinets	# of Antennas	XMIT Server	Interface
NJ07	HBE/NJTP@Kennedy Blvd	1	2	GWB	Cell Modem
NJ08	HBE/NJTP@Doremus Ave	1	2	GWB	Cell Modem
PA20	Inbound portal NJ side	1	1	GWB	Cell Modem
PA21	Inbound portal NY side	1	1	GWB	Cell Modem
PA22	Jersey Avenue @ 12th St	1	3	GWB	Cell Modem
PA23	Outbound portal NJ side	1	1	GWB	Cell Modem
PA24	Outbound portal NY side	1	1	GWB	Cell Modem

Staten Island Bridges (SIB)



The Staten Island Bridges consist of three Port Authority-owned bridges; the Goethals and the Bayonne Bridges, and the Outerbridge Crossing. All three span from New Jersey to Staten Island and cross the Arthur Kill and the Kill Van Kull. The Bayonne Bridge is currently under construction to have its roadway raised by 64 feet above the existing roadway to allow for a new generation of larger post-Panamax container ships to access the New York

Container Terminal and other New Jersey ports. The Goethals Bridge is being replaced entirely with a new cable-stayed twin span. All three bridges presently have limited ITS assets with the exception of CCTV cameras and/or TRANSMIT sites. However, all three bridges will be seeing ITS deployments in the near future. The Bayonne Bridge will be outfitted with all new ITS assets including Sensys Networks' wireless detection sensors. The scenarios and response plans for this bridge have been fully developed and are an example of the type of scenario/response plan detail that is expected to be developed for the other PA facilities.

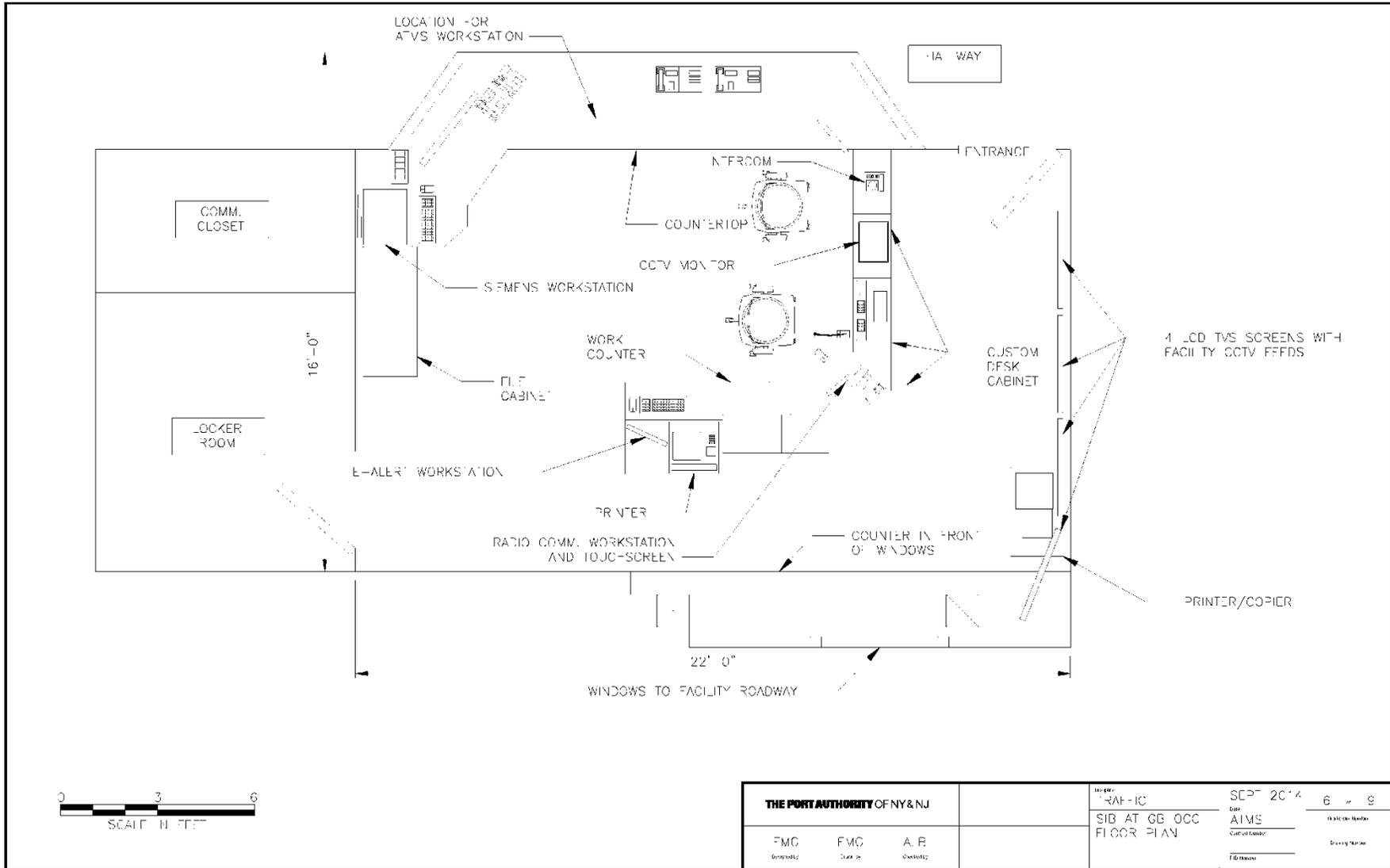
Since the Goethals Bridge is being constructed as a Design-Build-Finance-Maintain (DBFM) project, the final design and layout of ITS has not yet been developed. Guidelines for ITS design of the Goethals Bridge will, however, follow the Bayonne Bridge closely such that type and size of DMS, VLSL, CCTV, and Vehicle Detection is all the same helping to streamline the development of system interfaces. All three bridges will be on the new Verint Nextiva CCTV enterprise solution. CCTV images will reside on the Nextiva CCTV workstation. The only TMS integration with CCTV is for the TMS to bring up the necessary CCTV camera when and where an event on any of the three facilities occurs.

The three bridges are centrally controlled and monitored from the SIB CommDesk located at the Goethals Bridge. Each bridge will have its own local TMS workstation at each respective bridge facility, but central operations and control of the ITS assets is from the Goethals Bridge.

There are plans for an upgrade to the SIB CommDesk, including a new video wall. The schedule for this work is unknown at this time; however, each bridge will likely have one TMS workstation with three screens. The proposed location for this workstation is shown in the provided floor plan of the CommDesk. In addition to the proposed workstation at the CommDesk, access to the TMS should also be possible from the facility tour manager's office using the existing PC in that location.

Like the other TB&T facilities, in order to streamline workflow for the operator, all events and incidents are to be logged into the TMS. The TMS will, in turn, populate the E-log database and OpenReach.

The attached sample is based on the ITS Master Plan for the Bayonne Bridge facility. Defined within are the locations and quantities of ITS field assets, operational scenarios, incident scenarios, and the respective actions to be taken under those scenarios (response plans). Similar plans have been developed under other facility ITS master plans, but it will still be the responsibility of the Contractor to finalize and program the response plans for each TMS instance at each facility and for overall monitoring and control from the PA-AOC.



THE PORT AUTHORITY OF NY & NJ			Project: RA-11C	Sheet: 2014	Date: 6/1/15
			Title: SIB AT GB OCC FLOOR PLAN	Scale: AS SHOWN	Drawing Number:
F.M.C.	F.M.C.	A.P.	Checked by:	Drawn by:	Date:
<small>Proposed</small>	<small>Checked</small>	<small>Reviewed</small>	File Name:	Drawing Name:	Date:

INVENTORY AT GB, OBX, AND BB

The Staten Island Bridges (SIB) consist of the Goethals (GB) and Bayonne Bridges (BB) and the Outerbridge Crossing (OBX). All three facilities are operated from the SIB CommDesk at the Goethals Bridge. The quantities and System Interfaces (SIs) below represent anticipated ITS asset totals for all three bridges.

Dynamic Message Signs (DMS)

Manufacturer	Sign Model / Matrix	Qty	Controller Model	Vintage	Protocol	Interface
Daktronics	VF-2329-96x336-20-RGB	11	VFC-3000	Future	NTCIP	IP
Daktronics	VF-2320-64x192-20-RGB	2	VFC-3000	Future	NTCIP	IP
Daktronics	VF-2320-64x288-20-RGB	2	VFC-3000	Future	NTCIP	IP
Daktronics	VF-2329-64x288-20-RGB	2	VFC-3000	Future	NTCIP	IP

Variable Speed Limit Signs (VSLS)

Manufacturer	Sign Model / Matrix	Qty	Controller Model	Vintage	Protocol	Interface
Daktronics	VS-5220-2-18-W-VSLS	15	VFC-3000	Future	NTCIP	IP

Lane-Use Control Signals (LUCS)

Manufacturer	Sign Model / Matrix	Qty	Controller Model	Vintage	Protocol	Interface
Daktronics	-	11	-	Future	-	IP

Vehicle Detection System (VDS)

Manufacturer	Model Description	Qty	Controller Model	Vintage	Protocol	Interface
Sensys Networks	In-pavement Wireless Detection Sensors	150	AP240-E	Future	NTCIP	IP
Wavetronics Microwave	Non-Pavement-Invasive Detection Sensors	36	Wavetronics	Future	NTCIP	IP

Road Weather Information System (RWIS)

Manufacturer	Model Description	Qty	Controller Model	Vintage	Protocol	Interface
Vaisala Networks	Weather Detection Stations	6	Vaisala	Future	NTCIP	IP

2/8/16

Weigh-In-Motion System (WIM)

Manufacturer	Model Description	Qty	Controller Model	Vintage	Protocol	Interface
IRD	In-pavement Detection Sensors/CCTV images	3 (lanes)	-	Future	NTCIP	IP

Closed Circuit TV System (CCTV)

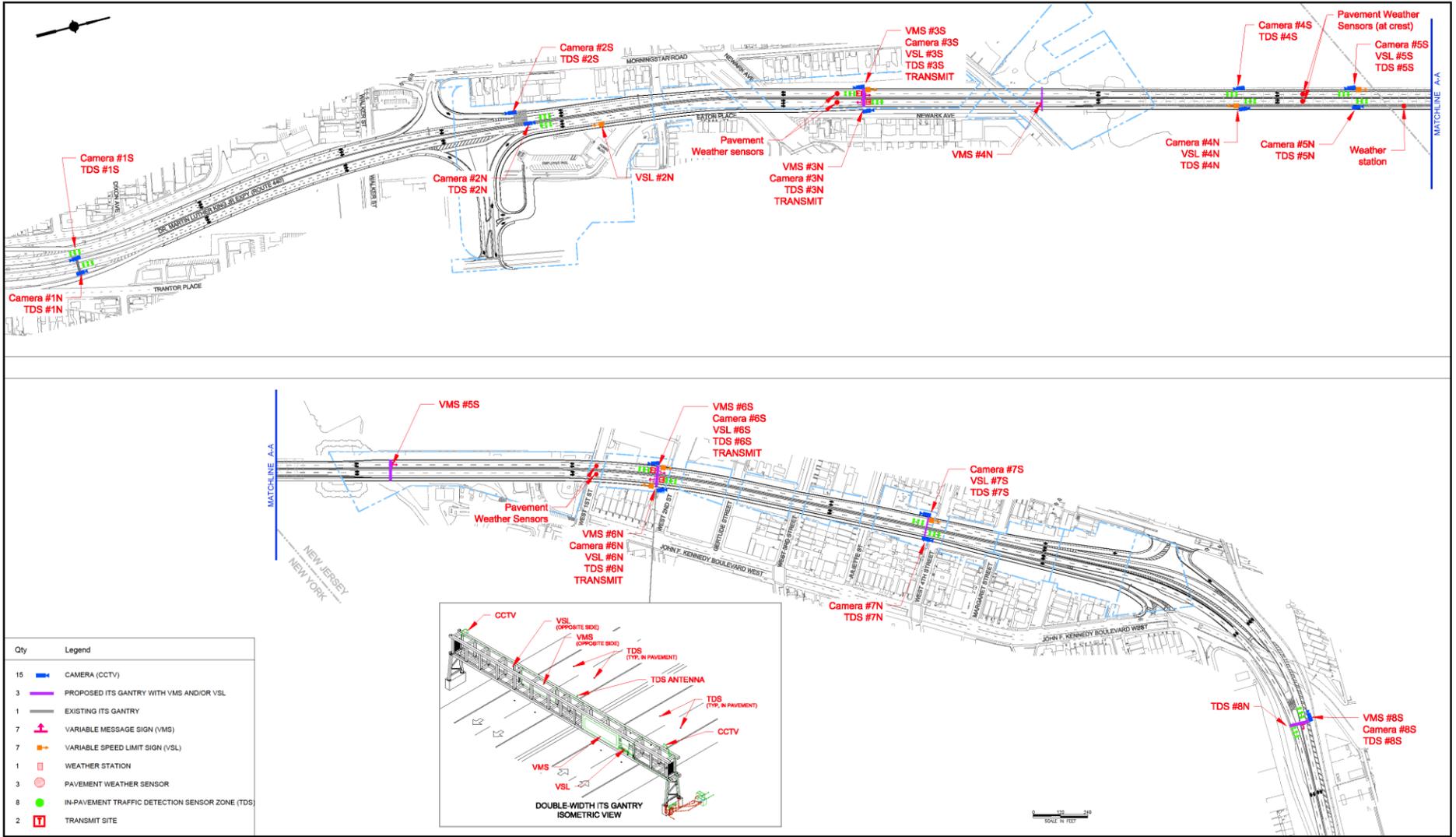
Manufacturer	Model Description	Qty	Controller Model	Vintage	Protocol	Interface
Verint	Nextiva Video Management Server	1	Nextiva	Version 6	-	Verint SDK
-	Camera	51	-	Future	-	IP

TRANSMIT (Travel Time System)

TRANSMIT is a TRANSCOM system that utilizes Kapsch Janus Multi-protocol readers. The TMS is to communicate with TRANSMIT through the use of TRANSCOM’s Bridge API, which can be obtained at no cost from TRANSCOM. All TRANSMIT Servers are Windows based and located at the GWB Administration Building.

ID	Site	# of Lanes	# of Reader Cabinets	# of Antennas	XMIT Server	Interface
-	Goethals Bridge	4	1	3	GWB	Cell Modem
-	Goethals Bridge	4	1	3	GWB	Cell Modem
-	Goethals Bridge	4	1	3	GWB	Cell Modem
-	Goethals Bridge	4	1	3	GWB	Cell Modem
NJ01	I-278 @ Brunswick Ave (Goethals Bridge)	4	1	3	GWB	Cell Modem
PA31	I-278 Near GB Toll Plaza (Goethals Bridge)	4	1	3	GWB	Cell Modem
NJ09	North Approach (Bayonne Bridge)	3	1	2	GWB	Cell Modem
PA36	South Approach (Bayonne Bridge)	3	1	2	GWB	Cell Modem

ITS DEPLOYMENT PLAN



BAYONNE BRIDGE REPLACEMENT OF MAIN SPAN ROADWAY & APPROACH STRUCTURES

THE PORT AUTHORITY
OF NY & NJ

TRAFFIC

PANY&NJ Bayonne Bridge Navigational Clearance Program (BBNCP)

Bayonne Bridge
ITS Operational Scenarios

Updated: 11-28-2012

Heading Northbound

Proposed					Bayonne Facility Messages																	
Zone ²	Device Info.	Device Sta.	Mounting Method	Traffic Detectors	CCTV Cameras	Scenario 1 ¹	Scenario 2 ¹	Scenario 3 ¹	Scenario 4 ¹	Scenario 5	Scenario 6	Scenario 7	Scenario 8	Scenario 9	Scenario 10	Scenario 11	Scenario 12	Scenario 13	Scenario 14	Scenario 15	Scenario 16	
						SB Left Lane Closure	SB Right Lane Closure	NB Left Lane Closure	NB Right Lane Closure	SB Full Bridge Closure	NB Full Bridge Closure	SB Rt 440 Full Closure S. of Bayonne Br.	NB Rt 440 Full Closure N. of Bayonne Br.	Full Bridge Closure	High Winds	High Winds (Restrictions)	Ice or Snow	Incident on Bridge ³	NYC Marathon	MTA Closures	Normal Condition	
Zone 1	VMS-1N ⁴	-4+80	Single Overhead Walk-through	In-pavement Vehicle Detection	Camera #1N			MUTCD SIGN W3-5 LEFT LANE CLOSED AHEAD	MUTCD SIGN W3-5 RIGHT LANE CLOSED AHEAD		BAYONNE BR CLOSED USE EXIT 13			MUTCD SIGN W3-5 RT 440 CLOSED AHEAD USE Kennedy Blvd	BAYONNE BR CLOSED USE EXIT 13	MUTCD SIGN W3-5 CAUTION HIGH WINDS REDUCE SPEED	MUTCD SIGN W3-5 ALL TRUCKS USE EXIT 13	MUTCD SIGN W3-5 CAUTION ICING (SNOW) REDUCE SPEED		TRAFFIC ALERT NYC MARATHON X TO Y EXPECT DELAYS	SUBWAY LIRR ALERT XY LINES SUSPENDED	
		15+80	Toll Gantry		Camera #2N, 2S																	
Zone 2	VSL-2N	19+28	Parapet Mount	In-pavement Vehicle Detection		45 MPH	45 MPH	30 MPH	30 MPH	45 MPH		45 MPH	30 MPH		30 MPH	30 MPH	30 MPH			45 MPH	45 MPH	45 MPH
Zone 3	VMS-3N	31+00	Double Overhead Walk-through	In-pavement Vehicle Detection & TRANSMIT	Camera #3N			LEFT LANE CLOSED AHEAD	RIGHT LANE CLOSED AHEAD				RT 440 CLOSED AHEAD USE Kennedy Blvd		CAUTION HIGH WINDS REDUCE SPEED	MUTCD SIGN R5-2 NO TRUCKS	CAUTION ICING (SNOW) REDUCE SPEED					
Zone 4	VMS-4N	39+00	Static Panel Structure	In-pavement Vehicle Detection																		
	VSL-4N	47+50	Portal Mount		Camera #4N, 4S	45 MPH	45 MPH	30 MPH	30 MPH	45 MPH		45 MPH	30 MPH		30 MPH	30 MPH	30 MPH			45 MPH	45 MPH	45 MPH
Zone 6	VSL-6N	72+65	Double Overhead Walk-through	In-pavement Vehicle Detection & TRANSMIT	Camera #6N	45 MPH	45 MPH	30 MPH	30 MPH	45 MPH		45 MPH	30 MPH		30 MPH	30 MPH	30 MPH			45 MPH	45 MPH	45 MPH
	VMS-6N														RT 440 CLOSED AHEAD USE Kennedy Blvd		CAUTION HIGH WINDS REDUCE SPEED		CAUTION ICING (SNOW) REDUCE SPEED			TRAFFIC ALERT NYC MARATHON X TO Y EXPECT DELAYS
Camera Controlled Activity by ATMS ⁴								All cameras active, Cameras #1N through 7N on priority screens	All cameras active, Cameras #1N through 7N on priority screens		All Cameras active, Cameras #6S and #2N on priority screens			All cameras active, Cameras #6N and 7N on priority screens	All cameras active, Cameras #6S and #2N on priority screens	All cameras active, selection to priority screens based on need	All cameras active, selection to priority screens based on need	All cameras active, selection to priority screens based on need	All Cameras active, Cameras #3N, 4N, 5S and 6S on priority screens	All cameras active, selection to priority screens based on need	All cameras active, selection to priority screens based on need	

Heading Southbound

Proposed					Bayonne Facility Messages																	
Zone ²	Device Info.	Device Sta.	Mounting Method	Traffic Detectors	CCTV Cameras	Scenario 1 ¹	Scenario 2 ¹	Scenario 3 ¹	Scenario 4 ¹	Scenario 5	Scenario 6	Scenario 7	Scenario 8	Scenario 9	Scenario 10	Scenario 11	Scenario 12	Scenario 13	Scenario 14	Scenario 15	Scenario 16	
						SB Left Lane Closure	SB Right Lane Closure	NB Left Lane Closure	NB Right Lane Closure	SB Full Bridge Closure	NB Full Bridge Closure	SB Rt 440 Full Closure S. of Bayonne Br.	NB Rt 440 Full Closure N. of Bayonne Br.	Full Bridge Closure	High Winds	High Winds (Restrictions)	Ice or Snow	Incident on Bridge ³	NYC Marathon	MTA Closures	Normal Condition	
Zone 8	VMS-8S	104+30	Double Overhead Walk-through	In-pavement Vehicle Detection	Camera #8S	MUTCD SIGN W3-5 REDUCED SPEED AHEAD	MUTCD SIGN W3-5 REDUCED SPEED AHEAD			BAYONNE BR CLOSED EXIT AVENUE A		MUTCD SIGN W3-5 RT 440 CLOSED AHEAD USE EXIT 13		BAYONNE BR CLOSED EXIT AVENUE A	MUTCD SIGN W3-5 CAUTION HIGH WINDS REDUCE SPEED	MUTCD SIGN W3-5 ALL TRUCKS EXIT AVENUE A	MUTCD SIGN W3-5 CAUTION ICING (SNOW) REDUCE SPEED			TRAFFIC ALERT NYC MARATHON X TO Y EXPECT DELAYS	CAUTION HIGH WINDS REDUCE SPEED	
Zone 7	VSL-7S	84+70	Static Panel Overhead Structure	In-pavement Vehicle Detection	Camera #7N, 7S	30 MPH	30 MPH	45 MPH	45 MPH		45 MPH	30 MPH	45 MPH		30 MPH	30 MPH	30 MPH			45 MPH	45 MPH	45 MPH
Zone 6	VSL-6S	72+65	Double Overhead Walk-through (ITS Gantry-3)	In-pavement Vehicle Detection & TRANSMIT	Camera #6S	30 MPH	30 MPH	45 MPH	45 MPH		45 MPH	30 MPH	45 MPH		30 MPH	30 MPH	30 MPH			45 MPH	45 MPH	45 MPH
	VMS-6S					LEFT LANE CLOSED AHEAD	RIGHT LANE CLOSED AHEAD						RT 440 CLOSED AHEAD USE EXIT 13		CAUTION HIGH WINDS REDUCE SPEED	MUTCD SIGN R5-2 NO TRUCKS	CAUTION ICING (SNOW) REDUCE SPEED			TRAFFIC ALERT NYC MARATHON X TO Y EXPECT DELAYS	SUBWAY LIRR ALERT XY LINES SUSPENDED	
Zone 5	VMS-5S	62+00	Cantilever	In-pavement Vehicle Detection																		
	VSL-5S	52+50	Portal Mount		Camera #5N, 5S	30 MPH	30 MPH	45 MPH	45 MPH		45 MPH	30 MPH	45 MPH		30 MPH	30 MPH	30 MPH			45 MPH	45 MPH	45 MPH
Zone 3	VSL-3S	31+00	Double Overhead Walk-through (ITS Gantry-2)	In-pavement Vehicle Detection & TRANSMIT	Camera #3S	30 MPH	30 MPH	45 MPH	45 MPH		45 MPH	30 MPH	45 MPH		30 MPH	30 MPH	30 MPH			45 MPH	45 MPH	45 MPH
	VMS-3S														RT 440 CLOSED AHEAD USE EXIT 13		CAUTION HIGH WINDS REDUCE SPEED		CAUTION ICING (SNOW) REDUCE SPEED			TRAFFIC ALERT NYC MARATHON X TO Y EXPECT DELAYS
Camera Controlled Activity by ATMS ⁴						All cameras active, Cameras #2S through #5S on priority screens	All cameras active, Cameras #2S through #5S on priority screens			All Cameras active, Cameras #6S and #2N on priority screens			All cameras active, Cameras #2S and 3S on priority screens	All cameras active, Cameras #6S and #2N on priority screens	All cameras active, selection to priority screens based on need	All cameras active, selection to priority screens based on need	All cameras active, selection to priority screens based on need	All Cameras active, Cameras #3N, 4N, 5S and 6S on priority screens	All cameras active, selection to priority screens based on need	All cameras active, selection to priority screens based on need		

NOTES:

- 1) For Scenarios 1 through 4, NB and SB lane closures are assumed to be on the bridge.
- 2) For Zone location references, see "Detection Zones"
- 3) For "Incident on Bridge" Scenarios see "ITS Detection Scenarios"
- 4) All cameras have PTZ capability and can look in both directions, for camera redundancy.
- 5) VMS-1N is located on NYSOT property (approximately 480 feet south of the Port Authority property line).

**Bayonne Bridge
ITS Detection Scenarios**

Updated: 11-28-2012

Heading Northbound

Proposed			Detection Zones		Incident Scenarios					
Device Info.	Device Sta.	Mounting Method	Zone ¹	Traffic Detectors	Incident Scenario A NB N. Side of N. Approach	Incident Scenario B NB S. Side of N. Approach	Incident Scenario C SB N. Side of S. Approach	Incident Scenario D SB S. Side of S. Approach	Incident Scenario E NB on Main Span	Incident Scenario F SB on Main Span
VMS-1N	-4+80	Single Overhead Walk-through	Zone 1	✓	MUTCD SIGN W3-6 ACCIDENT AHEAD BE PREPARED TO STOP	MUTCD SIGN W3-6 ACCIDENT AHEAD BE PREPARED TO STOP			MUTCD SIGN W3-6 ACCIDENT AHEAD BE PREPARED TO STOP	
VSL-2N	19+28	Parapet Mount	Zone 2	✓	30 MPH	30 MPH	45 MPH	45 MPH	30 MPH	45 MPH
VMS-3N	31+00	Double Overhead Walk-through	Zone 3	✓	ACCIDENT AHEAD BE PREPARED TO STOP				ACCIDENT AHEAD BE PREPARED TO STOP	
VMS-4N	39+00	Static Panel Structure	Zone 4		SLOW (STOPPED) TRAFFIC AHEAD ³	SLOW (STOPPED) TRAFFIC AHEAD ³	SLOW (STOPPED) TRAFFIC AHEAD ³	SLOW (STOPPED) TRAFFIC AHEAD ³	SLOW (STOPPED) TRAFFIC AHEAD ³	SLOW (STOPPED) TRAFFIC AHEAD ³
VSL-4N	47+50	Portal Mount		✓	30 MPH	30 MPH	45 MPH	45 MPH	30 MPH	45 MPH
VSL-6N	72+65	Double Overhead Walk-through	Zone 6	✓	30 MPH	30 MPH	45 MPH	45 MPH	30 MPH	45 MPH
VMS-6N					ACCIDENT AHEAD BE PREPARED TO STOP					
Camera Controlled Activity by ATMS ²					All cameras active. Camera #7N on priority screen	All cameras active. Camera #8N on priority screen	All cameras active	All cameras active	All cameras active. Camera #4N on priority screen	All cameras active

Heading Southbound

Proposed			Detection Zones		Incident Scenarios					
Device Info.	Device Sta.	Mounting Method	Zone ¹	Traffic Detectors	Incident Scenario A NB N. Side of N. Approach	Incident Scenario B NB S. Side of N. Approach	Incident Scenario C SB N. Side of S. Approach	Incident Scenario D SB S. Side of S. Approach	Incident Scenario E NB on Main Span	Incident Scenario F SB on Main Span
VMS-8S	104+30	Double Overhead Walk-through	Zone 8	✓			MUTCD SIGN W3-6 ACCIDENT AHEAD BE PREPARED TO STOP	MUTCD SIGN W3-6 ACCIDENT AHEAD BE PREPARED TO STOP		MUTCD SIGN W3-6 ACCIDENT AHEAD BE PREPARED TO STOP
VSL-7S	84+70	Static Panel Structure	Zone 7	✓	45 MPH	45 MPH	30 MPH	30 MPH	45 MPH	30 MPH
VSL-6S	72+65	Double Overhead Walk-through (ITS Gantry-3)	Zone 6	✓	45 MPH	45 MPH	30 MPH	30 MPH	45 MPH	30 MPH
VMS-6S							ACCIDENT AHEAD BE PREPARED TO STOP		ACCIDENT AHEAD BE PREPARED TO STOP	
VMS-5S	62+00	Cantilever	Zone 5		SLOW (STOPPED) TRAFFIC AHEAD ³	SLOW (STOPPED) TRAFFIC AHEAD ³	SLOW (STOPPED) TRAFFIC AHEAD ³	SLOW (STOPPED) TRAFFIC AHEAD ³	SLOW (STOPPED) TRAFFIC AHEAD ³	SLOW (STOPPED) TRAFFIC AHEAD ³
VSL-5S	52+50	Portal Mount		✓	45 MPH	45 MPH	30 MPH	30 MPH	45 MPH	30 MPH
VSL-3S	31+00	Double Overhead Walk-through	Zone 3	✓	45 MPH	45 MPH	30 MPH	30 MPH	45 MPH	30 MPH
VMS-3S							ACCIDENT AHEAD BE PREPARED TO STOP			
Camera Controlled Activity by ATMS ²					All cameras active	All cameras active	All cameras active. Camera #6S on priority screen	All cameras active. Camera #3S on priority screen	All cameras active	All cameras active. Camera #4S on priority screen

NOTES:

- 1) For Zone location references, see "Detection Zones"
- 2) All cameras have PTZ capability and can look in both directions, for camera redundancy.
- 3) Messages to be displayed automatically based upon detection. 0-15 MPH display STOPPED TRAFFIC, 16-30 MPH display SLOW TRAFFIC. Messages can appear on signs independent of all other VMS's.

**THE PORT AUTHORITY
OF NY & NJ**

HDR/PB, A JOINT VENTURE
HNTB CORPORATION

JOHN ORMAN
N.Y. Professional Engineer # 24CE03969100

JOHN ORMAN
N.Y. Professional Engineer # 089823

No.	Date	Revision	Approved

ENGINEERING DEPARTMENT

**BAYONNE
BRIDGE**

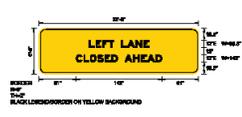
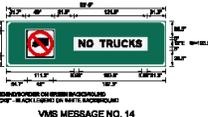
TRAFFIC

Title
REPLACEMENT OF MAIN SPAN ROADWAY
AND APPROACH STRUCTURES

**ITS VMS
DISPLAY LAYOUT**

The drawing is subject to modification in accordance with the project's needs. All modifications shall be approved by the project manager. The drawing is not to be used for construction purposes without the approval of the project manager. The drawing is not to be used for any other purpose without the approval of the project manager. The drawing is not to be used for any other purpose without the approval of the project manager.

H. CALERO H. CALERO J. ORMAN
Designed by Drawn by Checked by
Date 02/15/2013
Contract Number AKB-264.039
Drawing Number T
PID# 08431000



MESSAGE NO.	ITS SCENARIOS	VMS SIGN NO.
1	A, B, D, E, F	1N, 3N, 3N, 6N, 8N
2	12	1N, 3N, 3N, 6N, 8N
3	12	1N, 3N, 3N, 6N, 8N
4	10	1N, 3N, 3N, 6N, 8N
6	2, 4	3N, 6N
8	1, 3	3N, 6N
7	6, 9	6N
8	15	1N, 3N, 6N, 8N
9	14	1N, 3N, 6N, 8N, 2N
10	8	1N, 3N, 6N
11	7	6N, 8N
12	8, 9	1N
13	A THROUGH F	4N, 6N
14	11	3N, 6N
16	10	6N
18	11	1N
17	11	6N
18	4	1N
19	3	1N
20	1, 2	6N
21	7	6N
22	A, C, D, F	1N
25	C, D, F	6N
24	A THROUGH F	4N, 6N
25	12	6N
26	12	6N
27	A, B, E	6N

John F. Kennedy International Airport (JFK)



JFK International Airport is located in the borough of Queens in New York City about twelve (12) miles southeast of lower Manhattan. It is one of the busiest international gateway airports to the United States and the leading freight gateway by value of shipments. There are multiple operations control centers (OCC) on the airport property. The focus of this project deals with landside operations only.

JFK has three OCCs dealing with landside operations. One mostly deals with the observance of cameras owned by AirTrain and is situated within a set of cubicles and high monitors on the wall in an office-like environment, the second OCC is large with a fairly large video wall using current technology. Screens and workstation are dedicated by function, by virtue of the client software installed on a particular machine. The third OCC is seasonal and is referred to as the snow center. This OCC is active upon snow storms and is a sizeable elongated room with terminals for CCTV and Automatic Vehicle Location (AVL) called "In-Fleet" where plows can be tracked and monitored. There will be one instance of the TMS installed at JFK to be located in the second OCC. The floor plan layout with the TMS workstation location is shown below.

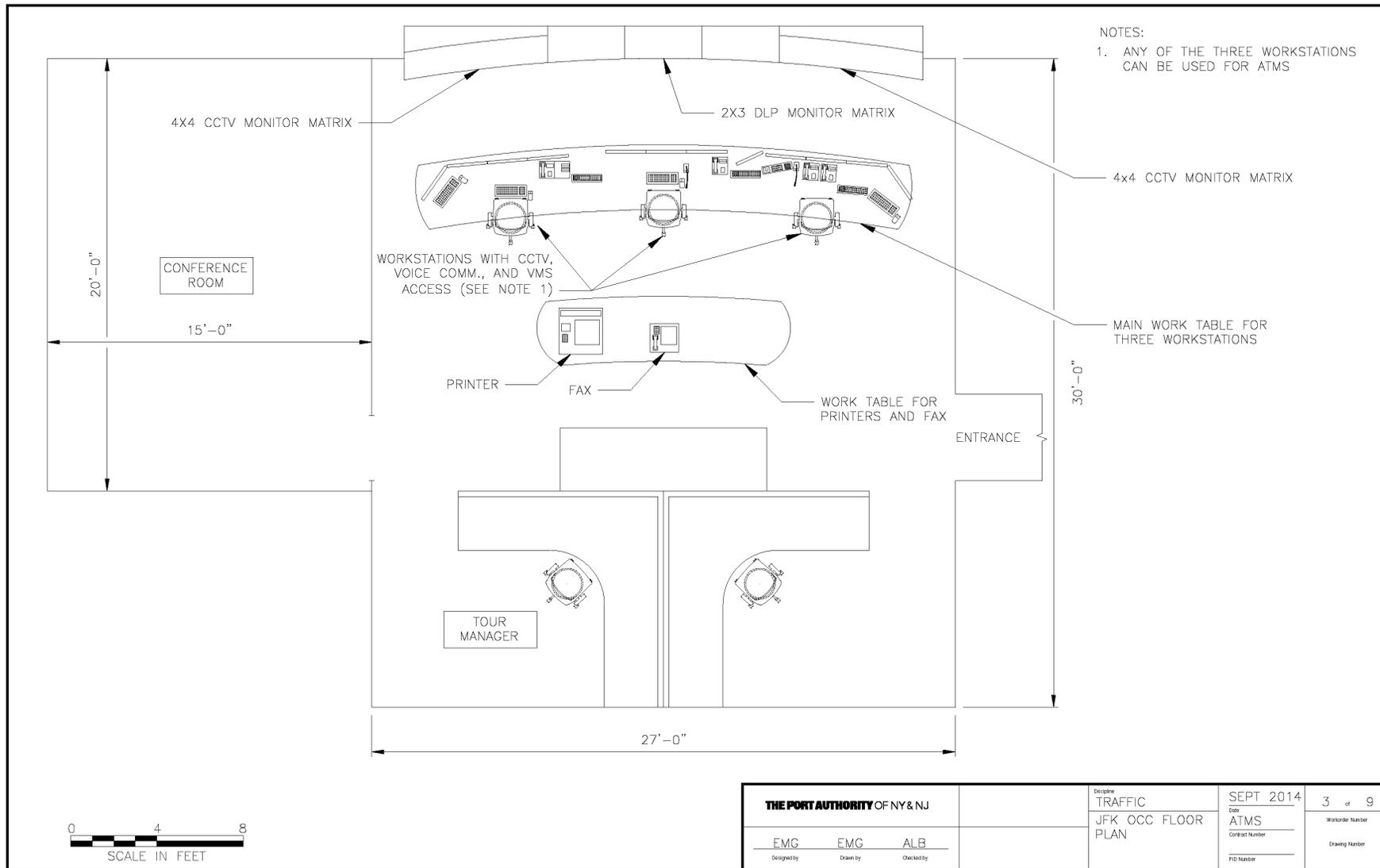
Roadways and arterials around JFK such as the Van Wyck Expressway (I-687), Nassau Expressway, Belt Parkway and JFK Expressway are all identified as having the need to convey delays to motorists. For local operations, this is one of the major requirements of the software. Working closely with the facility, the Contractor shall develop scenario and response plans based on the JFK ITS Master Plan that will be provided after award of this contract.

OpenReach will be installed at the facility. Similar to all other facilities, the logging of events, incidents, or delays are to be entered into the TMS and, in turn, the TMS should populate the E-log and OpenReach systems.

DMS for landside operations at JFK were upgraded about three (3) years ago. A total of 47 DMS are all recent Daktronics model signs that will need to be interfaced to the TMS. No VSLs exist. There is limited vehicle detection at the facility using VIDS technology. The JFK ITS master plan includes the installation of additional DMS, CCTV surveillance cameras and vehicle detectors to monitor volume, occupancy, and speed.

Over-Height Vehicle Detection (OHVD) could be employed at the Central Terminal Area and there is room for an escape route for over-height vehicles. This may be included in the final JFK ITS master plan.

All traffic signals are operated by Siemens TACTICS as a central traffic management system. The TMS is to interface to the Siemens TACTICS software to allow for pre-emptive triggers based on certain scenarios. Such triggers may be based on an evacuation scenario where extended green signals may be necessary, or other requested change in traffic signal timings. These are to be specifically determined by the facility when working to develop the scenario/response plans.



2/8/16

INVENTORY FOR JFK

Dynamic Message Signs (DMS)

Manufacturer	Sign Model / Matrix	Qty	Controller Model	Vintage	Protocol	Interface
Daktronics	VF-2350-16x112-34-A	3	VFC-3000	August 2011	NTCIP	IP
Daktronics	VF-2350-8x96-34-A	5	VFC-3000	August 2011	NTCIP	IP
Daktronics	VF-2350-16x128-34-A	1	VFC-3000	August 2011	NTCIP	IP
Daktronics	VF-2350-8x112-34-A	2	VFC-3000	August 2011	NTCIP	IP
Daktronics	VF-2320-16x160-20-A	2	VFC-3000	March 2011	NTCIP	IP
Daktronics	AF-3400-32x128-20-A-SF-120	2	VFC-3000	October 2008	NTCIP	IP
Daktronics	VF-1350-8x112-9-A, IMP W/TAC	4	VFC-3000	May 2007	NTCIP	IP
Daktronics	VF-1350-8x128-9-A, IMP W/TAC	1	VFC-3000	May 2007	NTCIP	IP
Daktronics	VF-1350-24x128-9-*, IMP W/TAC	8	VFC-3000	May 2007	NTCIP	IP
Daktronics	VF-1350-8x152-9-A, IMP W/TAC	6	VFC-3000	May 2007	NTCIP	IP
Daktronics	VF-1350-8x176-9-A, IMP W/TAC	1	VFC-3000	May 2007	NTCIP	IP
Daktronics	VF-1350-8x208-9-A, IMP W/TAC	1	VFC-3000	May 2007	NTCIP	IP
Daktronics	VF-1320-56x192-9-A	1	VFC-3000	May 2007	NTCIP	IP
Daktronics	VF-1350-24x112-9-A	4	VFC-3000	April 2007	NTCIP	IP
Daktronics	VF-1320-56x168-9-A	1	VFC-3000	March 2007	NTCIP	IP
Daktronics	VF-1350-24x88-9-*	5	VFC-3000	June 2006	NTCIP	IP

2/8/16

Vehicle Detection System (VDS)

Manufacturer	Model Description	Qty	Controller Model	Vintage	Protocol	Interface
Autoscope	Rackvision Image Sensor Model AIS Color Zoom Camera	5	-	Legacy	-	-

Closed Circuit TV System (CCTV)

Manufacturer	Model Description	Qty	Controller Model	Vintage	Protocol	Interface
Verint	Nextiva Video Management Server	1	Nextiva	Version 6	-	Verint SDK
American Dynamics	Analog Video Switch	1	-	Legacy	-	RS-232
COHU	Analog Camera Model 3925	21	-	Analog - Encoder	-	-
COHU	Analog Camera Model 3965	6	-	Analog - Encoder	-	-

TRANSMIT (Travel Time System)

TRANSMIT is a TRANSCOM system that utilizes Kapsch Janus Multi-protocol readers. The TMS is to communicate with TRANSMIT through the use of TRANSCOM's Bridge API, which can be obtained at no cost from TRANSCOM. All TRANSMIT Servers are Windows based and located at the GWB Administration Building.

ID	Site	# of Reader Cabinets	# of Antennas	XMIT Server	Interface
JFK01	VWE @ Monorail	1	4	GWB	Cell Modem
JFK02	VWE @ S. Service Rd.	1	4	GWB	Cell Modem
JFK03	JFK Exp @ S. Cargo Rd.	1	4	GWB	Cell Modem
JFK04	JFK Exp @ 150th Ave.	1	4	GWB	Cell Modem

Newark Liberty International Airport (EWR)



EWR is located about fifteen (15) miles southwest of midtown Manhattan in New York City, straddling Newark and Elizabeth, NJ.

There are several operations control centers on the facility, but the main OCC dealing with security and landside operations is located in Building 1 near the north terminal area. EWR OCC allows for communications with an adjacent Emergency Operations Center (EOC) and yet has privacy separation when needed. Workstations are universal in that each one has the ability to perform several of the same functions as the other, which allows for redundancy and ease of maintenance without down time. Workstations are ergonomically oriented with multiple screens sharing a common mouse and keyboard through a hardwired KVM. One of the existing workstations in the back row as shown on the floor plan is to run the TMS in conjunction with other functions at that workstation. In addition to the workstation in the OCC, access to the TMS should also be possible from the facility manager's office using the existing PC in that location as well.

The video wall is an array of CRT screens, which is controlled by an American Dynamics video switch. Operations indicated that the number of video screens displayed is plenty for those observing. Video can also be displayed at the workstations. While most of the security cameras are on the new Nextiva enterprise system, many of the legacy surveillance cameras are not yet. The Nextiva Enterprise system is being implemented Agency-wide but the schedule for full conversion is unknown at this time.

There are only a handful of CCTV cameras on landside around the facility. Operations stated that it is not enough to cover the access roadways.

GPS is employed on snow vehicles and on buses using the In-Fleet AVL system. The AVL system will not be interfaced to the TMS.

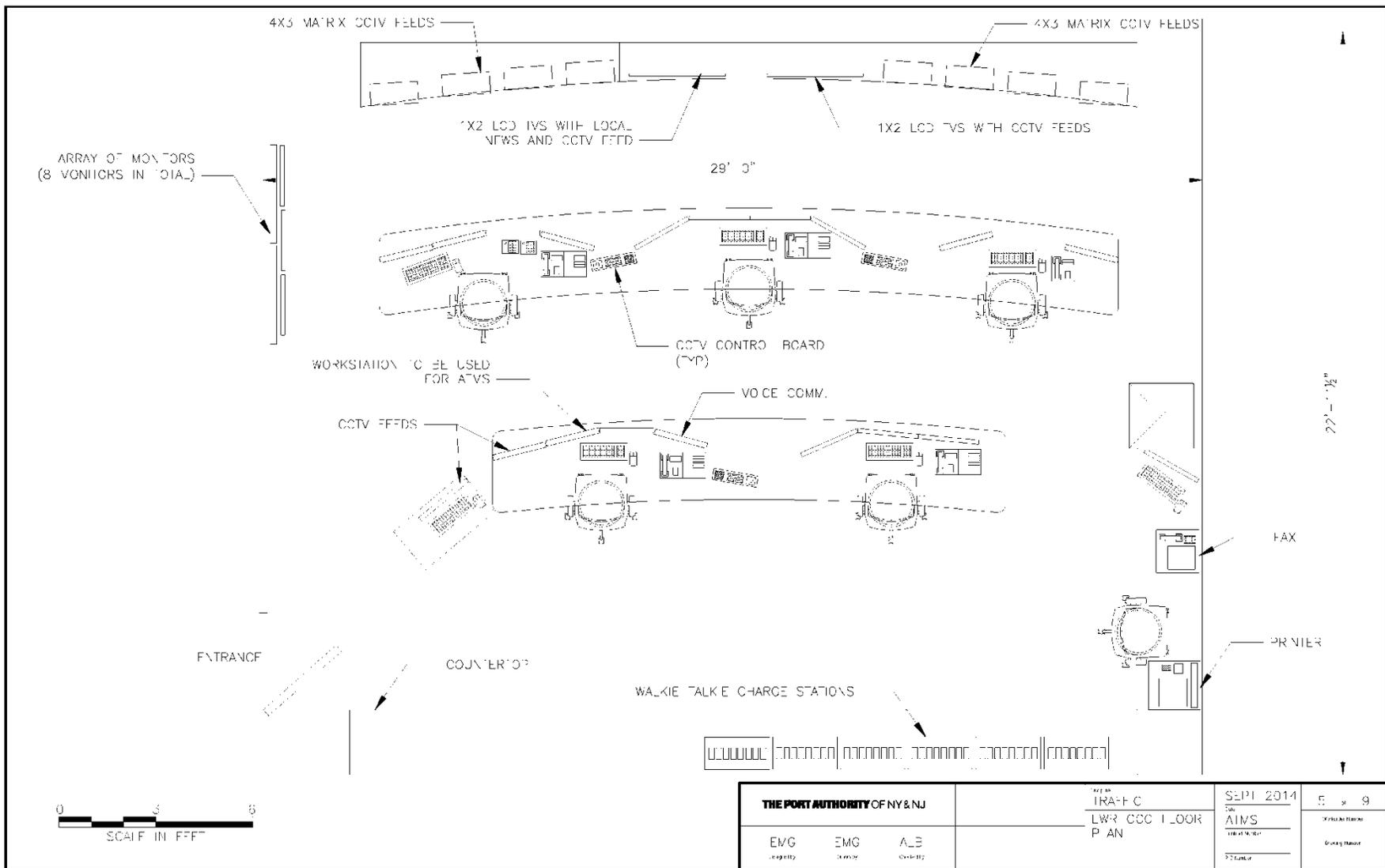
All traffic signals will, in the future, be operated by Siemens TACTICS as a central traffic management system. The TMS is to interface to the Siemens TACTICS software to allow for pre-emptive triggers based on certain scenarios. Such triggers may be based on an evacuation scenario where extended green signals may be necessary, or other requested change in traffic signal timings. These are to be specifically determined by the facility when working to develop the scenario/response plans.

EWR will not need any workstation or video wall configuration upgrade for the TMS, other than the integration of video switching from event-driven triggers within and by the TMS.

INVENTORY FOR EWR

Closed Circuit TV System (CCTV)

Manufacturer	Model Description	Qty	Controller Model	Vintage	Protocol	Interface
Verint	Nextiva Video Management Server	1	Nextiva	Version 6	-	Verint SDK
American Dynamics	Analog Video Switch	1	-	Legacy	-	RS-232
-	Camera	7	-	Legacy	-	-



LaGuardia Airport (LGA)



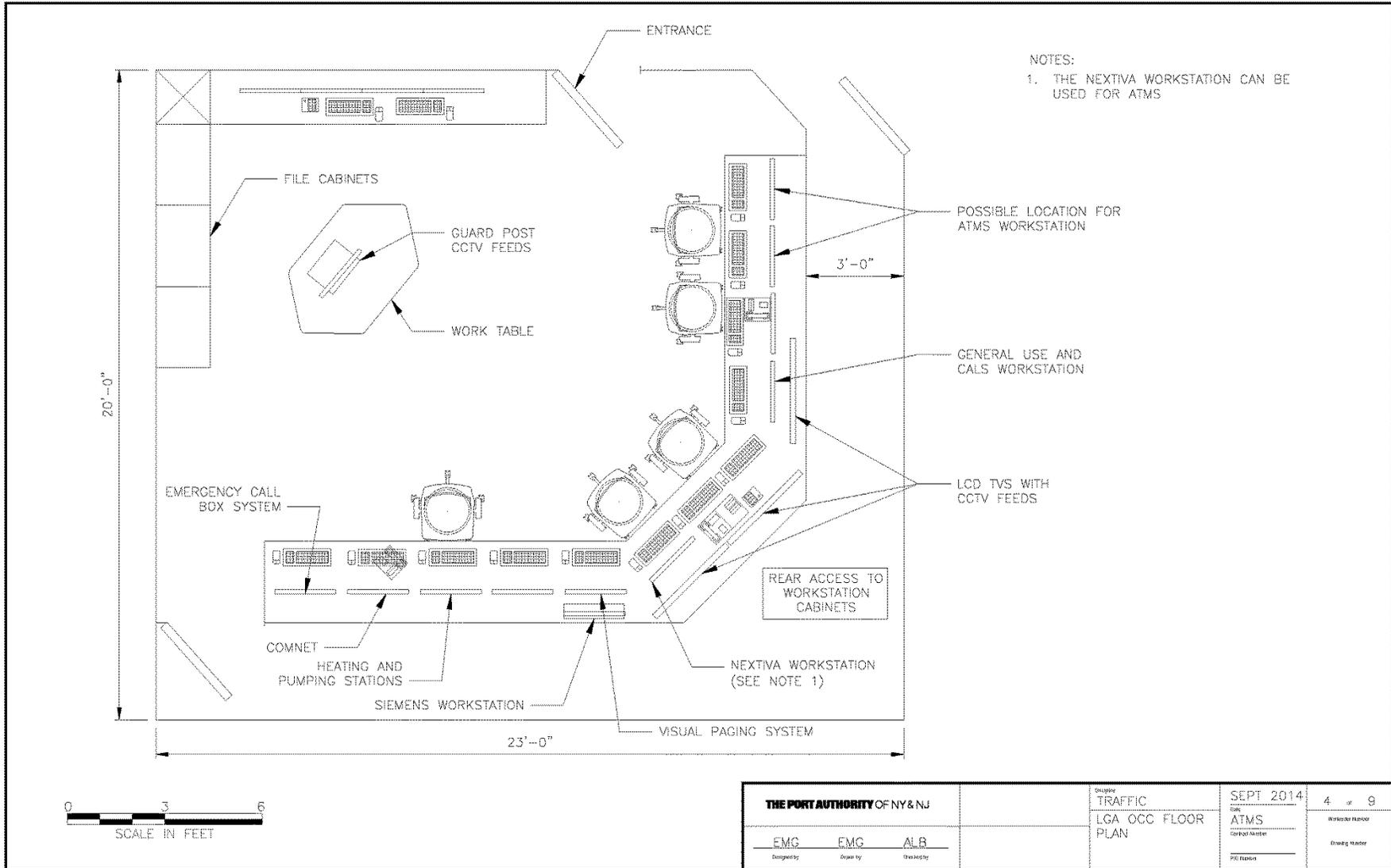
LGA is located in the northern part of the New York City borough of Queens. It is located on the waterfront of Flushing Bay and Bowery Bay and borders the neighborhoods of Astoria, Jackson Heights, and East Elmhurst. LGA is currently undergoing a major redevelopment program. It involves full demolition and rebuilding of Central Terminal, the parking structures and all access roads leading in and out of the airport.

There are few landside cameras overseeing the entrances and parking lots. Much of this will change with the start of construction, which will provide for a new Terminal Building, multi-level parking garages, and revised access roads.

Under the new LGA ITS master plan, Sensys Networks' in-pavement wireless detection will be employed at the entrance ramps and exits to and from the airport.

The facility mostly has portable DMS positioned throughout. These are locally programmed at the sign trailers themselves. A total of 27 permanent DMS (Daktronics) do exist and are remotely controlled using the standard Vanguard software and in the future 28 DMS will replace them as part of the LGA ITS master plan implementation. All permanent DMS are to be controlled from the TMS. Signs are currently controlled from the facility manager's office to provide ad-hoc messages only. In addition to the proposed workstation in the OCC, access to the TMS should also be possible from the facility manager's office using the existing PC in that location.

All traffic signals will, in the future, be controlled by Siemens TACTICS as a central traffic management system. The TMS is to interface to the Siemens TACTICS software to allow for pre-emptive triggers based on certain scenarios. Such triggers may be based on an evacuation scenario where extended green indications may be necessary, or other requested change in traffic signal timings. These are to be specifically determined by the facility when working to develop the scenario/response plans.



2/8/16

INVENTORY FOR LGA

Dynamic Message Signs (DMS)

Manufacturer	Sign Model / Matrix	Qty	Controller Model	Vintage	Protocol	Interface
Daktronics	-	20	VFC-3000	Future	NTCIP	IP

Vehicle Detection System (VDS)

Manufacturer	Model Description	Qty	Controller Model	Vintage	Protocol	Interface
Sensys Networks	In-pavement Wireless Detection Sensors	16	AP240-E	New	NTCIP	IP

Closed Circuit TV System (CCTV)

Manufacturer	Model Description	Qty	Controller Model	Vintage	Protocol	Interface
Verint	Nextiva Video Management Server	1	Nextiva	Version 6	-	Verint SDK
American Dynamics	Analog Video Switch	1	-	Legacy	-	RS-232
TBD	Camera	22	-	Future	-	IP

Port Newark-Elizabeth Port Authority Marine Terminal (PN-EPAMT)



The PN-EPAMT is a major component of the Port of New York and New Jersey. It is located on the Newark Bay and serves as the principal container ship facility for goods entering and leaving the metropolitan region. Port Newark and Elizabeth Port Authority Marine Terminal are side-by-side facilities and are owned and managed by the Port Authority. The PN-EPAMT monitors seaside ships coming in and out of the ports using the Automated Identification System (AIS) and

tracks/logs the arrival and departures of ships. Presently, PN-EPAMT utilizes Portable Dynamic Message Signs to advise truck traffic arriving at and leaving the facility. All facility ITS assets listed below will be included under TMS operations.

PN-EPAMT has an average size OCC with three existing terminals as shown on the floor plan provided below. The TMS workstation would be located in the front row between the radar tracking workstation and the facility CCTV workstation. In addition to the proposed workstation in the OCC, access to the TMS should also be possible from the facility manager's office using the existing PC in that location. The OCC is staffed by at least one person, 24/7. Presently PN-EPAMT has 40 CCTV cameras. Existing CCTV are a combination of pan-tilt-zoom (PTZ) and fixed cameras. The existing system is on the Loronix platform in conjunction with an American Dynamics video switch, but this is expected to be converted over to the Nextiva enterprise system in the near future.

PN-EPAMT has 5 portable DMS which are used at the entry and exits to the facility, but mostly at the exits to direct trucks and other vehicles leaving the facility with respect to outside traffic conditions. This is the primary basis of their traffic management. There is no real purpose or need for incident detection. The portable DMS are controlled through cellular service using Raven modems. The portable DMS system is furnished through ASTI Systems and is by Precision Solar Controls. ASTI provides its own software control using its proprietary CHIPS software. PN-EPAMT does not change the DMS messages that frequently. On average they change messages once every 3 days. Some permanent DMS as well as Sensys Networks' in-pavement wireless detection are planned as part of the future construction projects scheduled for 2015-17 deployment. The TMS should control both legacy portable DMS and proposed new DMS for an integrated solution to traffic control in and out of the facility.

All traffic signals will, in the future, be operated by Siemens TACTICS as a central traffic management system. The TMS is to interface to the Siemens TACTICS software to allow for pre-emptive triggers based on certain scenarios. Such triggers may be based on an evacuation scenario where extended green signals may be necessary, or other requested change in traffic signal timings. These are to be specifically determined by the facility when working to develop the scenario/response plans. Iteris video detection is used for intersection control. The TMS is also to interface to the Iteris software to allow for video to be displayed on the video wall.

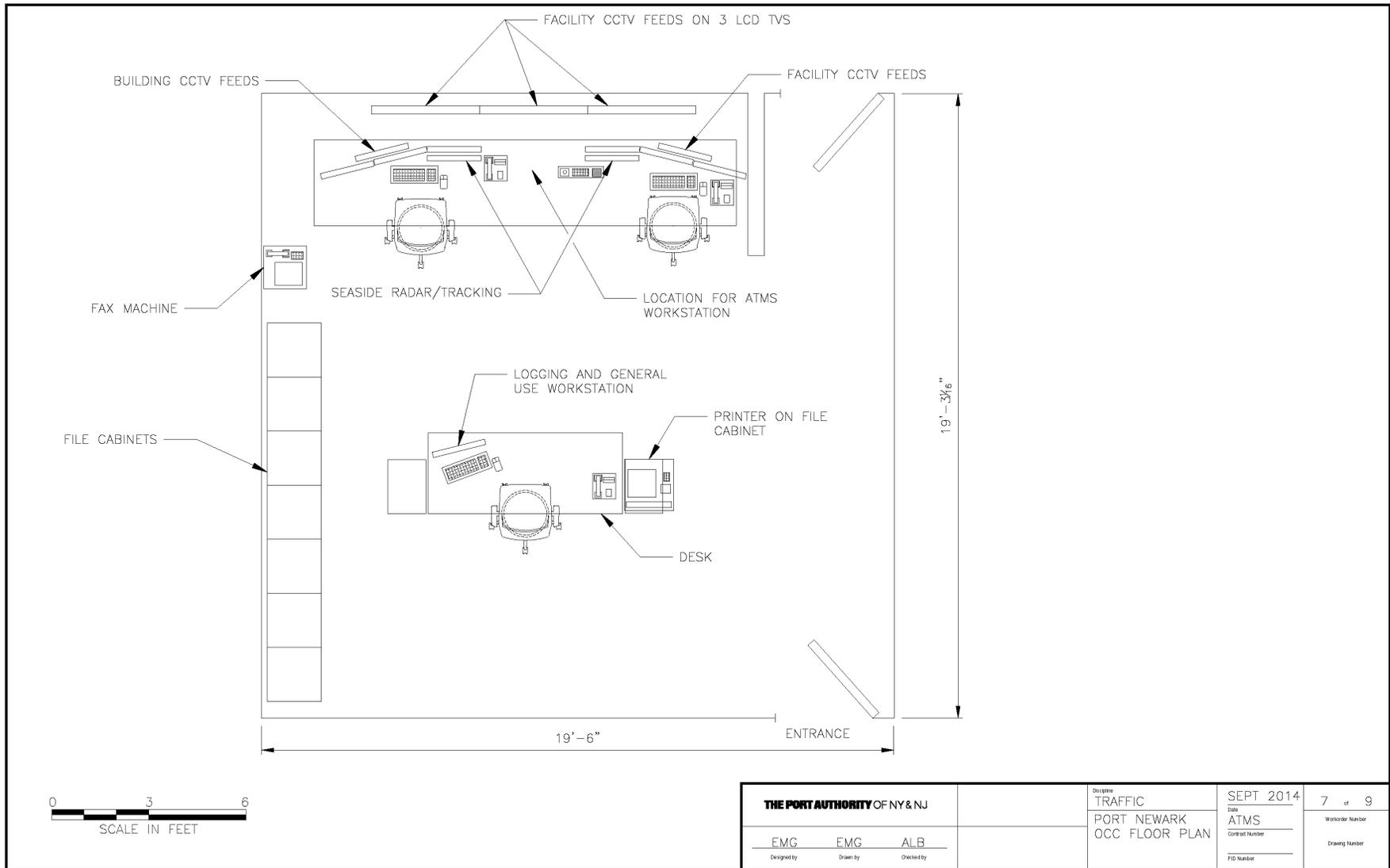
Most occurrences, traffic conditions and reports originate from Police calling in and reporting and motorists themselves. PN-EPAMT sometimes has a slowdown inbound to the facility but very rare that the PN-EPAMT will affect other roadways.

2/8/16

The facility does not use E-Log to log incidents and planned closures. However, it does make entries into E-Alerts. As with the other facilities, the TMS is to be the central point for logging entries into the system and have it populate OpenReach and E-Alerts.

PN-EPAMT Operations is divided among three (3) floors; Police on one floor, Operations on another floor, and maintenance on a third floor. For improved workflow and efficiency, it is best to provide real-time awareness among the three entities. In doing so, TMS access should be provided at existing workstations for Police, Maintenance, and the facility manager's office, which will be in addition to the proposed workstation in the OCC.

Most important to PN-EPAMT are evacuations, as was determined from a recent study conducted by the facility. The Contractor, in the development of scenarios and response plans for this facility, is to take this into account and include this important provision within the TMS.



INVENTORY FOR PN-EPAMTDynamic Message Signs (DMS)

Manufacturer	Sign Model / Matrix	Qty	Controller Model	Vintage	Protocol	Interface
Precision Solar Controls	SMC Model Series	5	-	Legacy	NTCIP	Cell Modem
Daktronics	-	6	-	Future	NTCIP	Cell Modem

Closed Circuit TV System (CCTV)

Manufacturer	Model Description	Qty	Controller Model	Vintage	Protocol	Interface
Verint	Nextiva Video Management Server	2	Nextiva	Version 6	-	Verint SDK
American Dynamics	Analog Video Switch	1	-	Legacy	-	RS-232
Camera	American Dynamics Speed Dome VIII (ADSDU8E35)	42	-	Legacy	-	-
Camera	SONY SSC-E-473	2	-	Legacy	-	-
Camera (Port Jersey)	American Dynamics Speed Dome VIII (ADSDU8E35)	6	-	Legacy	-	-

TRANSMIT (Travel Time System)

TRANSMIT is a TRANSCOM system that utilizes Kapsch Janus Multi-protocol readers. The TMS is to communicate with TRANSMIT through the use of TRANSCOM's Bridge API, which can be obtained at no cost from TRANSCOM. All TRANSMIT Servers are Windows based and located at the GWB Administration Building.

ID	Site	# of Reader Cabinets	# of Antennas	XMIT Server	Interface
PA60	Corbin St south of Marsh St	1	3	GWB	Cell Modem
PA61	Entrance to Port Elizabeth at North Avenue	1	4	GWB	Cell Modem
PA62	Mclester St bet. Polaris and APM Driveway	1	3	GWB	Cell Modem
PA63	Port Street west of Corbin Street ramp	1	3	GWB	Cell Modem
PA64	Port Street east of Corbin Street ramp	1	2	GWB	Cell Modem

Port Authority Trans-Hudson (PATH)



PATH is a rapid transit railroad that serves Newark, Harrison, Hoboken and Jersey City in northern New Jersey and Manhattan in New York City. PATH operates 24 hours a day and is 13.8 miles long, not including any route overlap. PATH runs underneath the Hudson River and uses only tunnels in Manhattan, Hoboken, and downtown Jersey City.

PATH is unlike the bridges or tunnel facilities in that the focus is on rail operations and not roadway operations. As such, there are less ITS assets and features such as incident detection for obvious reasons. The most critical aspect of train operations are arrival, departure times and delays. This is the information that needs to be exchanged with other facilities and/or conveyed to the public for optimal multimodal integration and awareness.

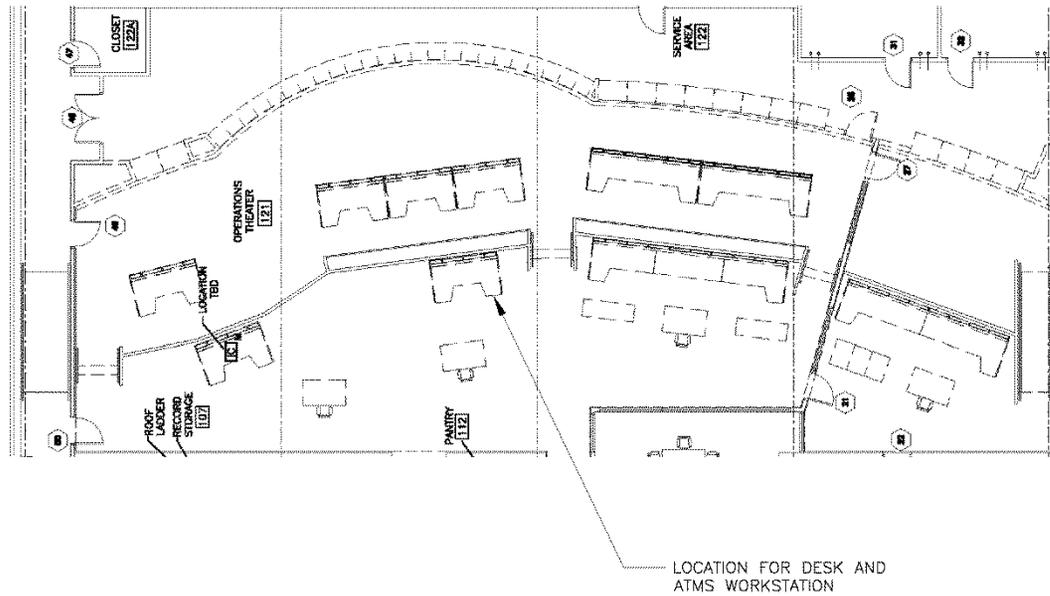
PATH employs PATHVision, a web-based application that provide train arrival departure information. PATH has used this system for nearly 20 years now and is pleased with its operation and purpose. PATHVision will not be integrated with the TMS; however, critical alerts such as delays, closures, etc are to be communicated with the TMS through XML or other industry-standard system interface.

PATH has a new state-of-the-art OCC. With this new facility an enterprise solution for CCTV using Nextiva has been implemented. The TMS is not to integrate to the CCTV security system. However, some cameras related to general surveillance will be on the Nextiva enterprise system, which the TMS is to integrate with. Partial floor plan for the new OCC is shown below with the TMS workstation location identified. The video wall is significant in size and is driven by Activu Corporation data collaboration software.

A software instance is to be installed at the OCC for intercommunications with other PA facilities. Presently, PATH indicated that it relies on TRANSCOM for intercommunications with other facilities and other transit agencies, particularly NYC Transit and NJ Transit. The implementation of the TMS alongside OpenReach is to improve on the real-time awareness and consistency of distributed information with TRANSCOM and other PA facilities.

PATH makes its entries into a master log called IRS (by TRA Associates). They do not use the E-Log (Web-EOC) system that TB&T uses. PATH does use a broadcast alert system called "PATH Alerts" as well as Twitter and Text Messages to patrons that sign up. See discussion on Additional Interfaces below.

Since PATH is a transit operation, there was a discussion with the facility as to how an ATMS software would benefit or integrate with PATH operations. One suggestion would be to provide kiosks at the airports. If PATH, NYC Transit and NJ Transit schedule and on-time/delay information can be provided to travelers in advance in addition to roadway travel times, this could be advantageous. The TMS would serve as a data warehouse of information for complete regional awareness, software decision making, and dissemination of information through various means including kiosks, E-alerts, PATH-alerts, Twitter, 511, OpenReach, website and text messages. While the implementation of kiosks is not a requirement of this project, the TMS should be configured in anticipation of this feature in the future should the PA decide to enhance its system.



THE PORT AUTHORITY OF NY & NJ			Discipline: TRAFFIC	Date: SEPT 2014	Sheet Number: 8 of 9
			Project: PTCC OCC FLOOR PLAN	Contract Number: ATMS	Drawing Number:
Designed by: EMG	Drawn by: EMG	Checked by: ALB			
			PG Number:		

ATTACHMENT F - COST PROPOSAL

ENTRY of PRICES:

- 1 The prices quoted shall be written in figures and in writing, in ink, preferably black ink where required in the spaces provided on the Pricing Sheet(s) attached hereto and made a part hereof.

- 2 Prices must be submitted for each item required on the Pricing Sheet(s). The Items on the Pricing Sheet(s) correspond to required services set forth in Attachment E – “Scope of Work.”

- 3 Proposers must insert all figures as required and verify all computations for accuracy. The percentage provided corresponding to each implementation milestone and associated deliverables is based on percentages allocated by the Authority and represent percentage breakdown adding up to 100% of the Price for Implementation.

- 4 The Authority in its sole judgment reserves the right to (1) reject Bids without checking them for mathematical errors or omissions, (2) reject Bids that contain or appear to contain errors or omissions, and (3) supply corrections to Bids that contain or appear to contain mathematical errors and omissions, and in this case the Authority reserves the right to recompute the Total Price (which amount shall govern in all cases) based upon the milestone prices inserted by the Proposer.

- 5 Compensation shall be in accordance with the Section of this Contract entitled “Payments.”

- 6 The Total Price shall be obtained by adding the Price for Implementation to the Price for Maintenance.

- 7 In case of discrepancy between the prices quoted in writing and those quoted in figures, the writing shall control.

PRICING SHEET - SUMMARY (1 of 9)

I. Implementation Phase (Years 1 - 2)				
Milestone	% of Total	Lump Sum Amount		
		Figures	Writing	
1 Project Start-Up	5			Dollars Cents
2 NOCs, Primary/Backup PA-AOC, DR Site, and TEC Implementation	15			Dollars Cents
3 TB&T Implementation (GWB, LT, HT)	18			Dollars Cents
4 TB&T Implementation (BB, GB, OBX)	12			Dollars Cents
5 Aviation Implementation (JFK, LGA, EWR)	12			Dollars Cents
6 Port Commerce Implementation (PN-EPAMT)	12			Dollars Cents
7 GWBBS, PABT, PATH, Ferry Transportation, TEB, SWR, and Public Affairs Implementation	12			Dollars Cents
8 Final Acceptance	14			Dollars Cents
Price for Implementation	100			Dollars Cents

PRICING SHEET - SUMMARY (1 of 9) (continued)

Application Maintenance and Support			
II. Maintenance Phase (Years 3 and 4)			
Year 3			Dollars Cents
Year 4			Dollars Cents
Total			Dollars Cents
III. Option Periods (Years 5 and 6)			
Option Period #1 (Year 5)			
Year 5			Dollars Cents
Option Period #2 (Year 6)			
Year 6			Dollars Cents
Total			
Price for Maintenance			Dollars Cents
IV. Recapitulation			
Price for Implementation			Dollars Cents
Price for Maintenance			Dollars Cents
Total Price			Dollars Cents

PRICING SHEET (2 of 9)

Milestone 1: Project Start-Up - Implementation Phase (Years 1 - 2)				
Task	% of Total	Lump Sum Amount		
		Figures	Writing	
1 System Documentation & Project Management Plan	2%			Dollars Cents
2 Mobilization and Project Management	3%			Dollars Cents
Total	5%			Dollars Cents

PRICING SHEET (3 of 9)

Milestone 2: NOCs, Primary PA-AOC, Backup PA-AOC and DR Site, and TEC Implementation Implementation Phase (Years 1 - 2)				
Task	% of Total	Lump Sum Amount		
		Figures	Writing	
NOCs and PA-AOC Implementation				
1 System Interface Development	2.00%			Dollars Cents
2 Software Configuration	2.00%			Dollars Cents
3 Field Acceptance Testing	0.75%			Dollars Cents
4 30-day Operational Testing	0.75%			Dollars Cents
5 Training	0.50%			Dollars Cents
Subtotal	6%			Dollars Cents
Backup PA-AOC and DR Site Implementation				
1 System Interface Development	2.00%			Dollars Cents
2 Software Configuration	1.00%			Dollars Cents
3 Field Acceptance Testing	0.75%			Dollars Cents
4 30-day Operational Testing	0.75%			Dollars Cents
5 Training	0.50%			Dollars Cents
Subtotal	5%			Dollars Cents

PRICING SHEET (3 of 9) (continued)

Milestone 2: NOCs, Primary PA-AOC, Backup PA-AOC and DR Site, and TEC Implementation Implementation Phase (Years 1 - 2)				
Task	% of Total	Lump Sum Amount		
		Figures	Writing	
TEC Implementation				
1 System Interface Development	1.00%			Dollars Cents
2 Software Configuration	1.00%			Dollars Cents
3 Field Acceptance Testing	0.75%			Dollars Cents
4 30-day Operational Testing	0.75%			Dollars Cents
5 Training	0.50%			Dollars Cents
Subtotal	4%			Dollars Cents
Total	15%			Dollars Cents

PRICING SHEET (4 of 9)

Milestone 3: TB&T Implementation (GWB, LT, HT) - Implementation Phase (Years 1 - 2)				
Task	% of Total	Lump Sum Amount		
		Figures	Writing	
GWB Implementation				
1 System Interface Development	2.00%			Dollars Cents
2 Software Configuration	1.00%			Dollars Cents
3 Field Acceptance Testing	1.00%			Dollars Cents
4 30-day Operational Testing	1.00%			Dollars Cents
5 Training	1.00%			Dollars Cents
Subtotal	6%			Dollars Cents
LT Implementation				
1 System Interface Development	2.00%			Dollars Cents
2 Software Configuration	1.00%			Dollars Cents
3 Field Acceptance Testing	1.00%			Dollars Cents
4 30-day Operational Testing	1.00%			Dollars Cents
5 Training	1.00%			Dollars Cents
Subtotal	6%			Dollars Cents

PRICING SHEET (4 of 9) (continued)

Milestone 3: TB&T Implementation (GWB, LT, HT) - Implementation Phase (Years 1 - 2)				
Task	% of Total	Lump Sum Amount		
		Figures	Writing	
HT Implementation				
1 System Interface Development	2.00%			Dollars Cents
2 Software Configuration	1.00%			Dollars Cents
3 Field Acceptance Testing	1.00%			Dollars Cents
4 30-day Operational Testing	1.00%			Dollars Cents
5 Training	1.00%			Dollars Cents
Subtotal	6%			Dollars Cents
Total	18%			Dollars Cents

PRICING SHEET (5 of 9)

Milestone 4: TB&T Implementation (BB, GB, and OBX) - Implementation Phase (Years 1 - 2)				
Task	% of Total	Lump Sum Amount		
		Figures	Writing	
BB Implementation				
1 System Interface Development	1.00%			Dollars Cents
2 Software Configuration	1.00%			Dollars Cents
3 Field Acceptance Testing	0.75%			Dollars Cents
4 30-day Operational Testing	0.75%			Dollars Cents
5 Training	0.50%			Dollars Cents
Subtotal	4%			Dollars Cents
GB Implementation				
1 System Interface Development	1.00%			Dollars Cents
2 Software Configuration	1.00%			Dollars Cents
3 Field Acceptance Testing	0.75%			Dollars Cents
4 30-day Operational Testing	0.75%			Dollars Cents
5 Training	0.50%			Dollars Cents
Subtotal	4%			Dollars Cents

PRICING SHEET (5 of 9) (continued)

Milestone 4: TB&T Implementation (BB, GB, and OBX) - Implementation Phase (Years 1 - 2)				
Task	% of Total	Lump Sum Amount		
		Figures	Writing	
OBX Implementation				
1 System Interface Development	1.00%			Dollars Cents
2 Software Configuration	1.00%			Dollars Cents
3 Field Acceptance Testing	0.75%			Dollars Cents
4 30-day Operational Testing	0.75%			Dollars Cents
5 Training	0.50%			Dollars Cents
Subtotal	4%			Dollars Cents
Total	12%			Dollars Cents

PRICING SHEET (6 of 9)

Milestone 5: Aviation Implementation (JFK, LGA, EWR) - Implementation Phase (Years 1 - 2)				
Task	% of Total	Lump Sum Amount		
		Figures	Writing	
JFK Implementation				
1 System Interface Development	1.00%			Dollars Cents
2 Software Configuration	1.00%			Dollars Cents
3 Field Acceptance Testing	0.75%			Dollars Cents
4 30-day Operational Testing (including PA-AOC Integration)	0.75%			Dollars Cents
5 Training	0.50%			Dollars Cents
Subtotal	4%			Dollars Cents
LGA Implementation				
1 System Interface Development	1.00%			Dollars Cents
2 Software Configuration	1.00%			Dollars Cents
3 Field Acceptance Testing	0.75%			Dollars Cents
4 30-day Operational Testing (including PA-AOC Integration)	0.75%			Dollars Cents
5 Training	0.50%			Dollars Cents
Subtotal	4%			Dollars Cents

PRICING SHEET (6 of 9) (continued)

Milestone 5: Aviation Implementation (JFK, LGA, EWR) - Implementation Phase (Years 1 - 2)				
Task	% of Total	Lump Sum Amount		
		Figures	Writing	
EWR Implementation				
1 System Interface Development	1.00%			Dollars Cents
2 Software Configuration	1.00%			Dollars Cents
3 Field Acceptance Testing	0.75%			Dollars Cents
4 30-day Operational Testing (including PA-AOC Integration)	0.75%			Dollars Cents
5 Training	0.50%			Dollars Cents
Subtotal	4%			Dollars Cents
Total	12%			Dollars Cents

PRICING SHEET (7 of 9)

Milestone 6: Port Commerce Implementation (PN-EPAMT) - Implementation Phase (Years 1 - 2)				
Task	% of Total	Lump Sum Amount		
		Figures	Writing	
1 System Interface Development	4.00%			Dollars Cents
2 Software Configuration	3.00%			Dollars Cents
3 Field Acceptance Testing	2.00%			Dollars Cents
4 30-day Operational Testing (including PA-AOC Integration)	2.00%			Dollars Cents
5 Training	1.00%			Dollars Cents
Total	12%			Dollars Cents

PRICING SHEET (8 of 9)

Milestone 7: GWBBS, PABT, PATH, Ferry Transportation, TEB, SWR, and Public Affairs (Lightweight) Implementation - Implementation Phase (Years 1 - 2)				
Task	% of Total	Lump Sum Amount		
		Figures	Writing	
1 System Interface Development	2.00%			Dollars Cents
2 Software Configuration	2.00%			Dollars Cents
3 GWBBS 30-day Operational Testing	1.00%			Dollars Cents
4 PABT 30-day Operational Testing	1.00%			Dollars Cents
5 PATH 30-day Operational Testing	1.00%			Dollars Cents
6 Ferry Transportation 30-day Operational Testing	1.00%			Dollars Cents
7 TEB 30-day Operational Testing	1.00%			Dollars Cents
8 SWR 30-day Operational Testing	1.00%			Dollars Cents
9 Public Affairs 30-day Operational Testing	1.00%			Dollars Cents
10 Training	1.00%			Dollars Cents
Total	12%			Dollars Cents

PRICING SHEET (9 of 9)

Milestone 8: Final Acceptance -Implementation Phase (Years 1 - 2)			
Task	% of Total	Lump Sum Amount	
		Figures	Writing
1 Final Acceptance of Fully Integrated and Functioning System	14%		Dollars Cents
Total	14%		Dollars Cents

In determining the rates to be paid to the Contractor for the performance of Extra Work and subject to the applicable adjustment clauses as described elsewhere herein, the Contractor will be compensated as follows:

Contractor Hourly Rates (Contractor to insert any other relevant Titles and all hourly rates):

<u>Title</u>	<u>Hourly Rate</u>
Field Technician/Engineer	_____
Programmer	_____
Database Administrator	_____
Business Analyst	_____
Office Engineer	_____
System Administrator	_____

2/8/16

ATTACHMENT G - CERTIFICATE OF NO CHANGE

**THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY
REQUEST FOR PRE-QUALIFICATIONS FOR RFPQ# 37893 FOR ADVANCED
TRANSPORTATION MANAGEMENT SYSTEM (ATMS) SOFTWARE PACKAGE – STAGE I**

Instructions: Please have a principal of the firm complete and execute one original. Forward directly to:

Jeanette Anderson, C.P.P.B
Procurement Contracts Manager
4 World Trade Center
150 Greenwich Street, 21st Floor
New York, New York 10007

Name of Firm:

Address:

I, _____, state, that to the best of my
(Title and Name of Firm)

knowledge, there has been no change in status with respect to the information and representations in my firm's June 2014 submission in response to the RFPQ #37893 for **ADVANCED TRANSPORTATION MANAGEMENT SYSTEM (ATMS) SOFTWARE PACKAGE – STAGE I**. I understand that the Port Authority will utilize said submission and rely upon its accuracy as of this date in order to make a determination as to whether my firm has met the requirements set forth therein.

If there have been any changes, they are as follows (attach additional sheets if necessary):

A materially false statement willfully or fraudulently made in connection with this certification, and/or failure to conduct appropriate due diligence in verifying the information that is the subject matter of this certification may prevent the Company and/or the undersigned from being found to be responsible bidders/proposers in connection with future agreements.

(Print Name)

Date: _____

(Signature)

ATTACHMENT H - PROPOSER REFERENCE FORM

Name of Proposer:

Please provide a list of references on the firm's performance of similar work within the last five years, including all current contracts. Use additional sheets as necessary.

Include the following information for each reference:

Customer Name:

Address:

Contact Name and Title:

Phone and Fax Numbers of Contact:

Contract date(s):

Contract cost:

Description of work:

.....

.....

Customer Name:

Address:

Contact Name and Title:

Phone and Fax Numbers of Contact:

Contract date(s):

Contract cost:

Description of Work:

Customer Name:

Address:

Contact Name and Title:

Phone and Fax Numbers of Contact:

Contract date (s):

Contract cost:

Description of work:

.....

.....

2/8/16

ATTACHMENT I - MBE/WBE PARTICIPATION PLAN

THE PORT AUTHORITY OF NY & NJ

OFFICE OF BUSINESS DIVERSITY AND CIVIL RIGHTS

MBE/WBE PARTICIPATION PLAN AND AFFIRMATION STATEMENT

PA 3760C/ 1-16

Instructions: Submit one MBE/WBE PARTICIPATION PLAN AND AFFIRMATION STATEMENT form for each MBE/WBE firm used on this Contract. To avoid undue repetition, the following terms, as used in this Agreement, shall be construed as follows: Bidder/Proposer/Respondent - can used interchangeably and mean any Contractor, Consultant, Supplier, or Vendor who submits a response to this solicitation.

RFP NUMBER AND TITLE: _____

PROPOSER:

Name of Firm: _____

Address: _____ Telephone: _____

Email Address: _____

MBE/WBE:

Name of Firm: _____

Address: _____ Telephone: _____

Description of work to be performed by MBE/WBE: _____

Calculation (supply only): _____

The Proposer is committed to utilizing the above-named MBE/WBE for the work described above. The estimated dollar value of this work is \$ _____ or _____ % of the total contract amount of \$ _____. The anticipated start date is _____ and the anticipated completion date is _____

AFFIRMATION of MBE/WBE

The above-named MBE/WBE affirms that it will perform the portion of the Contract for the estimated dollar value as stated above.

By: _____ Date: _____
Signature of Principal or Officer of MBE/WBE – Print Name and Title

I _____ (print name), an officer of _____ (company name), certify that I have read the PA 3760C MBE/WBE Participation Plan and Affirmation Statement and the information contained in it is true. I fully understand that any false statement within this submittal may prevent the company and/or the undersigned from being found to be responsible Bidders/Proposers in connection with future agreements. In addition, any false statement within this submittal may subject the company and/or the undersigned to criminal charges in the state and federal courts of New York and New Jersey.

Signature of Proposer _____ Title _____ Date _____

Please Note: Only 60% of the expenditure to a MBE/WBE material supplier will be counted toward the MBE/WBE goal. Please show calculation above. Example: \$100,000 x 60% = \$60,000 estimated MBE/WBE dollar value of work. Plan cannot be accepted without calculation.

Officer of Proposer must have ACKNOWLEDGEMENT BY NOTARY PUBLIC completed on the reverse side.

2/8/16

ACKNOWLEDGEMENT BY NOTARY PUBLIC

**PA 3760C
MBE/WBE PARTICIPATION PLAN AND AFFIRMATION STATEMENT (reverse)**

ACKNOWLEDGEMENT
of

STATE OF _____)

S.S.:

COUNTY OF _____)

On this _____ day of _____, before me personally came and appeared _____ to be known, who being by me duly sworn, did depose and say that he/she resides at _____, that he/she is the _____ of _____ company, that the seal affixed to said Certification is such corporate seal, that it was so affixed by order of the directors of said corporation, and that he/she signed his/her name thereto by like order.

(Notary's Seal or Stamp)

Notary Public
My commission expires:

MODIFIED MBE/WBE PARTICIPATION PLAN AND AFFIRMATION STATEMENT

PA 3760D / 01-16

Instructions: Submit one Modified MBE/WBE PARTICIPATION PLAN AND AFFIRMATION STATEMENT form for each MBE/WBE firm used on this Contract. To avoid undue repetition, the following terms, as used in this Agreement, shall be construed as follows: Bidder/Proposer/Respondent - can used interchangeably and mean any Contractor, Consultant, Supplier, or Vendor who submits a response to this solicitation.

RFP NUMBER AND TITLE: _____

PROPOSER:

Name of Firm: _____

Address: _____ Telephone: _____

Email Address: _____

MBE/WBE:

Name of Firm: _____

Address: _____ Telephone: _____

Description of work to be performed by MBE/WBE: _____

Calculation (supply only): _____

Proposer is committed to utilizing the above-named MBE/WBE for the work described above. The estimated dollar value of this work is \$ _____

or _____% of the total contract amount of \$ _____. The anticipated start date is _____ and the anticipated completion date is _____

AFFIRMATION of MBE/WBE

The above-named MBE/WBE affirms that it will perform the portion of the Contract for the estimated dollar value as stated above.

By: _____ Date: _____

Signature of Principal or Officer of MBE/WBE - Print Name and Title

If the Proposer does not receive award of the Contract, any and all representations in this Modified MBE/WBE Participation Plan and Affirmation Statement shall be null and void. I _____ (print name), an officer of _____ (company name), certify that I have read the PA 3760D Modified MBE/WBE Participation Plan and Affirmation Statement and the information contained in it is true. I fully understand that any false statement within this submittal may prevent the company and/or the undersigned from being found to be responsible Bidders/Proposers in connection with future agreements. In addition, any false statement within this submittal may subject the company and/or the undersigned to criminal charges in the state and federal courts of New York and New Jersey.

Signature of Proposer _____ Title _____ Date _____

Please Note: Only 60% of the expenditure to a MBE/WBE material supplier will be counted toward the MBE/WBE goal. Please show calculation above. Example: \$100,000 x 60% = \$60,000 estimated MBE/WBE dollar value of work. Plan cannot be accepted without calculation.

Officer of Proposer must have ACKNOWLEDGEMENT BY NOTARY PUBLIC completed on the reverse side.

ACKNOWLEDGEMENT BY NOTARY PUBLIC

PA 3760D

MODIFIED MBE/WBE PARTICIPATION PLAN AND AFFIRMATION STATEMENT (reverse)

ACKNOWLEDGEMENT

of

STATE OF _____)

S.S.:

COUNTY OF _____)

On this _____ day of _____, before me personally came and appeared _____ to be known, who being by me duly sworn, did depose and say that he/she resides at _____, that he/she is the _____ of _____ company, that the seal affixed to said Certification is such corporate seal, that it was so affixed by order of the directors of said corporation, and that he/she signed his/her name thereto by like order.

(Notary's Seal or Stamp)

Notary Public
My commission expires:

2/8/16



ATTACHMENT J- STATEMENT OF SUBCONTRACTOR PAYMENTS

INSTRUCTIONS FOR STATEMENT OF SUBCONTRACTOR PAYMENT

Attached is the Statement of Statement of Payments to MBE/WBE/DBE Subconsultants/Lessors/Suppliers form, which shall be submitted with every invoice to be used in conjunction with the MBE/WBE Participation Plan

STATEMENT OF PAYMENTS TO MBE/WBE/DBE SUBCONSULTANTS / LESSORS / SUPPLIERS Ver. 11-18-15

Agreement No _____	Award Date _____	Agreement Amount _____ (C)	Reporting Period To _____	Payment No. _____	The Port Authority of NY & NJ - For Office Use Only
Agreement Title _____			From _____	Total Paid to Date _____	Date Received: _____
Contractor _____	% Complete _____				Reviewed By: _____
					Title: _____

<p>MBE/ WBE Participation</p> <p>Number of MBE/WBE Sub/Suppliers _____ MBE/WBE Invoices to Date _____</p> <p>Total Value of MBE/WBE Subcontracts \$ _____ MBE/WBE Paid to Date _____ (A)</p> <p>Total Value of MBE/WBE Suppliers \$ _____ MBE/WBE Suppliers Paid to Date _____ (B)</p> <p>MBE/WBE % Agreement Amount to Date _____ = ((A) + ((B) x .8)) / (C)</p>	<p>DBE Participation:</p> <p>Number of DBE Sub/Suppliers _____ DBE Invoices to Date _____</p> <p>Total Value of DBE Subcontracts _____ DBE Paid to Date _____ (D)</p> <p>Total Value of DBE Suppliers _____ DBE Suppliers Paid to Date _____ (E)</p> <p>DBE % Agreement Amount to Date _____ = ((D) + ((E) x .8)) / (C)</p> <p style="text-align: center;">Column A + Column B + Column C</p>
--	--

Subconsultant's / SUPPLIER NAME	S = SUB P = SUPPLIER	DESCRIPTION OF WORK / MATERIAL SUPPLIED	MINORITY STATUS M / W / DBE	STATUS THIS PERIOD ACTIVE - (A) INACTIVE - (I) COMPLETE - (C)	SAR AMOUNT	START DATE	SUB % COMPLETE	PROJECTED COMPLETION DATE	Work Order No.	AMOUNTS PAID		
										Total of All Prior Statements	Paid This Statement	Cumulative To Date

- IF NECESSARY, USE A SEPARATE SHEET**
1. Did any of the MBE/WBE/DBE Subconsultants rent/lease equipment from the prime contractor or an affiliate company during the report period? If yes, explain the arrangement, including a description of the equipment and the cost. Y / N

 2. Did any of the MBE/WBE/DBE Subconsultants utilize employees or former employees of the prime contractor or an affiliate company during the report period? Y / N

 3. Did any of the MBE/WBE/DBE Subconsultants subcontract any portion of its work to a non-MBE/WBE/DBE during the report period? If yes, explain fully. Y / N

 4. Has the scope of work or the subcontract amount for any of the MBE/WBE/DBE Subconsultants changed since the last report? If yes, explain fully. Y / N

 5. Has the MBE/WBE/DBE Subconsultant(s) listed performed a commercially useful function consistent with their trade or business? If No, fully explain. Y / N

Date Prepared: _____ Phone: _____

Prepared by: _____

Title: _____

An Officer of the Prime Contractor must complete the Certification on The Reverse Side

ATTACHMENT K - CERTIFIED ENVIRONMENTALLY PREFERABLE PRODUCTS/PRACTICES

Proposer Name: _____ Date: _____

In line with the Port Authority’s efforts to promote products and practices which reduce our impact on the environment and human health, Proposers are encouraged to provide information regarding their environmentally preferable/sustainable business practices as they relate to this contract wherever possible. Proposers **must** complete this form and submit it with their response, if appropriate. Proposers **must** submit appropriate documentation to support the items for which the Proposer indicates a “Yes” and present this documentation in the proper sequence of this Attachment.

1. Packaging

Has the Proposer implemented any of the following environmental initiatives? **(A checkmark indicates “Yes”)**

- ___ Use of corrugated materials that exceed the EPA recommended post-consumer recycled content
- ___ Use of other packaging materials that contain recycled content and are recyclable in most local programs
- ___ Promotes waste prevention and source reduction by reducing the extent of the packaging and/or offering packaging take-back services, or shipping carton return
- ___ Reduces or eliminates materials which have been bleached with chlorine or chlorine derivatives
- ___ Eliminates any packaging that may contain polyvinyl chloride (PVC), or polystyrene or heavy metals

If yes, a description of the practices being followed must be included with the submission.

2. Business Practices / Operations / Manufacturing

Does the Proposer engage in practices that serve to reduce or minimize an impact to the environment, including, but not necessarily limited to, the following items? **(A checkmark indicates “Yes”)**

- ___ Recycles materials in the warehouse or other operations
- ___ Use of alternative fuel vehicles or vehicles equipped with diesel emission control devices for delivery or transportation purposes
- ___ Use of energy efficient office equipment or signage or the incorporation of green building design elements
- ___ Use of recycled paper (that meets federal specifications) in their marketing and/or resource materials
- ___ Other sustainable initiative

If yes, a description of the practices being followed must be included with the submission.

2/8/16

3. Training and Education

Does the Proposer conduct/offer a program to train or inform customers and employees of the environmental benefits of the products to be offered under this contract, and/or does the Proposer conduct environmental training of its own staff?

Yes No If yes, Proposer must attach a description of the training offered and the specific criteria targeted by the training.

4. Certifications

Has the Proposer or any of its manufacturers and/or subcontractors obtained any of the following product / industry certifications? **(A checkmark indicates “Yes”)**

____ ISO 14000 or adopted some other equivalent environmental management system

____ Other industry environmental standards (where applicable), such as the CERES principles, LEED Certification, C2C Protocol, Responsible Care Codes of Practice or other similar standards

____ Third Party product certifications such as Green Seal, Scientific Certification Systems, Smartwood, etc.

If yes, Proposers must attach copies of the certificates obtained.

5. Other Environmental Criteria

Proposers are encouraged to respond to criteria specifically indicated in this RFP as “Management Approach” (and attach the appropriate documentation) to receive consideration in the evaluation.

I hereby certify, under penalty of the law that the above statements are true and correct.

_____ Signature

_____ Date

ATTACHMENT L - PORT AUTHORITY FACILITIES

Aviation Facilities

LaGuardia Airport, Flushing, NY 11371
John F. Kennedy International Airport, Jamaica, NY 11430
AirTrain JFK, Jamaica, NY 11430
Newark Liberty International Airport, Newark, NJ 07114
AirTrain Newark, Newark, NJ 07114
Teterboro Airport, Teterboro, NJ 07608
Stewart International Airport, Newburgh, NY 12553
Atlantic City International Airport, Egg Harbor Township, NJ 08234

Tunnels, Bridges and Terminals Facilities

Holland Tunnel, Jersey City, NJ 07310
Lincoln Tunnel, Weehawken, NJ 07087
George Washington Bridge, Fort Lee, NJ 07024
George Washington Bridge Bus Station, Fort Lee, NJ 07024
George Washington Bridge Toll House, Fort Lee, NJ 07024
George Washington Bridge Palisade Station, Fort Lee, NJ 07024
Bayonne Bridge, Staten Island, NY 10302
Goethals Bridge, Staten Island, NY 10303
Outerbridge Crossing, Staten Island, NY 10309
Port Authority Midtown Bus Terminal, New York, NY 10018

Port Authority Trans-Hudson (PATH) Corporation Facilities

PATH Rapid Transit System Call Stations, Jersey City, NJ 07306
Journal Square Transportation Center, Jersey City, NJ 07306
Harrison Car Maintenance Facility, Harrison, NJ 07029
Consolidated Shops, Jersey City, NJ 07302
Waldo Shops, Jersey City, NJ 07302

Port Commerce Facilities

Port Newark, Newark, NJ 07114
Elizabeth Marine Terminal, Elizabeth, NJ 07201
Brooklyn/Red Hook Container Terminal, Brooklyn, NY 11201
Howland Hook Marine Terminal, Staten Island, NY 10303
274 Kellogg Street, Newark, NJ 07114
255 Kellogg Street, Newark, NJ 07114
Bayonne Cruise Terminal, Bayonne, NJ

Regional Development Facilities

Bathgate Industrial Park, Bronx, NY 10457
Teleport, Staten Island, NY 10311
5 Marine View Plaza, Hoboken, NJ 07030

2/8/16

Other Facilities

- 225 Park Avenue South, New York, NY 10003
- 233 Park Avenue South, New York, NY 10003
- 115 Broadway, New York, NY 10006
- 4WTC 150 Greenwich Street, New York, NY 10007
- 2 Montgomery Street, Jersey City, NJ 07302
- Gateway Center, Newark, NJ 07102
- Port Authority Technical Center, Jersey City, NJ 07310
- 22 Cortland Street, New York, NY
- 116 Nassau Street, New York, NY
- 1160 McLester Street, Newark, NJ
- 1170 McLester Street, Newark, NJ
- Sealink/TWIC Facility, Elizabeth, NJ
- 100 Washington Street, New York, NY

ATTACHMENT M - AUDIT SECURITY CHECKLISTS

Audit Department

Controls Requirement Contract Checklist

General

- Documented procedures, flowcharts and process maps for the application.
- Conduct regular audits, vulnerability testing, and security scanners.
- SSAE 16 SOC 2 Type II (previously known as SAS 70 Level 2)
- Federal Risk and Authorization Management Program (FedRAMP) Certification
- ISO27001 Certification
- Criminal Justice Information Services security policies and procedures (CJIS) compliant for law enforcement information and systems.
- Background check should be performed on all personnel.

System/Security Administration

- Administrative personnel should receive training.
- Administrative staff should receive general security awareness training before access is provided. All security training must be reinforced at least every three years and must be tracked as per the PA Information Security Handbook.
- System and security administration procedures should be documented and distributed.
- Administrator(s) roles and responsibilities should be documented.
- Developers and/or programmers should not have access to the production server.
- Operating system administrators should not have access to the production database and application.

Hardening of operating system/database that supports the application:

- Disable and/or remove unnecessary ports/services.
- Remove all manufacturer samples from the production system. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.
- Default, public, and guest accounts should be secured/locked/removed.
- Change all default passwords; delete all default content and login scripts.
- Limit administrative and user account privilege and access.
- Document system accounts like administrator, root, oracle, and sys.
- Document user/group access rights
 - Users/groups should be setup with least access required to perform job responsibilities.
- Implement access control at the database level (i.e., user roles and permissions, passwords, secure links)
- Use secure encrypted remote access methods.

- If the application is a web application, log (and monitor) web traffic and trend the activity looking for abnormal activity.
- Ensure that appropriate security and vulnerability assessment tools are running.
- At login, last user login should not display.
- Inventory listing of hardware and software should be current and maintained.

License Management

- Ensure that application licensing requirements are documented, reviewed and maintained.
- Application licenses should be current/valid and individuals/groups with application access should have completed the necessary access request forms and adhere to licensing requirements.

Logical Access Controls

- All users are required to read the Agency Policy Computing Resource Administrative Instruction (AI 15-4.03) and sign an acknowledgement of the Agency IT Acceptable Use Code of Conduct policy prior to account activation.
- Procedures to grant/modify/delete access should be documented.
 - Access request forms for adding/modifying/deleting users should be used.
 - Account expiration for contractors and consultants.
 - Accounts adequately identify the user – no generic accounts
- Ensure that security administrator procedures exist to:
 - Create/remove application access in a timely manner
 - Review user roles/permissions
- Validate that all users have accessed the application within the past 90 days.
 - Review dormant accounts
 - Inactive accounts should be removed.
- Each user has a unique user ID as described in the Port Authority Standard and Guidelines.
 - All user accounts profile should include Employee ID# and full user name.
- Roles are setup with least access required to perform job responsibilities.
- Roles should have a segregation of duties/roles.
- All accounts must have an individual or business group assigned to be responsible for account management.
- Segregation of duties and areas of responsibility must be implemented where appropriate.
- Whenever segregation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision. The PA must approve these compensating controls.
- Review of audit trails and system approvals must be performed independent and retained to document the implementation of these security controls
- Access Control List (ACL) should include:
 - Current list of ACL
 - Creation and updates to ACL
 - Testing and approvals of ACL

- The application should have the PA's warning banner on the login screen. The application has a warning banner, terms of use, and/or privacy statement that was approved by the Port Authority on the login screen.
- The system should have an access role that would allow real only access to all application, database and operating system screens, functions, logs and reports.
- Remote access should be approved, secured, and documented in accordance with PA policy. Remote access, at a minimum, must consist of multifactor authentication mechanisms, secured communications (SSL/ VPN encryption methodology), access control mechanisms and logging of user activity.

Password Controls

- Ensure that password controls for the system are consistent with this requirements or more stringent
 - Passwords must be at least 10 alphanumeric characters long
 - Passwords must be changed every 90 days (administrators every 30 days)
 - Passwords must not be shared
 - Password complexity enable (capital letter, number, special character)
 - contain at least two upper and lowercase alphabetic characters,
 - contain at least one number (0-9)
 - contain at least one special character (e.g.-+}>_?&\$%#).
 - Accounts should be locked after a three logon failures
 - Passwords should not be the same account name
 - No concurrent login capabilities
- End user accounts will be disabled (not deleted) after 60 days of non-use.
- Password file should be securely stored with limited access and encrypted.
- Application forces initial passwords to be changed and the initial passwords should not be easily guessable.
- Maintain a password dictionary and password history should be set to 5.
- Set "automatic session timeout" to 15 minutes of inactivity and require user to log back in with valid ID and password.
- Smartphones and smart device, where capable, shall leverage biometric access to provide the most security for the least inconvenience.

Application Controls

Data Validation & Input Controls

- The application should have input controls to verify the validity of the data entered.

Data Retention and Management

- All data should be classified according to its sensitivity (confidential, etc) and protected accordingly.
- Data archive strategy should be documented and in place.
 - Should specify how long active data is kept.

Data Integrity and Security

- Sensitive data, such as credit card #s and social security #s, should be encrypted.
- Data should be restricted and audit trails should be available to identify all user activity include view access to sensitive data.
- Sensitive data should be stored in the database encrypted and blocked from user views in the application unless it is authorized.
- Encryptions level at a minimum should be AES 256bit when encryption is used.

Application Interfaces

- Interfaces should have secured transmission and be archived.
- Reconciliation of data should be done on a batch record and totals. Detail data reconciliations should be completed on periodic basis.

Processing Controls

- Application databases/interfaces should have the necessary controls to prevent processing of inaccurate, duplicate, or unauthorized transactions and producing inaccurate outputs.
- Controls to ensure that all data is processed and accounted for should be in place.
- Rejected items should be logged, tracked and resolved in a timely manner.

Change Management

- Processes and tools should be used to report, track, approve, fix, and monitor changes on the application.
- The application and all changes to the application should be tested before being put into production.
 - Documentation of approval for change and evidence of testing should be in place.
 - Specific timetable/schedule should be documented.
- Emergency procedures should be documented and distributed.
- Separate environments are required for development, test, quality assurance, production.
- Procedures should require that no changes be made directly in the production environment without going through the development/test/quality assurance environments.
- Formal change control procedures for all systems must be developed, implemented and enforced.
- Where technically feasible, development software and tools must not be maintained on production systems.
- Source code for application or software must not be stored on the production system running that application or software.
- Privileged access to production systems by development staff must be restricted.

Application Logging, Audit Trails and Record Retention

- Audit trails for operating, application, and database systems should exist and reviewed.
- Users and roles should be tracked and reviewed
 - Maintain documentation

- All failed logon attempts should be logged.
- All sensitive transactions and changes should be logged and an audit trail created.
- Audit trails should contain who made the change, when it was made, and what was changed.
- Only the security administrator should have access to change or delete these logs or audit trails.
- Audit trails should be reviewed by the business owner(s) and security administrator.
- Management reporting should be produced through the application.
- Access reports by user and privilege should be produced and reviewed periodically including access violation reports.

Contingency Planning, Disaster Recovery and Backup Management

- A business contingency plan and a disaster recovery plan for the application should be documented and stored off-site, including escalation plan and current call tree.
- Plans should be tested and the outcomes of the tests (success/failure) should be documented.
- Regular backups of the application and the application data should be stored off-site.
- Application executables should be stored off-site or in escrow.
- Application configurations should be documented and backed-up.
- Full system backup should be encrypted.
- Backup procedures should be documented.
- Tape maintenance should include:
 - Periodically testing integrity of tape
 - Procedures for tape destruction due to faulty or scratched hardware.

Performance Monitoring

- Incident monitoring procedures should be documented and incidents logs should be reviewed to ensure that appropriate action is taken.
- Performance statistics should be examined and reviewed periodically by system administrators/business owner(s).
 - If vendor(s) support the application, a service level agreement for uptime, performance monitoring, updates, etc should be confirmed.
- Baseline tools or security products should be used and checked on a quarterly basis.

Patch Management

- Patch management procedures and documentation
 - Procedures should include testing, approvals, and distribution.
 - Documentation should include emergency procedures.
- Apply all new patches and fixes to operating system and application software for security.
- All security patches must be reviewed, evaluated and appropriately applied in a timely manner. This process must be automated, where technically possible.

Physical Protection

- Physical access to the application hardware should be appropriately restricted.
 - Physical access secured by single authentication mechanism i.e. swipe card.

- Physical security adequate for equipment (locked cabinets).
- Appropriate fire suppression systems should be in place.
- Environmental condition adequately controlled (no water, dirt, clutter) and monitored.
 - Temperature and humidity monitoring should be implemented.
- Security cameras installed in sensitive areas
- Power surge protection and emergency power backup are in place.
- All hardware and software assets must be inventoried.
- Visitors including maintenance personnel, to data center, server and network equipment storage facilities must be escorted at all times.

Anti-virus/Malware/ Integrity/Vulnerability Software Management

- Virus patch management procedures must be documented, including emergency update procedures.
- Anti-virus and software integrity checkers must be implemented to prevent and detect the introduction of malicious code or other threats.
- Virus software engines and definitions must be implemented and up-to-date.
- A remote distribution server should be implemented for virus software updates and documentation on remote distribution should be current and maintained.
- Intrusion detection system must be in place,
- All systems must have vulnerability scans performed before going into production and periodically thereafter. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities.
- Host-based intrusion detection/ firewalls software must be installed and enabled on all systems to protect from threats and to restrict access. Incident response procedures must be in place to address any alerts identified and system owner should be notified of alerts and what action was taken to mitigate the issues.
- Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic network locations to monitor inbound, outbound and internal network traffic.
- Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.
- Procedures must be established to maintain information security during an adverse event.
- Firewalls should be implemented.
- Firewall rules documentation should be up-to-date.
- Network management connections must be performed from a secure, dedicated network.
- Network authentication is required for all devices connecting internal networks.

Wireless Device

- Devices should be using WPA/WPA2 and AES encryption or better.
- Devices should disallow broadcasting of the SSID.
- All default parameters should be changed.

- Devices should have MAC address filtering enable or some type of authentication mechanism in place.

Web Application Vulnerabilities and Controls

- The following best practice and standards from these three web sites shall be followed:
 - The Open Web Application Security Project (OWASP) - www.owasp.org
 - www.webappsec.org (a consortium of web application security professionals)
 - Center for Internet Security (CIS) – www.cisecurity.org
- Perform data validation & integrity checks for field values and ensure the HTML special characters are stripped for all HTML request.
- Do not allow site pages to be cached by user browsers.
- All sensitive, personal or confidential data (including SSN, passwords, session IDs for sensitive applications, confidential or sensitive business transactions, etc.) should be transmitted between browser and server within an SSL-encrypted session (or other encrypted transmission) and are encrypted in the database at rest.
- All sensitive and personal data should be masked and encrypted were possible.
- Legal Issues:
 - The site should have a privacy statement and term of usage.
 - American Disability Act – Section 508 should be consider during the development process due to the requirement that federal agencies’ electronic and information technology is accessible to people with disabilities.
- Web Authentication: To prevent passwords from being passed in the clear, have authentication occur within an SSL encrypted tunnel. Use SSL (certificate) to protect the password.
- Password Reset:
 - For internal applications, reset passwords via the helpdesk or security administrator of the site
 - For external applications, send temporary password to known e-mail address, that must be changed upon login and/or
 - Have customer service reset after the user has been validated.
 - If possible, use two factor authentications like Secure ID fobs.

Credit Card Processing Checklist

- If credit cards are accepted, PCI Standards (PCI DSS v3.0) should be followed and the process should be PCI compliant. Ensure all vendors and consultants are required to be PCI compliant. Attachment - The payment card application should be PCI compliant (PA-DSS v3.0).
- A segregated network and/or an approved Point of Sale terminal should be in place for the system or terminal used to process credit card transactions.
- Maintain the security of the customer information, including not storing credit numbers, the cardholder CVC/CVV numbers or any of the data from the magnetic strip on the credit card.

- Maintain the transaction data for contesting chargebacks, ensure that the processor fees are appropriate and do reconciliations of the transactions processed and the money deposited in the Port Authority bank accounts.
- The appropriate Port Authority functional areas should be made aware credit card processing activity and should be involved applying for the Merchant ID for MasterCard/Visa, Discover and American Express.
- Create a privacy policy and procedure for staff and consultants.
- Perform quarterly vulnerability scans of the network that contains the credit card processing, annual PCI reviews according to the PCI DSS, and annual system penetration testing.
- Perform the appropriate annual assessment and provide a report on compliance (ROC) which state shows compliance.

Disaster Recovery

- The Disaster Recovery plan should include at a minimum the following areas.
 - Business Impact Analysis
 - Critical Time Frame
 - Application System Impact Statements
 - Recovery Strategy & Approach
 - Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems.
 - Disaster Definition
 - Detailed Recovery Steps for each Disaster Definition
 - Escalation Plans and Decision Points
 - System Components- An inventory of the criticality of systems (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment).
 - Disaster Recovery Emergency Procedures
 - Plan Procedure Checklist
 - Disaster Recovery Team Organization
 - Salvage Team & Team Responsibilities
 - Disaster Recovery Responsibilities
 - Essential Position – Require back-up personnel to be assigned.
 - Contacts information Disaster Recovery Team and critical vendors - this area should be reviewed semi-annually for updates and changes.
 - Post-Disaster – Detail what steps need to be taken to move from disaster mode back to normal operations.
- Contingency plans (e.g., business continuity plans, disaster recovery plans, continuity of operations plans) must be established and tested regularly.
- Backup copies of procedures, software, and system images should be taken regularly and moved offsite.
- Backups and restoration must be tested regularly

Disaster Recovery Plan Checklist

Disaster recovery is a plan which could be executed in the event of a total disaster in order to bring the computer systems back to a functioning whole. Typically, the disaster in question is one, which destroys a complete site that requires restoration of support, particularly Information Technology support. Most commonly considered causes of disasters are fire, explosion, flooding, hurricanes and tornados. Disaster recovery planning normally involves alternate locations for major systems as well as the planning and testing of switch over measures, emergency transportation and so on.

The Disaster Recovery plan should include at a minimum the following areas.

1. Disaster Recovery

- Manager Responsibilities
- Plan Administration
 - Distribution of the Disaster Recovery Plan – All team members, LAN and an offsite location should have a copy of the current plan and its attachments.
 - Maintenance of the Business Impact Analysis
 - Training of the Disaster Recovery Team
 - Testing of the Disaster Recovery Plan
 - Evaluation/Review of the Disaster Recovery Plan and Tests – the DR Plan should be reviewed and the DR Test should be performed at a minimum twice a year. Update the plan to reflect changes in activities, procedures, performance, staff, and etc. Set a regular time for the review.
 - Maintenance of the Disaster Recovery Test Results – Maintain copies of the test results and what scenarios and areas of the plan were tested.

2. Business Impact Analysis - Minimize the impact on the business with respect to dollar losses and operational interference

- Critical Time Frame - Recover the system and/or component of the system within the critical time frames established and accepted by the user community. This should include the time estimate of how long it would take to recover the whole system or any sub components.
- Application System Impact Statements - This area is where a business owner decision of what areas of the system has a priority in how it is brought back into normal operation. How long could these operations be performed without computer support?
 - Essential – Are systems or components of the system that are very critical and need to be back in operation immediately because the business cannot function.
 - Delayed – Are systems that are needed but could be delayed and could not adversely effect the business process.
 - Suspended – Are system or components that are not critical and can wait until the full system is back to normal operation.
- Recovery Strategy & Approach

3. Disaster Definition – All possible interruptions should be defined, and then the steps to minimize their impact need to be documented. This includes disk array failure, power loss, loss of network, loss of wireless network, loss remote access, equipment, computer processor failures, etc.
 - Detailed Recovery Steps for each Disaster Definition - This should be the technical steps to recover the different areas of the system like the Operating system, database, application, routers, firewall, and etc.
 - Escalation Plans and Decision Points

4. Data Center Systems – Dependencies should be notated.
 - System Components- A copy of all essential office equipment and records should be stored off-site. Specify any special computer hardware, software, databases, networks or other technology.
 - Backup Strategy
 - Storage Rotation
 - Back-up Files
 - Off Site Storage of Back-up Files
 - Back-up Files Retrieval Process, Vendor information and Forms for Off Site Storage

 - Hardware -
 - Hardware inventory for system in operation
 - Desktop Workstations (In Office)
 - Desktop Workstation location
 - Desktop Workstations (Offsite including at home users)
 - Laptops

 - Software -
 - Software inventory of the system in operation
 - Systems, Applications and Network Software
 - Communications
 - Operations

 - Off-Site Inventory

 - Supplemental Hardware/Software Inventory

5. Escalation Plans and Decision Points

6. Disaster Recovery Emergency Procedures

- Plan Procedure Checklist - should have a checklist of the plan procedures and area for documenting exceptions where the plan was not adhere to and what was done in its place. Disaster Recovery Procedures in a check list with approval format.

- Disaster Recovery Organization – should have the full disaster recovery team listed by position or individual and what are their responsibilities. This section of the plan should include Port Authority and PATH personnel, PA/PATH management, and all vendors that work or have responsibilities during a disaster. This area should be reviewed semi-annually for updates and changes.
 - Recovery Organization Chart
 - Disaster Recovery Team & Recovery Team Responsibilities
 - Recovery Management & Senior Manager Responsibilities
 - Damage Assessment and Salvage Team & Team Responsibilities

Problems and Changes - Need to be documented and what was done to rectify them.

Essential Position – Require back-up personnel to be assigned.

7. Pre-Disaster - What steps need to be in place prior to a disaster for this plan to work? If there are any assumptions, they should be notated here.

- Recovery Management
- Damage Assessment and Salvage
- Hardware Installation

8. Contacts information - This area should be reviewed semi-annually for updates and changes.

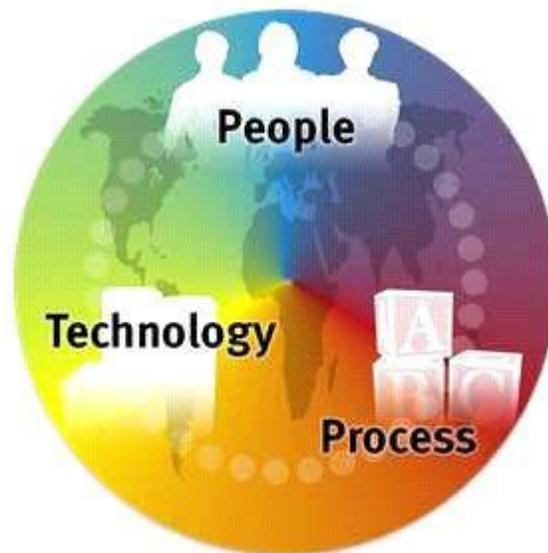
- Disaster Recovery Team - This should include primary and secondary phone numbers, home address, emergency contact information, and their backups information.
- Vendor Phone/Address List – Include account information and account representative information.
- Command Center – Primary and Alternative site locations, hot spots, phone numbers, time scheduling

9. Post-Disaster – Detail what steps need to be taken to move from disaster mode back to normal operations.

2/8/16

**ATTACHMENT N - STANDARDS AND GUIDELINES FOR PORT AUTHORITY
TECHNOLOGY**

STANDARDS AND GUIDELINES FOR PORT AUTHORITY TECHNOLOGY



Technology Department

Version 7.5
5/28/14

(PREPARED FOR RFP: Acquisition and Deployment of Agency-wide Transportation Management Software)

Table of Contents

Introduction	4
1.0 The Port Authority Wide Area Network (PAWANET).....	4
1.1 PAWANET Overview.....	4
1.2 VOIP Circuit Diagram –	5
1.3 Inter-site Services Providers	5
1.4 PAWANET Functions.....	6
1.5 Features of PAWANET	6
1.6 Supported Protocols.....	6
1.7 PAWANET Switches and Routers.....	6
1.8 Approved Servers	7
1.9 Enterprise Addressing Scheme (including IP addressing).....	7
1.10 Enterprise Network Monitoring Software	7
2.0 Network Resources	7
2.1 Network Overview.....	7
2.2 Enterprise Network Architecture.....	8
2.3 Network Naming Conventions.....	13
2.4 Directory Services and Structure.....	13
2.5 System Backup and Recovery.....	13
2.6 Business Resumption Plan.....	14
2.7 Telecommunications Standards for Enterprise Network Resources	14
2.8 Documentation	16
3.0 Virus Scanning & Management	16
3.1 Overview	16
3.2 Standards.....	16
3.3 Acquisition and Installation	17
3.4 Virus Detection and Response	17
4.0 Electronic Mail.....	17
4.1 E-Mail Overview	17
4.2 E-Mail System Architecture	17
4.3 E-Mail Environment: Design Considerations and Infrastructure	18
4.4 Integrating Applications Server with Port Authority Email System.....	19

5.0	Intranet	19
5.1	Intranet Overview.....	19
5.2	Direction of eNet Development.....	19
5.3	eNet Software Infrastructure Standards & Guidelines	20
6.0	Workstation Hardware and Operating System Software	21
6.1	Overview	21
6.2	Workstation Operating System Standard	21
6.3	Workstation Configuration	21
6.4	Workstation Security.....	23
7.0	Distributed Systems Environment.....	24
7.1	Overview	24
7.2	Microsoft Windows Servers	24
7.3	Unix	24
7.4	z/OS	25
7.5	Application Security	25
7.6	Server Physical Security.....	25
7.7	Load Balancing – Failover Architecture.....	25
8.0	Vendor Provided Dedicated Systems	26
8.1	Overview	26
8.2	Physical Security Technology Standards.....	26
8.3	Communications Infrastructure Standards.....	28
8.4	Server Infrastructure Standard.....	28
9.0	Wireless Technologies	29
9.1	Wireless Guidelines.....	29
9.2	Scope.....	30
9.3	Principles.....	30
9.4	Compliance Requirements	30
9.5	Device Specifications	30
9.6	Paging Device Policy.....	33
9.7	Cellular Phone & Wireless Modem Policy and Procedures.....	33
9.8	Technology Services Mobile Device (Windows Mobile and Apple) Policy.....	33
9.9	BlackBerry Guidelines.....	35

Introduction

The purpose of this document is to communicate the standards established by the Technology Department (Technology Department) and provide guidance in proposing Information Technology (IT) solutions for the Port Authority of New York & New Jersey (PANYNJ), the Agency.

To that end, these guidelines intend to help RFP Submitters do the following:

- Implement computing and networking solutions that ensure the utmost reliability, availability and security.
- Procure hardware and software that advances business needs in a manner that is compatible in an ever-changing IT environment that enables departments to work with each other more effectively.
- Easily and efficiently communicate and exchange information throughout the agency.
- Achieve greater systems integration so that the application will be interoperable resulting in cost effectiveness and quality control.
- Adherence to these standards ensures that IT investments achieve Enterprise connectivity, interoperability, consistency, and will enhance performance in a cost-effective way.

1.0 The Port Authority Wide Area Network (PAWANET)

1.1 PAWANET Overview

The Port Authority has a modern distributed computing network, called the Port Authority Wide Area Network (PAWANET), which is managed as an enterprise resource. It connects all the various Port Authority facilities and transportation systems using high-speed voice, data, and video lines or links.

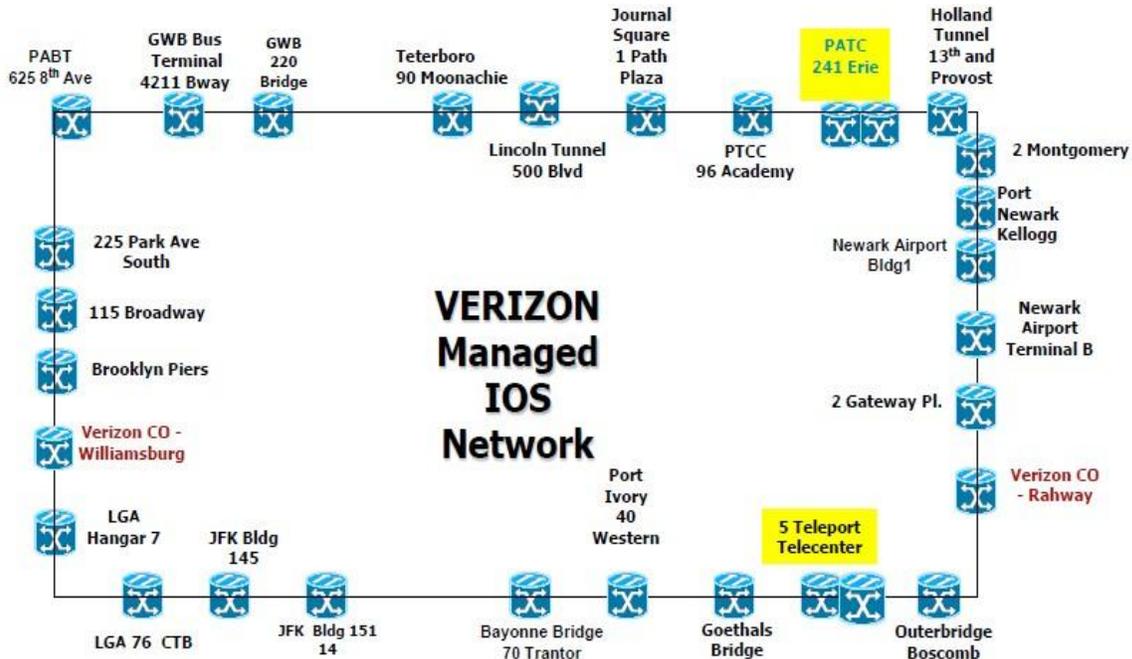
This network is crucial to all Port Authority businesses because it provides the connections for applications such as e-Mail, Internet and Intranet access, SAP, PeopleSoft, Electronic Toll Collection, Computer Aided Design and Drafting (CADD), Lease Image, Closed Circuit Television (CCTV) surveillance systems, and in the future, videoconferencing, and more.

PAWANET consist of a Managed Fiber Optic Dense Wave Division Multiplexed (DWDM) Network, provided by Verizon Select Services, as an Integrated Optical Service (IOS) network. This network consists of eleven separate and distinct (1) Gbps lightwave networks, each interconnecting with the data centers at Telecenter and the Port Authority Technical Center (PATC). Site-to-Site interconnectivity is achieved via the “hub and spoke” topology through the data centers. Additional high-speed Ethernet Private Lines (EPL) have been deployed to support key Port Authority off-ring facilities. Remote locations are linked using redundant high-speed dedicated point-to-point leased communication lines.

Remote locations are linked using redundant high-speed dedicated point-to-point leased communication lines. Wireless connectivity also supported when hardwired connections are not practical.

The network consists of state-of-the-art Cisco Systems equipment and services, such as, high performance Cisco Catalyst switches and routers. The Port Authority uses Bluewater Network Monitoring Services to monitor PAWANET, and Cisco Systems SMARTnet hardware/software maintenance services, and Cisco's Technical Assistance Center (TAC) to support and maintain the network.

1.2 VOIP Circuit Diagram –



1.3 Inter-site Services Providers

The Technology Department (TEC) has contracted with a variety of companies to provide inter-site services. Companies providing communications services for the Wide Area Network are listed below.

- AT&T Local Services
- Verizon

1.4 PAWANET Functions

Currently PAWANET is used to transport the following:

Data	Supports the low and high volume transfer of data used for applications, such as SAP and PeopleSoft, and for network communications, such as e-Mail. Provides a data path for off-site, mainframe data backup of file, print and application servers. Enables the use of Storage Area Network (SAN) for network storage of user files and routing jobs to shared network printers.
Video Voice	The transfer of Closed Circuit TV (CCTV) data is supported across the entire network to provide security for the Port Authority's key facilities. The network provides the hardware capabilities for voice and VoIP transmission.
Videoconferencing	The network switches and transmission lines are used for videoconferencing to enable diversely located staff participate in meetings across large geographic area.
VOIP	Voice Over Internet Protocol (VOIP) is in the process of being implemented for the agency to replace the legacy Nortel system, which currently serves the majority of Port Authority users. VOIP will be another data stream utilizing the PAWANET infrastructure.

1.5 Features of PAWANET

PAWANET provides a high performance and reliable fail-safe communications network. These are its key features:

- Alternate paths of communication
- Support of high volume traffic such as CADD, CCTV and others
- Catalyst 3000, 4000 and 6500 switches at all the major sites, and at the Teleport
- Cisco high performance 2000, 3000 and 7200 router family products with redundant power supplies

1.6 Supported Protocols

The network supports the following network protocols, allowing dissimilar platforms to communicate within PAWANET:

TCP/IP:	TCP/IP is the universal protocol that allows communications between all systems within the Port Authority's network, as well as other networks.
IPX/SPX:	This protocol allows communications between all Novell platforms.
SNA/SDLC:	This protocol allows communications between all IBM systems and other systems that support System Network Architecture (SNA).

1.7 PAWANET Switches and Routers

The current standard switches and routers used on PAWANET are:

- Tellabs Reconfigurable Optical Add Drop Multiplexers (ROADMS) are the DWDM nodes on the Verizon Managed IOS Network.
- Cisco High performance 3000, 4000, and 6000 series switches
- Cisco High performance 2000, 3000 series routers for intermediate connectivity. Cisco 7200 high performance routers Provide high-speed connectivity and routing capabilities across the network in support of TCP/IP, IPX/SPX and bridging functions, and provides routing capabilities for Port Authority Internet access.

- A pair of fault tolerant 10 Gbps links on IOS are established on IOS to provide the required band with between the data centers at Telecenter and PATC.

1.8 Approved Servers

Only IBM File & Print and Application servers may be connected to PAWANET.

This includes turnkey and distributed systems where File & Print or Application servers are used. Any replacement File & Print or Application servers must be IBM servers. Deviation from this policy will not be allowed, without prior approval of the Chief Technology Officer or their designee.

1.9 Enterprise Addressing Scheme (including IP addressing)

The Port Authority's enterprise network is a TCP/IP Class B network allowing for a maximum of 255 subnet assignments. Subnets assigned on a geographical basis according to the number of resources required. Workstations are configured for dynamic assignment of IP addresses via Dynamic Host Configuration Protocol (DHCP).

TD will assign static IP addresses for servers, printers and faxes that are to be connected to PAWANET.

1.10 Enterprise Network Monitoring Software

The Port Authority has selected Bluewater Network Monitoring Services to continually provide real time monitoring of PAWANET, and its data and voice link availability. To provide for real time network monitoring, the following software utilities are used by Bluewater and the Port Authority, respectively:

- Remedy Network Management software used by Bluewater
- Cisco Works for Switched Internetworks used by Port Authority

2.0 Network Resources

2.1 Network Overview

The Port Authority has a modern distributed computing network, which is managed as an Enterprise resource. The network connects all individual PCs, servers, printers, and other devices in a unified computing infrastructure that makes it possible for the Port Authority to conduct its business.

The Enterprise Network consists of the PAWANET (see Section 1.1) and connected Local Area Networks (LAN's). The line of demarcation between the cable and wiring is the responsibility of the carrier and the Port Authority's area of responsibility is usually a wiring closet. The Port Authority's Enterprise Network consists of the following components on the Port Authority side of demarcation:

Enterprise Devices

- Cabling
- Routers
- Switches
- Wiring Closets
- Communications Equipment Racks
- Server Racks
- File and Print Servers
- Application Servers
- Storage Area Networks (SAN)
- Network Printers
- Security Devices (Video Encoders, IP Cameras, ACS Panels)

LAN Devices

- Desktop PCs
- Workstations
- Voice Over IP Phones
- Laptops
- Video Conference Units
- Local Printers
- Scanners
- Copiers
- PC Peripherals

2.2 Enterprise Network Architecture

The Port Authority operates an extensive network of Enterprise file, print and application servers. These devices are linked to an Enterprise Wide Area Network. The flexibility provided by the use of multiple servers, server clusters and Storage Area Networks (SAN) offers users improved network response, greater reliability, increased data security and reduced operating cost. Adherence to the standards outlined in this section allows the Port Authority to manage their systems, applications and data in a way that best meets our business needs while maintaining interoperability and safeguarding Port Authority's information assets.

2.2.1 Server Operating System and Software

All Enterprise File & Print services in the Port Authority are currently, based on the Windows Operating System. Microsoft Windows, Linux and Sun Solaris are supported as application servers when required for functionality.

In addition to the base operating system, all servers must include the following components:

- Virus Protection (minimum: McAfee Engine 8.5.0i, with current DAT files)
- Network Security
- Remote Monitoring and Management
- Intrusion Detection
- Mainframe Systems Backup (minimum: Upstream 3.5.0c)
- Uninterrupted Power Supply (If central UPS is not installed at the location)
- Current Service Packs and security patches (minimum: SP1)

Note: All operating system and server software shall be provided and configured by the Technology Department prior to connection to PAWANET.

2.2.2 Configuration

All network devices--including servers, workstations, network printers, and network faxes--must use IP addresses which conform to the standards outlined in sections, 1.9 Enterprise Addressing Scheme, and 2.3.1, Server Names. System Administrators may refer to the Guide to System Administration for specific instructions on how to install and configure the Windows operating systems.

2.2.2.1 Drive Mapping Conventions and Organization

Mapping of workstation drive pointers to SAN or server disk volumes or folders is accomplished through a Windows Active Directory Login Script or the Microsoft equivalent. The following drive letters are reserved for Windows Active Directory installations:

Pointer	Volume or Folder
M:	Reserved
P:	Public Applications

Q:	Installation and Upgrade Utilities
S:	Departmental shared directories and files
T:	Reserved
U:	Users Private Home Directory

- Public (Shared) application software installed on a file and print server cluster must reside on a separate volume named "APPS".
Example:
P:\APP S
- Each software application installed on the file and print server, or server cluster, must have its own sub-folder.
Examples: P:\APPS\EXCEL
P:\APPS\WORD
- Shared Data stored on a file and print server cluster, shall reside in a volume named Data, and shall be mapped to the "S:\" drive pointer.
Example <Cluster_name>:\DATA\<Department_NAME>\SHARE on a server cluster
- Each Department's SHARE folder will contain at least three sub-folders titled Org, Everyone and Projects.
- Under the Projects folder will be two additional folders, one called "Active" and one called "Completed". Active projects reside in the "Active" folder.
- When staff identifies a project as being completed, the project folder will be moved to the "Completed" folder and all rights, except for "Browse" will be removed from the folder. This will ensure that the final project documents remain unchanged, while still allowing authorized staff to review the old documents and use them as templates for new documents if desired. The "Completed" folder will be set to archive its data.
- Under the "ORG" folder will be subfolders with names corresponding to the various divisions within the department. By default, only staff within a division will have access to a division's folder. These folders are intended to hold data for a specific division that would not normally be shared departmentally. Staff from other divisions would not have access to these folders unless the division manager of the owning division gives their approval. Having folders setup by divisions will simplify the process of identifying who is responsible for the contents of a folder.
- The "S" and "U" drives should only be used to store business related files.
- The Systems Administrator, at the direction of the Chief Technology Officer, may from time to time remove any data deemed to be non-business related.
- A folder called "Everyone" will be created in the Share folder. All staff in the department will have full access to this folder to store and retrieve files that are not related to a project or a division's day-to-day operations.
- Additional shared folders, with access restricted to only specific users, if required, will be created in the Share folder. Access will be restricted through the use of Inherited Rights Filters and access will be granted through the use of groups. These groups will be named using the same name as the folder name.
- In general, rights to any folder will be granted through the use of a group having the same name as the folder. The group would have trustee rights to the folder, and users would be added to or removed from the group as needed. All rights would be granted or revoked through the use of form PA-3624A. Designated staffs in each department are required to approve these requests.

- A user “U” drive will be assigned to each standard Windows Active Directory account for use by each individual user to store business related data on the network. Access to the “U” drive is restricted to the account owner only. Users receive all rights to this folder”. Users cannot share data on their “U” drive. Files should be shared only by using the Share, (“S”) drive.
- Access to a user’s home directory, by anyone other than the owning user is prohibited and will be removed after notifying the end-user.
- Installation files used in the installation of desktop software must reside in a sub-folder under the “APPS” volume

Example P:\APPS\Psoft

2.2.2.2 Connecting LAN Devices to the Enterprise Network

The Technology Department (TD) is responsible for connecting all LAN devices to the Enterprise Network (PAWANET) provided they meet the Port Authority’s standards. The following system components must meet the standards in order to connect department devices:

Type of Device or Software

- Primary Network Operating System (NOS)
- Application Server Operating System
- Network Interface Card (NIC)

2.2.3 Server Network Resources Security

2.2.3.1 Server Physical Security

All servers and communication equipment must be located in locked rooms or secured with a cable and lock with the keyboard secured to prevent tampering and unauthorized usage.

2.2.3.2 Server Logical Security

To safeguard the Port Authority’s Information Technology (IT) systems and data, TD has implemented a number of processes and procedures, including the requirement that all users accessing the Port Authority’s networks authenticate to the Microsoft (MS) Windows Active Directory (Active Directory). The Active Directory Service is a database containing descriptions of all network devices including servers, workstations and user accounts.

In plain English, this means that by executing a login when you first power on your PC you are telling the network who you are. This is accomplished by providing your Windows Username and password. Just as you are issued an ID card for access to certain facilities, buildings or rooms you need to visit to perform your job, your Windows authentication grants you access to network resources, such as shared data volumes, software applications and network printers you use in performing your assigned tasks.

TD, or its contracted vendor, is responsible for providing all enterprise servers with the following protection of their logical resources:

- Guard against unauthorized access.
- Perform daily incremental backups of servers and authorized workstations and full backups weekly.
- Store all monthly backups off site at a secure location and secure daily and weekly backups on-site in a locked area.
- Test recovery procedures annually.
- Use system and application passwords that conform to the Technology Services Department standards.
- Configurations must conform to security parameters identified by NetVision and Quest

- Intrust Suite software.
- Control all remote access using the Port Authority's Remote Access System.
- Maintain current patch levels and critical security updates.

2.2.4 Network Access and User Account Security

2.2.4.1 Account Creation

User accounts are created and managed in MS Windows Active Directory Services for the Windows network resources. Documentation for the creation of user accounts and authority for access is maintained by the Customer Service Desk Manager.

2.2.4.2 Time Restrictions

Due to the fact that The Port Authority serves its clients 24 hours a day, we do not have Login Time Restrictions on our File & Print servers. All staff may access their account 24 X 7.

2.2.4.3 Concurrent Logins

Login sessions will be limited to one connection per user. User accounts should not have the ability to login to multiple workstations after establishing one active connection to the network.

2.2.4.4 Intruder Detection

These system-monitoring features must be active:

- Restrict the count of incorrect login attempts to three before the account is locked out.
- The time for which unsuccessful login attempts are retained to determine a possible intruder attack should be a minimum of 30 minutes before the counter is reset to zero.
- The time for which a user account remains disabled before the account can be used again should be a minimum of 30 minutes.

2.2.4.5 Passwords

All user accounts must have passwords conforming to the following standards:

- Minimum length is six (6) characters.
- The password should not be easily guessed. It should not be related to one's job and should not be a word in the dictionary or a proper name.
- Should be set to expire at least every 90 days and 30 days for accounts with system or application administrator access
- Grace Logins should be activated and limited to three
- Users should be notified several days in advance of password expiration.
- Users should be forced to change their password on initial login and once it expires.
- Unique passwords should be required when changed. Users should be prevented from reusing a previous password for a minimum of one-year.
- Users should not be permitted to change their passwords more than once a day.
- Passwords should be encrypted in storage.
- Passwords must be entered in a non-display field with a re-enter verify function for new passwords.
- Passwords must not be available on hard copy.
- Passwords used in system startup files and login scripts must be encrypted.
- If an application uses a default password, change it on installation.
- Do not use cyclical passwords, such as the word, February, during the month of February.
- Do not reveal your password to anyone except authorized persons.
- Use both upper and lower case characters and special characters where possible.
- Change password if it has been disclosed or compromised.

- Protect by using a screen saver password with a recommended 15-minute time-out period.
- Passwords should not be the same as the user ID

Passwords are considered confidential data. They protect the Port Authority's network resources and grant system privileges and access. Disclosure may result in unauthorized access to data, system files and transactions. Passwords are also your signature and identify you as the individual who is responsible for the system activity.

2.2.4.6 Modems and Switches

Staff is prohibited from connecting dial-up modems and switches including wireless switches (e.g. Linksys wireless switches) to workstations that are simultaneously connected to PAWANET or another internal communication network unless approved by the Technology Department (TD).

Where modems have been approved, users must not leave modems and/or switches connected to personal computers in auto answer mode, such that they are able to receive in-coming dial-up calls.

2.2.5 Remote Access System

The use of local modems to establish direct dial connections to devices on the Port Authority's network is prohibited. Exceptions to this policy require the approval of the Technology Department's Chief Technology Officer.

The approved mechanism for remote access to the Port Authority network is through the Remote Access System (RAS). The Remote Access System utilizes an Internet-based Virtual Private Network (VPN) tunnel established over the Internet linking remote users to the Port Authority Wide Area Network (PAWANET) (remote client to PA site). It is designed to provide authorized Port Authority users with secure access to corporate applications and to files available on their departmental file servers. This access to applications and resources is delivered through a thin-client environment consisting of a farm of Citrix MetaFrame/Microsoft Terminal Services servers capable of supporting 200 or more simultaneous users each. There is no provided access to the user's office PC desktop. Port Authority offices without direct connection to the Port Authority Wide Area Network (PAWANET) can use this system to establish remote access to corporate applications located on PAWANET.

RAS provides multiple security mechanisms to ensure that only authorized users gain access to the Port Authority's computing resources and systems. Through multiple security steps, the user must respond to security challenges. After successful authentication verification, authorized users are provided with access to corporate applications and their departmental network resources through the thin-client environment.

The Port Authority also supports corporate site-to-site VPN connections and utilizes Cisco equipment for these connections.

Remote access is authorized on a case-by-case basis by the Chief Technology Officer.

2.2.6 Hardware Standards

The TD Enterprise Architecture team is responsible for setting the agency hardware standards. As of October 2012, the hardware standards are as follows:

- | | |
|------------------------------------|-----------------|
| • Desktop, Laptop, CAD* | Lenovo |
| • High End Multimedia Workstation* | Apple |
| • Mobile Devices | BlackBerry |
| • Printers* | Hewlett Packard |
| • Routers and Switches | Cisco |

- Servers* IBM and NEC
- Smart Devices iPhone/iPad
- Storage Area Network (SAN) IBM (Entry Level and Mid-Range)

* Note: To maintain optimal operating efficiency of the computing environment a standard “refresh” age has been adopted. The agency standard refresh age is greater than 5 years. TD is responsible for the automatic replacement/upgrade of hardware that has exceeded the agency standard age limit.

2.2.6.1 Standard Servers

A representative sample of standard servers is as follows:

Server Description	IBM Model
WEB Server, Small applications server	xSeries 3550M4
Medium applications server	xSeries 3650M4
Database Server, Multiple and Large application server	xSeries 3850M4
Virtual Clusters	NEC Express 5800 series or IBM as stated above

Each server shall have at least three (3) network interface ports to support a production, management and backup network, and redundant power supplies.

The Port Authority manages servers models via a lifecycle process with a minimum ‘in service’ life of three (3) years.

2.3 Network Naming Conventions

2.3.1 Server Names

The Port Authority employs a naming convention for all servers within PAWANET. That convention will be discussed during a solution implementation phase.

2.4 Directory Services and Structure

The Port Authority uses Windows Active directory to manage network resources and user access. Port Authority departments are designated as organizational units (OU) and servers are network objects contained within the OU.

All network printers should be created using Printer Properties Pro utility.

Applications are distributed using Microsoft System Center Configuration Manager (SCCM). Applications are distributed based on the type of workstation and user definitions. Scheduling of distributions is performed in conjunction with client departments.

2.5 System Backup and Recovery

There are two Port Authority approved standard software products, used to perform scheduled server backups:

- **Upstream Reservoir** is a centralized backup tool used to create data backups for all distributed systems.
- **FDR Upstream** is a Mainframe based tool used to backup all Mainframe data. Backup

data is stored on disk storage for prompt backup and restore. Encrypted tape backup is stored remotely at a secure facility, and is required to assure off-site disaster recovery data storage. All backup media and records must be treated with the same level of security and confidentiality as the original data.

The System Administrator is responsible for verifying that system backups, both local and remote backups, can be used to restore the data. Tests of the ability to successfully restore from both backup systems should be performed annually. It is recommended that:

- Tests of the ability to restore system and application files will be performed on a non-production server.
- When incremental or differential backups are routinely used, the test restore procedure should incorporate both.
- Immediately prior to performing the test restore procedure, do a special full backup on the directories being tested.

2.5.1 Backup Logs

The System Administrator will maintain the following logs for a period of two years:

- Back-up activity
- Rotation of back-ups
- Usage/rotation of back-up media
- Off-site data storage

2.5.2 Backup Scheduling

The System Administrator is responsible for performing back-ups of data, application and system files. This must be as follows:

- Weekly full back up of each server. A full back-up is a back up of all files on the server.
- Daily differential, incremental or full back up of each server or server cluster. The type of back-up performed is dependent on time constraints and the amount of data to be backed up. Incremental back ups are back-ups of all files changed since the last back up. Differential back ups are back-ups of all files changed since the last full back-up.
- A Grandfather, Father, Son (GFS) scheme based on a 33 tape rotation should be used to ensure complete back-up and recovery.

2.6 Business Resumption Plan

The vendors, providing IT services to the PA, shall work with the Technology Department (TD) to develop a disaster recovery and contingency plan. The System Administrator will participate in the planning, design, implementation, testing, updating and documentation of the plan. [Appendix 1](#) shows a recommended outline for such a plan. The Business Resumption Plan will be reviewed quarterly and tested at least annually.

2.7 Telecommunications Standards for Enterprise Network Resources

To see the standards and guidelines for the following telecommunications components, please see the Appendix.

[Appendix 2](#) - Communication Rooms/Closets Standards

[Appendix 3](#) - Standard Cabling Schemes

- [Appendix 4](#) - Unified Wiring Specifications
- [Appendix 5](#) - Telephone Closet / IDF Termination Blocks
- [Appendix 6](#) - Workstation Jacks
- [Appendix 7](#) - Standard Switches
- [Appendix 8](#) - Workstation and Lateral Cable Identification Management
- [Appendix 9](#) - Fiber Optics Specifications for Network Services - PAWANET

2.7.1 Closet and Telecommunications Room Access

The following standards must be followed regarding access to closets and communication rooms:

- All telecommunications rooms must be physically secured. Remote locations, which are not secured, by a guard or within line of sight of personnel, must be secured by a card access system and/or video cameras.
- The Network Connections (NC) group is responsible for installing routers, switches (along with Cisco Staff when applied) and station drops. They also patch connections and troubleshoot LAN cabling.
- System Administrators requiring routine maintenance of data communications equipment should call the Customer Support Desk when new devices or reconfigurations are required.

2.7.2 Telecommunications Installation Contractor's Responsibilities

1. Adherence to all of the above specifications
2. Assurance of labor harmony by providing installation technicians whom currently maintains appropriate union membership
3. The contractor must supply all cable, blocks, brackets, connectors, jacks, housings, face plates, special tools, etc., as necessary to perform an installation which is satisfactory to the Port Authority.
4. The contractor must label every workstation (jack faceplate) and the corresponding cross connect point (punch down block or patch panel) in accordance with the cable identification management plan, as previously described.
5. Install all Category 5e cabling in the proper manner, with the appropriate number of twists, to maintain Category 5e integrity and capabilities, as outlined in the TIA/EIA 568-B.2 standard.
6. The contractor must ensure that cable connections are in accordance with standard telecommunications practices and that all cabling maintains normal connectivity and continuity.
 7. All materials must be agreed upon by PA Network Services prior to the start of installation.
 8. All computer or network communication rooms and closets are to be isolated, locked, and secured. No other equipment, storage area, or smoking area are to be located in this room. This room must provide appropriate cooling and ventilation. Access to this room will be reserved to TD staff and an agreed upon Facility Manager or designee of the site where the PAWANET equipment is located. This procedure is to ensure the security and the integrity of the Port Authority's computer network and its users.

2.7.3 Electrical Requirements

The following power and receptacles should be installed to support different equipment requirements such as:

- Standard 110/120 volt power receptacles
- Standard and/or NEMA 5L630P 220/240 volt 30 amp power receptacles
- Dedicated circuit breaker per AC feed, with alternate power source.
- Server rack electrical requirements are specified in the appropriate design document.

Currently, services obtained through the PA's contract are required to have the APC (American Power Conversion) UPS included in the delivered service.

2.7.4 Telephone Company Interface

The following items are needed for the telephone company interface, if needed for a specific vendor solution:

- a) Install a dedicated wallboard for Telco demarcs (if none available for implementation)
- b) Standard Telco demarcs:
 - P66 Block
 - Network Termination Unit (Rj48 interface) Smartjacks
 - Network Termination Unit (DB15-pin female interface)
 - Network Termination Unit (V.35/V.36 female interface)
 - Digital Signal X-connect (DSX)
 - Basic T1 CSU/DSU
 - Basic DS3 handoff coax/HSSI unit
 - High-speed dialup modems for network trouble-shooting when needed

2.8 Documentation

It is the responsibility of the System Administrator to update and maintain a library of all documentation designated as standard by the Port Authority. These include archived system files and system backups. Vendors will be provided our "Guide to Systems Administration" during the implementation phase of a project. The "Guide to Systems Administration" covers the provisioning and setup of computing & networking resources to successfully implement a project within the Port Authority.

3.0 Virus Scanning & Management

3.1 Overview

This section describes the standards and guidelines for the prevention, detection and removal of computer viruses, (malware). Its purpose is to minimize the risk and negative impact of computer virus infections in the work environment by establishing clearly defined roles, responsibilities and procedures for the effective management of computer viruses.

3.2 Standards

Standard virus protection software must be installed on all network servers and personal computers, and updated on a regular basis. The Port Authority currently uses McAfee ePolicy Orchestrator (ePO) v4.5 to monitor, manage and maintain the virus definition (DAT files) of the Agency desktop computing platform. The McAfee ePO Management Agent (v4.6), and VirusScan / AntiSpyware Enterprise (v4.8), are part of the standard desktop core image.

3.3 Acquisition and Installation

The Technology Department maintains current versions of standard virus protection software and virus detection files, (DATs), including configuration-specific instructions for downloading and installing the software on network servers and desktops

3.4 Virus Detection and Response

The Port Authority's IT support vendor is responsible for responding to all virus outbreaks, as well as eradicating them and, where possible, preventing them.

The speedy reporting of all computer viruses is essential for the protection of the information stored on Port Authority LANs. Much of that information is important to the safety of the public, as well as the day-to-day business of the PA.

If the anti-virus software has detected a virus and cleaned it, no further action is required on the end user's part. If the virus is not cleaned, or the end-user suspects that a virus still exists, the end-user should immediately contact the Customer Support Desk, and they will work to remove the virus.

The Port Authority IT support vendor will respond quickly to all such alerts by doing the following:

Assess the risk

- Confirm the existence of a virus.
- Take appropriate measures to quarantine the virus so that it does not infect other Port Authority devices.

Notify Appropriate Parties

- Contact the originating party who introduced the virus to the Port Authority.
- If it is a new virus, contact our antivirus vendor, McAfee, for further assistance.

Remove the virus

- Work with appropriate parties until the virus is removed.

In addition, the Port Authority's IT support vendor will report on all such outbreaks on a weekly basis. The report must include:

Support Ticket Number

User Name

Virus Name

Information which was lost, (if any)

Time to correct the problem, (lost staff time)

Virus Origin, (if this can be determined; Diskette, CD, Internet)

4.0 Electronic Mail

4.1 E-Mail Overview

The Port Authority's Electronic Mail System (E-Mail) is designed to facilitate business communication among employees, job shoppers, contractors, consultants, and outside business associates. This E-Mail system is comprised of Microsoft Outlook desktop software accessing e-mail stored on Microsoft Exchange servers. This solution also includes group calendaring and workgroup collaboration.

4.2 E-Mail System Architecture

The Port Authority's E-Mail system is hosted by AT&T Corp, who acquired USinternetworking, a managed application service provider; and consists of Microsoft Exchange servers connected to the Port Authority's enterprise network. Authorized Port Authority staff access their corporate e-mail through Microsoft Outlook desktop software on the network. The system has multiple Exchange servers containing mailboxes and Public Folders. Additional servers host Outlook Web Access,

BlackBerry services, and perform Internet-based e-mail services including anti-spam and anti-virus e-mail checking.

The hosted Exchange site is on a Windows resource domain with a one-way trust to the Port Authority's corporate user account Windows domain located on the Port Authority network. This Port Authority Windows domain is used for Windows authentication services when the Outlook client is opened. In addition, the Port Authority hosts DNS servers to satisfy requests from the Outlook client as needed.

High-speed, secure, and redundant network connections connect the AT&T's data center and network to the Port Authority network.

4.3 E-Mail Environment: Design Considerations and Infrastructure

The E-mail environment is further described below:

- The E-Mail system is comprised of Microsoft Outlook 2007 desktop software accessing e-mail (via MAPI mail protocol) stored on several Microsoft Exchange 2007 servers
- E-mail is protected by TrendMicro's InterScan Messaging Security Suite and ScanMail for Microsoft Exchange virus protection software products on the Exchange servers.
- Incoming Internet-based e-mail is also scanned for Spam and for viruses through McAfee (MX Logic), a web-based service provider.
- The servers are currently configured for the following messaging protocols:
 - o MAPI (Microsoft's Messaging Mail protocol) and SMTP
- IMAP4 and POP3 mail protocols, NNTP news protocol, and LDAP directory protocol are disabled.
- Front-end Exchange servers running TrendMicro's InterScan Messaging Security System (IMSS) are being used to send and receive Internet SMTP mail. No other mail system connectors (such as Lotus Notes) are in place.
- RIM's BlackBerry Enterprise Server software for Exchange provides wireless e-mail and calendar access to BlackBerry wireless handheld device users.
- There are several forms of SMTP addresses used at the Authority. Exchange Active Sync is used to provide email and calendar access to Apple iPads/iPhones and Windows Mobile devices.
- Exceptions are governed by the Authority's directory services structure and user account requirements.
- Each individual e-mail message and its file attachments have a combined limit of 10MB.
- Each regular user mailbox has the following size limits:
 - 80 MB - user receives warning notice
 - 90 MB - user is prohibited from sending
 - 100 MB - user is prohibited from sending or receiving
- Other mailbox sizes exist on an exception basis.
- This E-Mail system also includes group calendaring and workgroup collaboration.
- Public Folders are supported based on departmental and agency-wide requirements and, in general, are used for dynamic items for a form of workgroup collaboration. Static documents like corporate policy statements are placed on the corporate intranet (EmployeeNet) and not on the Public Folders. Documents requiring long-term storage are stored elsewhere such as on Windows file servers.

4.4 Integrating Applications Server with Port Authority E-mail System

4.4.1 Requesting SMTP Services

The vendor will request SMTP services from and coordinate its work with the Technology Department

Port 25 needs to be available to utilize it for SMTP services.

4.4.2 Email Restrictions

The following restrictions are in place to protect the SMTP system and the “reputation” of Agency mail servers on the Internet:

- Forged email headers are STRONGLY discouraged, but applications for circumvention will be entertained, and valid business justifications must be included. The “From” and “Reply-to” fields should be valid users on the system sending email.
- Settings: The maximum number of recipients per email is currently 90. This includes “To”, “cc”, and “bcc”; maximum size with attachments is 10MB. Emails that do not conform to these restrictions will be rejected by the SMTP servers.
- Mail will be relayed only if your server has an entry in the SMTP access database.

Note: SMTP logs are checked periodically for policy violations. Repeated violations and failure to correct them will result in SMTP services being disabled for the offending system.

5.0 Intranet

5.1 Intranet Overview

The Port Authority EmployeeNet (eNet) is intended to provide timely information and resources to employees via the web browser on their desktops. eNet is a decentralized collection of web pages, data lookup services and applications that are managed as if they were a centralized enterprise resource. It is accessible to all personal computer workstations on the Port Authority Wide-Area Network (PAWANET). eNet is housed on servers at the Teleport. Examples of business information hosted on eNet include:

- Departmental Websites
- Directories
- Corporate Announcements
- Reference Materials
- Document Collections
- Library Services
- News Displays
- Enterprise and Departmental Applications

5.2 Direction of eNet Development

eNet is intended to provide a convenient, timely and accurate source of information for Port Authority employees as well as providing access to enterprise and departmental applications. The owner of content on eNet is responsible for authorizing its publication, its accuracy and timeliness. Technology Services provides a common infrastructure and technical support for those departments that electronically publish agency information or make available electronic resources.

Infrastructure standards and guidelines are recommended to ensure compatibility and facilitate maintenance. Departments requesting specific applications should discuss their requirements with eNet staff to determine a solution that best meets the department's business needs.

5.3 eNet Software Infrastructure Standards & Guidelines

Category	Software Name	Minimum Version
Browser:	Microsoft Internet Explorer	7.0
Browser Plug-in	Windows Media Player	10.0
	Adobe Acrobat Reader	9.0
	Macromedia Shockwave Player	9.0
Web Server Software	Sun One Web Server	6.1
	Microsoft IIS	5.0
Media Server Software	Microsoft Media Server	9.0
Application Server Software	Adobe Cold Fusion 9	7.0
Development and Design Tool	Adobe CS5	11.0
Database	Oracle Database	9i
	MS SQL Server	2008
	MS Access	2007
Programming Language/Scripts	ColdFusion MX	7.0
	Java	6.0
	PERL for Windows	5.0
	JavaScript	1.0
Search Engine Software	UltraSeek	5.7
Web Performance Monitoring	WebTrends Marketing Lab 2	2.0
Content Management	Stellent	7.5
	Open Text Website Management	10.1

5.3.1 Design Guidelines

We have developed the following guidelines to ensure that all web pages on eNet have a consistent look, feel and navigation scheme, while providing creative flexibility.

Departmental Web Site Standards and Guidelines

Prescribed standards are assigned to only the following items:

- Resolution: Pages are designed for optimal viewing at the 1024x768 setting.
- Page Width: Each page has a fixed page width of 960 pixels.
- Page Justification: The entire page is center-justified within the browser window.
- Page Layout: Each web page will follow the same, basic layout:
- A Global Navigation strip;
 - A Masthead;
 - A Local Navigation strip;
 - A Body area (with a 1-column, 2-column or 3-column layout);
 - A Footer.

5.3.2 Accessibility Guidelines

TD's eBusiness Unit is committed to making all eNet content accessible to persons with disabilities. In order to ensure that all eNet web content is in compliance with accessibility guidelines and applicable legal requirements, contact the Webmaster via email at webmaster@panynj.gov, or call 212-435-3294.

6.0 Workstation Hardware and Operating System Software

6.1 Overview

The Port Authority makes extensive use of computers (workstations) networked into an Enterprise Wide Area Network to accomplish its business objectives. For the purpose of this section, the term computer and/or workstation will be used to reference desktop, laptop and CAD computing devices. In order to ensure compatibility with the agency's enterprise network and to make optimal use of its resources, this section defines the standards governing workstations and their configuration and use.

6.2 Workstation Operating System Standard

The Port Authority's standard operating system for workstations is Microsoft's Windows XP Professional. The following are operating systems used within the Agency:

- Microsoft Windows XP SP3
- Microsoft Windows 7
- Apple OS X

6.3 Workstation Configuration

6.3.1 Workstation Naming Conventions

All departmental workstations must contain a unique computer name which is the machine's serial number.

Example: Workstation name: 23AAH86

System Administrators are responsible for naming workstations and maintaining an up-to-date inventory of equipment and names used.

6.3.2 Automated Software Distribution for Computers

The Port Authority currently uses Microsoft System Center Configuration Manager (SCCM) 2012 to, at a minimum, do the following:

- Install new, or upgrade existing, software on Agency desktop, laptop, and CAD computers
- Create packages to automate system tasks (e.g. data migrations of desktop computers, eDiscovery requests, etc.).
- Bare Metal Provisioning of Servers.

6.3.3 Remote Workstation Management

The Port Authority also distributes software applications and upgrades via Novell's ZENworks. Each workstation should have Novell's Workstation Management module installed as part of the NetWare workstation client. This will enable remote distribution and updates of software, hardware inventory and workstation troubleshooting.

6.3.4 Drive Mappings

Computer drive mappings are automatically accomplished using a Microsoft login script. The script is executed upon successful login to the Agency's Microsoft domain.

6.3.5 Standard Workstation Hardware Configurations

There are standard configurations established for workstations and laptops. The standards specify the product approved for the following devices: processor, memory, storage, CD/DVD-ROM/multimedia and monitor. The following is current workstation standard:

Lenovo ThinkStation D30 4223-CC9 - Custom PA configuration based on Lenovo Model 4223-69U; (1) Intel Xeon E5-2650 2.0Ghz 8core – (2) x 8GB RAM - (2) 500GB SATA HDD - NVIDIA Quadro 4000 2GB - Windows 7 Professional x64.

Lenovo ThinkPad T430 2347-EZ4 - Custom PA configuration based on Lenovo Model 2347-G6U; i5-3320M, (2) x 4GB RAM, 14.0" High Definition+ Wide Screen Display, 720p Camera, 500GB 7200rpm Hard Drive, Backlit Keyboard-None, Intel 6205 PCIe mini card, PCIe WWAN upg, Finger Print Reader, Blue Tooth, Battery Cells 9, Intel vPro, Windows 7 Professional x64.

Lenovo ThinkCentre M92p 3212-C14 - Tower - Custom PA configuration based on Lenovo Model 3212-C7U; 4x5 i5-3550, (2) x 4GB RAM 1600MHz, 250GB 7200 rpm hard drive, Bay DVD±RW, Media Reader-None, High Definition 2500 Graphics Card, Display Port Dongle-None, Chassis Intrusion Switch-None, Energy Star 5.2, Intel vPro, Global Program-None, Windows 7 Professional x64.

NEC AccuSync AS191WM-BK Flat Panel display- TFT-19" widescreen 1440 x 900 /250 cd/m² 1000:1 5ms 56 - 75 Hz Analog RGB 0.7 Vp-p/75 Ohms DVI-D and VGA 15-pin D-Sub

NEC MultiSync EA243WM-BK - LED monitor - 24" - 1920 x 1200 - TN - 250 cd/m² - 1000:1 - 25000:1 (dynamic) - 5 ms - HDMI, DVI-D, VGA, DisplayPort - speakers - black

6.3.6 Standard Workstation Software

The following software is the standard Port Authority software for departmental workstations. New computer installations should conform to the existing standard.

6.3.6.1 Standard Workstation Software

The following list is a compilation of the core software components found on the computer Arc Build (commonly referred to as an image).

- Windows XP, Professional Edition
- Lumension Patchlink
- System Center Configuration Manager - SCCM
- McAfee Antivirus
- Internet Explorer
- Microsoft Office Professional

Because technology is rapidly changing, TD should be consulted to obtain the most recent versions of standard software.

6.3.7 Enterprise Software

The following is a list of standard enterprise application software used in the Agency. The applications supported by third party service providers are: PeopleSoft, SAP and Livelink Content Management.

6.3.8 Other Business Applications

Other Enterprise applications are deployed on occasion to user workstations. This includes systems like the Business Expenses system, (BEAM) and BudgetPro. System Administrators are responsible for deploying the workstation clients and network server software according to standards and guidelines provided by the Technology Department.

Current list of Enterprise applications, is shown below –

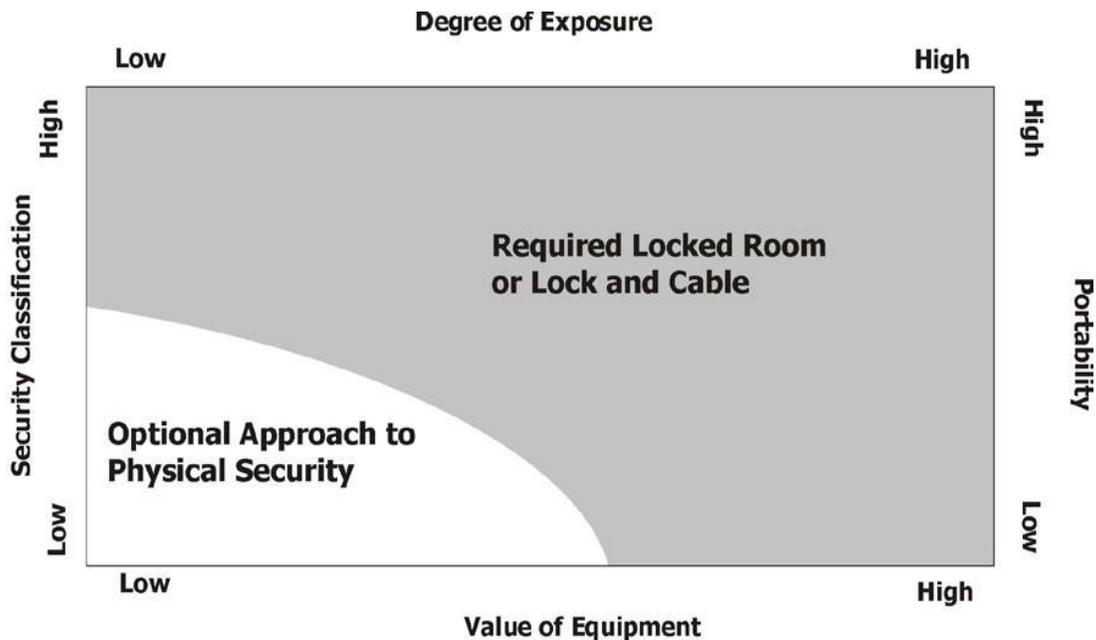
AutoCAD	Oracle
BudgetPRO	PeopleSoft
Cognos Client Software	Primavera
Livelink	SAP
Microsoft Server	Schedulesoft
MS SQL	TRIM

6.4 Workstation Security

Workstation users and their managers are responsible for the security of computer equipment and safeguarding critical corporate data and access to Port Authority network resources. This includes both the physical securing of equipment as well as logical safeguarding equipment and data.

6.4.1 Physical Security

The method of control should be based on the value of the equipment, the sensitivity of the data, its portability and the degree of exposure to theft. The department's Business Manager should make the appropriate determination of physical security required based on their best business judgment. The graph below provides general guidance to Business Managers in determining the level of physical security required.



In all cases, laptops must be secured with a Lock/Cable product (e.g., Kensington).

6.4.2 Logical Security

The Technology Department (TD) is responsible for providing for the security of computer resources and devices:

- Workstations are protected with Novell and Microsoft directory security mechanisms.
- Screen saver passwords are implemented with a maximum of a fifteen (15) minute time-out.
- All critical data are backed up nightly onto either external media or a network drive.

7.0 Distributed Systems Environment

7.1 Overview

A number of enterprise servers provide critical application and system services. Different operating systems and configurations may be required for specific applications. This section provides information on the standards and guidelines for supported systems within the Port Authority.

7.2 Microsoft Windows Servers

The standard for general-purpose application servers and File and Print Computing is IBM servers. Microsoft Windows 2003 & 2008 Server (Enterprise) are supported Operating Systems for application servers.

7.2.1 Virtual Environment

The standard for Virtualization Computing is both IBM and NEC FT host servers. The Port Authority will provide a VMware ESX-based Guest Virtual Machine (VM) to operate all Contractor-provided applications software on one of the above host computing platforms depending on the critical nature of the application.

All applications software shall be capable of operating in a virtual environment under VMware ESX server and shall operate in a VMware ESX-based Guest Virtual Machine (VM) on a 'shared' host-computing platform for Contractor application, unless performance or other requirements mandate a dedicated system.

7.2.2 Windows Data Encryption

For those applications that require additional data security measures, TD offers additional tools that provide encryption services to protect the data stored in the application's database, even from authorized individuals that have physical access to the applications and database servers but not the decryption key.

7.3 Unix

Sun/Oracle Solaris is the currently supported UNIX operating system for infrastructure (e.g., SMTP services) and corporate servers. RedHat Enterprise Linux Server is the supported operating system for infrastructure and corporate servers (e.g., SAP, Peoplesoft).

7.3.1 Unix Security

Unix and Linux servers must be physically and logically secured from unauthorized access. Operating system logical security is defined by the Technology Department (TD).

7.3.2 Backup

Critical system backup must be performed regularly (daily and/or weekly) utilizing our centralized backup strategy and associated tools. Extra copy of backup is kept offsite for disaster recovery purposes if required.

7.3.3 Download Scripts in the Unix/Linux Environment

- The script must be written in a generally supported language: Perl, Korn shell and Powershell. Powershell should be consistent with Microsoft standards and best practices.
- The script must be limited in access, as well as the script's owner's user account. The owner of the script should be able to read, edit, and execute the script, but no one else (with the exception of the root or administrator accounts).
- If the content being downloaded is public information or widely available on the Internet, File Transfer Protocol (FTP) may be used.
- For all other content, Secure FTP must be used, and a key exchange made with the entity who is providing the content. A username and password must be used when retrieving the content.
- If the entity cannot accommodate the use of SFTP, ftp may be used as long as the content is encrypted with a secure, widely used utility like PGP.
- Information and guidance on securing passwords should follow Recommendations of the National Institute of Standards and Technology.

7.4 z/OS

z/OS (currently release 1.5) is the IBM-supplied operating system on the IBM 2096-R07. This hardware/software supports multiple users and multiple applications. Provided on this platform for transaction-processing applications are TSO/E, ISPF, and CICS. The database is DB2, although other file structures are also supported.

7.4.1 Databases

Oracle 10.2.0.5 or higher and MS/SQL 2005 Server or higher are the supported database platforms for Port Authority systems. Auditing trail enabled for all database accounts with administrator privileges.

7.4.2 Geospatial Databases

This GIS environment is built on an ESRI platform using ArcSDE for the spatial database. ArcGIS Server 10 and ArcSDE Version 10 are the supported platforms for the current GIS environment.

7.5 Application Security

TD recognizes the critical importance of application security and maintains a Best Practices document containing rules and recommendations for purchased applications, and those developed in-house.

7.6 Server Physical Security

All servers and communication equipment must be located in locked rooms or secured with a cable and lock with the keyboard secured to prevent tampering and unauthorized usage. The Business System Manager is responsible for determining the appropriate access control method (receptionist, metal key lock, magnetic card door locks, etc.) This person must also maintain a list of persons authorized to enter secured areas. Technology Department staff is available to provide technical assistance in making this determination.

7.7 Load Balancing – Failover Architecture

Depending on the requirements of the application, load balancing and failover architectures are supported.

8.0 Vendor-Provided Dedicated Systems

8.1 Overview

Vendor-Provided Dedicated Systems refers to the application software and possibly the computer hardware that may be furnished and/or installed by an outside contractor. These systems are usually procured through either a Request for Proposal (RFP), or a “Low Bid” contract and are specifically engineered to support a dedicated application.

These systems generally support Capital Projects, which are usually large scale, multi-year engagements, requiring specialized technical and management staff, as well as, Systems Integration support. These projects normally have significant construction components and require the coordination, design and support from many diverse Engineering and Technology disciplines.

On all technology related projects a representative from the Technology Department (TD) provides a single point of contact for technology oversight, accountability, adhering to standards and systems integration, which is required under the Roles and Responsibilities of the Director and is expected by our client departments.

To ensure a successful project implementation and honoring our responsibility to the Agency and our customers, one of the steps undertaken by TD is to provide guidance and focus attention on, adherence to and compliance with the Port Authority Technology Standards and Guidelines.

By following the Standards and Guidelines, it enables the Port Authority to

- Leverage large discounts negotiated in the various requirements contracts.
- Ensure that the seamless integration of equipment with other existing systems.
- Ensure that long-term maintenance and systems administration contracts are focused on the same product lines.
- Ensure that the relevant sections of the Standards and Guidelines are included in either, the basic design of a low bid contract or as requirements in an RFP. Responses to RFP's shall be reviewed for their compliance with the Standards and Guidelines.
- Deployment, integration and testing shall be monitored by TD to ensure that equipment or infrastructure is not duplicated, that the integration and migration plan will not adversely affect existing systems, and to integrate new systems under existing maintenance contracts where applicable.

In cases where a specific vendor or system is so specialized that it normally does not adhere to the hardware, software, infrastructure and operations guidelines of the Standards and Guidelines, the vendor shall be directed to work with TD in exploring all options. If an exception is required, the vendor should work with TD to prepare the necessary business case scenarios to receive written concurrence from the Chief Technology Officer for this deviation from the Port Authority Technology Standards and Guidelines.

8.2 Physical Security Technology Standards

8.2.1 Agency Standard for Digital Video Recording, Access Control and Alarm Monitoring

Based upon the Agency's investment and positive experience with Lenel's Systems OnGuard access control and alarm monitoring application offering as well as Verint Nextiva, CCTV and Digital Video recording technologies, these product sets are the Agency's standard. Below is a description of when these standards apply.

The Port Authority has long recognized the need for a corporate architecture for its security systems that would allow us to integrate digital video and access control recording compatible technologies agency-wide. Using these standards will improve the Agency's security posture and will permit us to leverage additional operations and business benefits while keeping our operations resources, maintenance and support costs at a minimum.

The standard will also improve:

- Access to and the sharing of information from a centralized location
- Centralized monitoring of all facilities from an Emergency Operations Center
- The operational and cost-effectiveness of adding a variety of modular features to the core systems, such as paging, e-mail, fire systems, facility management, etc.
- Alarm notification, response, and acknowledgement
- Operational flexibility for facility and Public Safety staff
- Single learning curve
- Reduce the cost for maintenance and system administration

Guidelines for using the Verint Nextiva standard

include:

1. If the CCTV system needs to be recorded
2. When an existing system is in place, at a PA facility or at a tenant facility that is monitored/reviewed by PA personnel, and needs to be upgraded or expanded to accommodate a particular project.
3. When rule based intelligence is to be added like motion detection and other related algorithm processes, all efforts should be made to ensure compatibility, functionality, maintainability (version upgrade resiliency) with the existing Verint system.
4. If WEB based video needs to be made available
5. When monitoring at remote locations is needed to view on site operations and archived events via the corporate WAN
6. When live video monitoring is required
7. When distributed recording is required i.e. at multiple locations, concurrently
8. When network transport (communication) medium has limited bandwidth and the video needs to be sent to designated workstations on the network. All network transport tasks and bandwidth planning is required to be discussed with Technology Department before proposing any solutions
9. On all new projects where Verint Nextiva is the current site base system
10. When the Office of Emergency Management (OEM) department needs override capabilities in the event of an emergency
11. If third party technology (non-Verint supplied) is required to be integrated with the current Verint system at a facility, that technology must be compatible with the existing Verint system at the particular facility. Any third party integrations need to be reviewed and approved by the Technology Department and be approved for use by the manufacturer (Verint) for the software version in production at the facility. When a (Verint) software upgrade is required in order to deploy a third party interface, that upgrade will have to be coordinated through TD, the facility, and the appropriate contractors(s).
12. Any server or workstation supplied in conjunction with a particular system must comply with the hardware and software requirements of both the Port Authority and the manufacturer of the video management software.
For more information regarding CCTV standards, reference the CCTV Standards and Guidelines documentation.

Guidelines for using the Lenel OnGuard standard

include:

1. All new or upgrade projects that require electronic card access and / or alarm monitoring
2. All projects that will have security that needs to be monitored by PA personnel or contractors (airports are monitored by contractors)
3. All new projects where Lenel OnGuard is the site base system currently
4. Where access is required to work with ID cards that exist and are compatible with the agency standard
5. When the OEM department needs override capabilities in the event of an emergency
6. If third party technology (non-Lenel supplied) is required to be integrated with the current Verint system at a facility, that technology must be compatible with the existing Verint system. Any third party integrations need to be reviewed and approved by the Technology

Department and be approved for use by the manufacturer (Lenel) for the software version in production at the facility. When Lenel software upgrade is required in order to deploy a third party interface, that upgrade shall have to be coordinated through TD, the facility and the appropriate contractor(s).

7. Any expansion of card access systems (added card readers, sensors, etc.) need to be reviewed and approved by the Technology Department to ensure that the new devices meet the agency standards for card access (including but not limited to: card formats, badge layouts, encryption algorithms, etc.)
8. Any server or workstation hardware required in conjunction with a specific system must be provided by the Technology Department.

Currently the Access Control Task Force is working on the Access Control Standards for the Agency. The work is tentatively scheduled to complete by year-end 2013. The Access Control Standards documentation will be available upon completion.

8.2.2 Situational Awareness Platform Software

The Situational Awareness Platform Software (SAPS), is a software application that allows multiple, independently manufactured and installed security, life safety, and building systems to all interoperate under a single, common operating picture, giving a user access to information spreading across multiple systems as if they were all one single system. This “common view” is made even more valuable by the incorporation of powerful, rules-based tools within the SAPS system, which allows intelligent linking of seemingly unrelated events into “Situations” that represent patterns of activity that pose a threat to security or site-wide operations.

The SAPS objective is to monitor the identity and event data from the various systems, identify incidents and anomalies, and detect trends that could be a threat to our facilities. SAPS turns data into actionable intelligence when an incident is detected. SAPS have the capability to automatically alert the security operations staff and push the information to security control centers and first responders.

- Provide a software platform to enable integrating the various electronic systems across all agency sites
- Provide a single software perform solution for situational awareness.
- Provide a single system database for reports
- The SAPS will provide transparent notification of security related events for all agency security systems.

8.3 Communications Infrastructure Standards

The Port Authority Standard for Communications Infrastructure is Cisco. This applies to all future systems, as well as, upgrades to existing systems. This standard ensures the interoperability of all deployed systems and permits the full integration of systems into PAWANET. In addition, all Cisco equipment either designed in a low bid contract or specified in an RFP must be purchased through the Cisco Requirements contract, which is administered by TD and permits the Agency to purchase equipment, maintenance and support services under the high discounts negotiated in the Requirements Contract.

This standard applies but is not limited to; Layer 2 and 3 Ethernet switches, Routers, Wireless Access Points (WAP), Mobile Access Routers (MAR), GIG E (Gigabit Ethernet) switching and networking and SONET (Synchronous Optical NETwork) equipment. Deviation from this standard requires the written consent of the Chief Technology Officer.

8.4 Server Infrastructure Standard

The Port Authority’s standard platform for File & Print and Application servers is IBM. Technology Services has contracted discounted pricing with our service provider for its servers

and hardware support. In order for the agency to take full advantage of these savings, any new Application servers or File & Print servers must be built using IBM hardware purchased by TD. This includes turnkey and distributed systems where File & Print or Application servers are specified in the design. Any replacement File & Print or Application servers must be IBM servers. Deviation from this policy will not be allowed without prior approval of the Chief Technology Officer or his designee.

9.0 Wireless Technologies

9.1 Wireless Guidelines

9.1.1 Purpose and Scope

This section references the standard policies and procedures for all wireless devices and technologies including voice and data capabilities that store, process, transmit or access data. This includes but is not limited to commercial and unlicensed wireless networks and laptops, cellular devices, scanning devices, messaging devices (email devices) and PDAs.

9.1.2 General Policy

Employees will only use PA owned wireless devices to store, process, transmit or access PA data. The following must be considered:

- Wireless Technologies Vulnerabilities Protection
- Minimum Requirements
- Identification and authentication at both the device and network level.
- Confidentiality encryption of data transmitted is required.
- Data end-to-end over an assured channel (a communication link with security protocol such as Secured Sockets Layer).
- At the device level, implement file system encryption where applicable.
- Devices should not be connected to PA systems for data synchronization, data transfer, or any other purpose without virus protection, mobile code restrictions (executable information delivered to information system and directly executed on any architecture that has appropriate host execution environment) and other preventative measures.

9.1.3 Personal Area Networks - PAN

PAN technologies should not be used for transmitting information without encryption.

Bluetooth security alone is unacceptable because it is not encrypted and does not use Federal Information Processing Standardization (FIPS) 140-1/2.

Wireless devices should be procured without Bluetooth embedded transmitters, when not possible transmitter should be disabled.

9.1.4 Wireless Local Area Networks – WLANs

9.1.4.1 Overview

Business requirements have arisen throughout various Port Authority locations for the improved use of Wireless LAN technology to facilitate local user mobility. Research performed on the different technologies support the use of Cisco as opposed to various wireless vendors in an attempt to produce a standard that will provide the agency with a secure, robust and scalable solution as WLAN's continue to grow within the agency.

In summary, the current Port Authority Wireless LAN standards are based upon IEEE 802.11n draft 2.0 technologies. (802.11n is backwards-compatible with existing 802.11a/b/g network adapters.)

The physical infrastructure is now based upon a centralized WLAN architecture that relies upon Cisco wireless bridges, access points, mesh routers and newly implemented controllers. WLAN's

should be standardizing on the 4404 and 4402 controllers at this time as described further in this document.

Wireless LAN technology is continually developing with rapidly evolving industry standards, government regulations, and vendor products. As a result, the WLAN Standard presented in this document will likely be superseded in the future as the technology and products change.

9.2 Scope

The scope of this document shall present some standards for the Agency Wireless LAN and the specification of all devices and configurations.

9.3 Principles

At the highest level, the principles for the Wireless Standard are based upon the following attributes:

- Security - use of strong encryption (e.g. WPA-TKIP/ WPA2- AES) for use as authentication of all traffic on a port-to-port basis, with the use of credentials stored on a back-end RADIUS server utilizing key distribution.
- Scalability - with LWAPP access points & use of LWAPP tunnels
- Reliability - via authentication of users to the networking enterprise mode.
- Manageability - via secured ports and VPN / FW access.

9.4 Compliance Requirements

All specifications defined in this document may be effective upon approval of and complete concurrence with TD's Chief Technology Officer, to update wireless standards and policies as per IEEE and Wi-Fi Alliance Standards

9.5 Device Specifications

The following sections will provide the various hardware components, and related firmware versions, that are specified for use in the Port Authority's WLAN solution.

9.5.1 Access Point (AP) Standard

Standards Details:

- 3600 AP's are the agency standard for WLAN deployment. These AP's have 802.11n 2.0 radios. Backward compatible to 802.11 a/b/g.
- 1310 AP/ Bridge is certified for use in unique situations where both internal and external antennae are supported. The major distinction is that of a more rugged chassis designed for higher-stress outdoor-type conditions. 3250 mobile routers for mesh deployments.
- AP Deployments will be Lightweight Access Point (LWAP)
- AP Standard Summary:
 - a) Two cables per pull during wiring for wired to wireless.
 - b) AP's & controller placements via RF propagation results. c) PA supported standard AP's need to be verified with TD
 - d) If wireless is primary connection-'load-balance' AP' cabling connection to two different network switches
- WLAN Controller Standard
This standard is in the process of being upgraded to Network Control System (NCS) & Identity Services Engine (ISE) Appliance to accommodate more advanced wireless deployments.

- **Best Practice**

The following information is industry best practices for wireless hardware implementation agency- wide deployments, not for wireless device configuration practices.

WLAN Best Practices Add-ons:

1. Ensure that the PA maintains an up-to-date wireless hardware inventory.
2. Identify rogue wireless devices via wireless intrusion prevention systems (IPS)
3. Enable automatic alerts on the wireless IPS
4. Perform stateful inspection of connections.
5. Augment the firewall with a wireless IPS
6. Mount AP in location that do not permit easy physical access
7. Secure handheld devices with strong passwords
8. Enable WPA and WPA2 under ENTERPRISE mode
9. Synchronize the AP's clocks to match networking equipment.
10. Manage remote physical locations of all access points which support an isolated network that needs access to PAWANET for server farms and internet access.
11. Maintain cryptographic strength range from 128-bits to 256-bits with matching symmetric algorithms AES-128 to AES-256

Wireless Control System (WCS):

1. Single license
2. Secure "WIRELESS LOCATION APPLIANCE" with real-time client tracking & RF fingerprinting
3. Secure Windows-Based deployment as minimum, for example, windows server 2003; intel dual-core; 3.2 GHz; 4-GB RAM; 80-GB hard drive; IPS devices; IOS firewall routing; HTTP port 80; HTTPS port 443.
4. Multi-homed server (i.e., two NIC cards)
5. Secure WCS and IIS (i.e., internet information service), installation sequence
6. Create configuration group (configure multiple controllers)
7. Secure auto provisioning with filtering
8. Secure WCS with RF modeling for heat map planning
9. Secure 15 second alarm summary refresh

9.5.2 Portable Electronic Devices (PEDs) – Cell Phones, PDAs, messaging devices, laptops and tablets

If a device receives information via a wireless technology, and that device allows that information to be placed directly into the corporate network at the workstation level, then all perimeters and host-based security devices have been bypassed. Therefore, the following procedures apply:

- PEDs connected directly to a PA wired network via a hot sync connection to a workstation shall not be permitted to operate wirelessly at the same time. Wireless solutions could create backgrounds into corporate networks.
- IR, Bluetooth and 802.11 peer to peer should be set to "off" as the default setting. Mobile code should be downloaded only from trusted sources over assured channels.
- Anti-virus software should be on devices and workstations that are used to synchronize/transmit data, if available. Where not available on a device, you need to disable the synchronization capability or provide server or workstation based handheld anti- virus protection.
- PEDs are easily lost or stolen therefore approved file system/data store encryption software should be installed.
- PEDs need to be capable of being erased or overwritten to protect data. If the device is no longer needed and cannot be erased or overwritten, it must be physically destroyed.

9.5.3 Cellular and Wireless Email

Cellular and wireless email devices are subject to several vulnerabilities (e.g. interception, scanning, remote command to transmit mode, etc). Therefore, the following procedures apply:

- These devices are not to be allowed into an area where classified information is being discussed unless it is rendered completely inoperable.
 - Must have end-to-end encryption.
- PC based redirectors are not allowed as it requires the PC to be active at all times only server based redirectors should be used.
- Electromagnetic sensing shall be periodically performed to detect unauthorized LANs, Bluetooth transmitters etc.

9.5.4 Synchronization

Some synchronism systems will operate even if the workstation is locked and the wireless or handheld device is not registered with the sync application on the workstation. As long as the workstation is on, the user is logged on, the data application client (e.g. MS Outlook) is active, and the “hot sync” cable is attached to the workstation; any person can place a compatible wireless or handheld device in the “hot sync” cradle and download data. Therefore, the following procedures apply:

- “Hot sync” cable or cradle has significant security risks, therefore perform “hot sync”, and then remove immediately once “hot sync” operation is complete.
- Secure “hot sync” cables and cradles.
- Use only PA approved third party sync access control software installed on all workstations.
- PA owned devices may only be synchronized with PA owned computer systems

9.5.5 Responsibilities of Technology Department

- Monitor and provide oversight of all PA wireless activities, insure interoperability of wireless capabilities across the agency.
- Develop appropriate technical standards and guidelines for secure wireless and handheld solutions.
- Establish a formal coordination process to ensure protection of PA information with PA information systems employing wireless technologies.
- Review and evaluate wireless technologies, products, solutions that meet PA requirements.
- Identify approved monitoring mechanisms for wireless devices to ensure compliance with policy.
- Periodically review approved wireless technology standards and procedures to ensure products and solutions remain compliant.
- Support risk management activities associated with evaluating wireless services
- Act as central coordination point and final approval authority for any exceptions to this policy.
- Define or approve acceptable wireless devices, products, services and usage.
- Provide immediate consultation to PA units.

9.5.6 Responsibilities of Technology Services Voice Networks Group

- Adhere to wireless procedures and standards, establish procedure for reviewing and approving requests for using wireless devices to store, process, or transmit information.
- Establish procedures for periodically reviewing approved wireless devices and services to ensure that the business requirement for device/service/system is still valid and meet current PA guidance.
- Establish procedures for inventory and control of wireless devices and equipment.
- Establish procedures and implementation plans for auditing wireless connections to the network.
- Provide user training.

9.5.7 Responsibilities of Wireless and Handheld Device Users

- Coordinate all requests through Technology Department...
- Read and follow standards and guidelines.
- Access information systems using only approved wireless hardware, software, solutions and connections.
- Take appropriate measures to protect information, network access, passwords and equipment.
- Use approved password policy and bypass automatic password saving features.
- Use extreme caution when accessing PA information in open areas where non-authorized persons may see PA info (airport lounge, hotel lobby).
- Protect PA equipment and information from loss or theft at all times, especially when traveling.
- Keep current anti-virus software on devices.
- Use appropriate Internet behavior (e.g. approved downloads).
- Exercise good judgments in efficient cooperative uses of these resources and comply with current and future standards of acceptable use and conduct at all times.
- Report any misuse of wireless devices, services or systems to management.

9.6 Paging Device Policy

9.6.1 Policy

The Port Authority obtains its paging services under governmental contracts. All orders for paging service or equipment must be placed under these contracts. If the contract service provider cannot meet the paging requirements, a memorandum requesting approval to obtain paging service outside of the contract's must be sent to the Chief Technology Officer.

9.7 Cellular Phone & Wireless Modem Policy and Procedures

9.7.1 Policy

The Port Authority obtains cellular service under governmental contracts. All orders for cellular service or equipment must be placed under these contracts. If the contract service provider cannot meet the requirements, a memorandum requesting approval to obtain cellular service outside of the contracts must be sent to the Chief Technology Officer.

9.8 Technology Services Mobile Device (Windows Mobile and Apple) Policy

9.8.1 Introduction

Mobile devices are a class of handheld computers that currently offer limited functionality with compact size and portability. Mobile devices are designed to replace the paper organizer; functionality typically includes maintaining a date book, address list, to-do lists, email, etc. Additional functionality such as Word and Excel are already included in many Mobile devices, with further enhancements predicted.

In order to better serve the PA, and to limit the expense of supporting a wide variety of Mobile device hardware and software, Technology Services will support the use of the Windows and Apple IOS based devices.

With a Mobile device, a user can maintain their calendar, address book, to-do list, and e-mail on a platform that is very portable and easy to use. Integration with Outlook makes it possible for users to keep identical, synchronized copies of data on both the desktop application and the Mobile devices.

9.8.2 Hardware – Hyper Link

Manufacturers using the current Windows Mobile or Apple IOS software are supported.

9.8.3 Software

The current version of Windows Mobile or Apple IOS software are supported.

Microsoft ActiveSync is used for connecting to the corporate E- Mail system.

Any software found to interfere with normal operation must be uninstalled in order to receive support from Technology Services.

9.8.4 Support

Support for Mobile devices hardware and software is provided by Technology Services through the Customer Support Desk. TD will support the physical hardware connection (PDA cradle to PC) and software to support this connection. No software can be added to company owned mobile devices without TD's assistance and Chief Technology Officer approval.

9.8.5 Training

Training will be available covering basic mobile devices use and integration with Outlook at the time of installation of the equipment. Training classes for the mobile devices may be provided in the future depending on user demands.

9.8.6 Acquisition

The PA will purchase Mobile devices for employees with a business need for the mobile device. Employees are responsible for obtaining management approval. TD also recommends that a protective case (preferably a zippered case) be purchased to reduce damage to the units. Since the PA owns the device, if an employee leaves the PA, the device is returned to the director's office of their department.

9.8.7 Personal Acquisition

Employees, who purchase their own mobile devices, will not be allowed to connect to the PA corporate network or equipment, unless approved by Technology Services.

Customer Support Desk personnel will support all PA owned and authorized mobile devices.

9.8.8 Data Security Considerations

Since in most cases the data residing on a mobile device is not encrypted or password-protected, data can be easily browsed by anyone having possession of the device. Users should carefully consider what type of information they store on their mobile. Extreme caution should be taken when using company confidential data on the mobile units.

All mobile devices accessing corporate resources should be password protected.

At the present time, Technology Services is researching options for encrypting mobile data using a third-party application. Until a solution is found, great care should be taken to ensure that important or confidential information does not end up in the wrong hands.

9.8.9 Data Backup

Though it does not happen often, it is possible to lose, damage or duplicate the data that resides in the mobile devices and PC applications. Technology Services will provide assistance in attempting to recover files or data from data corruption.

9.8.10 BlackBerry Device Policy & Procedure

The Port Authority provides corporate wireless e-mail services using the BlackBerry device from RIM.

The BlackBerry is a palm-sized device designed to synchronize with Outlook and other e-mail systems. With a BlackBerry device, one can read, compose and respond to e-mail messages and meeting requests, which are transmitted through the Port Authority's E-Mail System. The

BlackBerry contains the user's synchronized Outlook "Contacts" address book, Outlook Calendar, memo pad and task list as well as a calculator and an Internet browser.

9.9 BlackBerry Guidelines

9.9.1 Introduction

BlackBerry devices (data only or combined data (e-mail) & voice) are available from most wireless carriers in the Port District. Combined BlackBerry devices are designed to replace stand-alone cellular telephones and stand-alone BlackBerry data devices and they operate on the same wireless network as a stand-alone cellular telephone from the same carrier.

9.9.2 Support

Support for BlackBerry devices is provided by Technology Services through the Customer Support Desk. The Customer Services/PMO Group provides additional support as needed.

9.9.3 Breakage and Loss

Be aware that the screen used on a BlackBerry device is very fragile. Dropping a device from the height of a desktop can result in breakage. It is also sensitive to water damage. Once this happens, the device is likely to be unusable. Broken, lost or stolen devices should be reported to the Customer Support Desk at 212-435-7469, who will notify the appropriate staff for further action. As with all PA equipment, BlackBerry devices should be used for business purposes only.

9.9.4 Data Security Considerations

Data residing on a BlackBerry device can be easily browsed by anyone having possession of the device. Agency policy automatically activates the password security available on the device. Users should not disable this security feature. Users should carefully consider what type of information they store on their devices. Extreme caution should be taken when using company confidential data on the devices.

9.9.5 Data Backup

Though it does not happen often, it is possible to lose, damage or corrupt the data that resides on the BlackBerry device. There are data backup features on the PC utilizing the BlackBerry Desktop Manager software. We recommend setting the advanced automatic backup to 7 days with the backup of all device application data. In the event of a lost or broken device, this backup may be used to recover lost data.

Appendices

Appendix 1 -- Business Resumption Plan Document Format

I. PURPOSE

- Goals and objectives of plan
- Benefits obtained if plan properly implemented

II. SCOPE OF PLAN

- Planning assumptions
- Facilities and resources included in plan

III. NOMENCLATURE

- Recovery terms
- Definitions and acronyms

IV. DISASTER SEVERITY DEFINITION

Define level of potential disaster based on impact to critical functions. Explain what degree of operational disruption would constitute each level of disaster:

- catastrophic
- serious
- major
- limited

V. OPERATIONS RECOVERY PROCEDURES (Procedures for recovering services)

1. Indicate time frames in which essential operational/business functions must be resumed.
2. Specify sequence of operations recovery events and individuals responsible for activity. Note any specific activities required for particular levels of disaster severity. For example:
 - Notifications
 - Preliminary evaluation
 - Activate operations recovery personnel
 - Coordinate with emergency personnel
 - Evaluate recovery options and issue directive which details:
 - Assigned tasks
 - Project schedule/time frame
 - Coordination required
 - Identify relocation activities, if required
 - External/internal status updates
3. Identify items required for backup of critical functions. For example:
 - Alternate work site
 - Hardware/software
 - Personal computers

- Necessary software packages
- Documentation
- Peripherals (printers, modems, etc.)
- Databases
- Emergency equipment
- Communications
- Transportation
- Supplies
- Security
- Operations and procedures manuals

VI. OFFICE/FACILITY BUSINESS SITE RESTORATION PROCEDURES

(Procedures for restoring physical facilities)

- Identify restoration responsibilities
- Assess damage
- Develop restoration plan/time frames

VII. BRP UPDATE PROCEDURES

- Specify responsibility for updating and communicating BRP changes
- Indicate frequency of review/update

Appendix 2 -- Communication Rooms/Closets Standards

SPACE

All data communication rooms must be designed with required and estimated space to meet immediate requirements, as well as, future growth.

ENVIRONMENTAL

The following conditions must be met:

- a) Doorways/Entrances must be designed to support at least the minimum space requirements of 90”Hx72” Wx60” D.
- b) The room’s cooling capabilities must be sufficient to support the heat dissipation requirements for the equipment. This requirement will be measured in minimum and maximum BTUs powered by AC-powered systems. Equipment specs will be supplied by TD upon request.
- c) Backup UPS systems are necessary to avoid equipment damage in case of site power failure.
- d) Telco demarcs must be located in a central location with sufficient space to house Telco termination equipment.
- e) The room should be designed with the appropriate fire safety regulations such as a sprinklers, pre-action of FM 2000 systems.
- f) Cables trays must also be installed in the communications room ceiling where appropriate, to support the routing of data communications and Telco cables.
- g) Basic 24”W/30”D/84”H cabinets with 19” racks must be installed to house communications equipment such as: routers, switches, hubs, DSUs/CSUs and monitors.
- h) To create more wall space the use of wall mount racks can be installed. Appropriate sized plywood must be installed prior to mounting racks.
- i) Category 5e/6 cable must be terminated in wall/rack mounted patch panel.
- j) Fiber patch panel must be installed in fiber IDF panel with SC female interface.
- k) The fiber must be neatly tie wrapped and enclosed in flexible inner-duct.
- l) Telephone access must be installed in the appropriate location to provide for basic troubleshooting and vendor support.
- m) All communications equipment and cabinets must have ample room for easy access and proper ventilation.

Appendix 3 – Standard Cabling Schemes

- a) Teflon-coated cables will be installed per fire code regulations.
- b) Overhead cable trays and drop post must be installed for cable routing.
- c) Cabling scheme must be used to label and identify all cables. All cables must be neatly tie-wrapped.

Appendix 4 -- Unified Wiring Plan

To satisfy existing and future voice and data communications requirements, while minimizing the need for wiring changes and additions, the Port Authority has adopted the following lateral wiring specifications for all workstations being constructed. This plan is applicable to all PA locations, except when specifically noted.

LATERAL CABLE:

Voice and data telecommunications requirements for each workstation will be provided by a combination of three individual cables, installed between the workstation and the serving telephone closet / intermediate distribution frame (IDF), in a "home run" configuration. All cabling installed will be of plenum type, fire retardant (FEP) rated.

Cable specifications:

- (3) Cables capable of supporting Category 5e capabilities as outlined in the TIA/EIA-568-B.2 standard. Specifically:

Gauge: 24 AWG Pair

Size: 4

Insulation: Plenum, fire code rating (FEP)

Cable allocations will be as following:

Cable #1: Voice** Cable
 #2: Data
 Cable #3: Data

- *100.0MHz is the speed the PA wants to deliver to the desktop.
- **Cable #1 is to be split in the workstation to support 2 telephones.

Technical specs for the Cat 5e cable is as follows

TECHNICAL DATA - ELECTRICAL

Frequency MHz	Horizontal		Patch	
	Attenuation dB/100 m max.	Next dB min.	Attenuation dB/100 m max.	Next dB min.
1	2	62.3	2.4	62.3
4	4.1	53.2	4.9	53.2
10	6.5	47.3	7.8	47.3
16	8.2	44.2	9.8	44.2
20	9.3	42.7	11.1	42.7
31.25	11.7	39.8	14.1	39.8
62.5	17	34.3	20.4	34.3
100	22	32.3	26.4	32.3

TECHNICAL DATA--PHYSICAL

	CMR	CMP	CM (Patch)*
	0.02	20	24
Conductor diameter-in. (mm)	-0.52	-0.52	-0.61
Cable diameter-in. (mm)	0.195 -5	165 -4.2	215 -5.5
Nominal cable weight-lb./kft. (kg/km)	21 (31)	21 (31)	23 (34.2)
Max. installation tension-lb. (N)	25 -110	25 -110	25 -110
Min. bend radius-in. (mm)	1 -25.4	1 -25.4	1 -25.4

* Patch cables utilize stranded tinned copper conductors

PARAMETRIC MEASUREMENTS

	Horizontal	Patch
Mutual Capacitance	4.6 nF/100 m nom.	5.6 nF/100 m nom.
DC resistance	9.38 Ohms/100 m max.	9.09 Ohms/100 m max.
Skew	45 ns/100 m max.	45 ns/100 m max.
Velocity of Propagation	72% nom. Non Plenum	72% nom.
Input Impedance	100 + 15% 0.7772-100 MHz	100 + 15% 0.772-100MHz
	ISO/IEC 11801	

COLOR CODE			TEMPERATURE RATING	
Pair 1	White/Blue	Blue	Installation	0 degrees C to +50
Pair 2	White/Orange	Orange	Operation	-10 degrees C to +60
Pair 3	White/Green	Green		
Pair 4	White/Brown	Brown		

Appendix 5 -- Telephone Closet / IDF Termination Blocks

Lateral Data cabling serving each workstation will be terminated on a CAT5e/6 patch panel (RJ45 face, 110 punch rear) in the telephone closet. For analog phone service, termination is to be on 110 blocks in telephone closet, allowing access to the telephone riser. For data, a patch cord is installed between patch panel and IT device. The patch panel can be mounted on the wall with a wall mount kit or in a rack if one is needed and should be appropriately numbered with the workstation number. The patch panel must be capable of supporting Category 5e/6 the TIA/EIA-568-B.2 standard. The patch panel shall have a swing away faceplate or rack mountable.

NOTE: The Category 5e/6 patch panel should be equivalent to the AMP SL series 110Connect Category 5e/6 patch panel or approved Category 6 patch panel. The number of ports may vary.

Each workstation shall be assigned a unique station identification number.

Appendix 6 -- Workstation Jacks

Workstations will be equipped with various components of the AMP Communications Outlet system (AMP equivalent can be used with TD approval). Each workstation will be installed with (1) double-gang jack housing box and matching face plate, capable of securely mounting three Category 5e cables or Category 6 and four modular data connectors, maintaining the integrity of category 5e/Category 6 capabilities as outlined in the TIA/EIA-568-B.2 standard. All workstation jacks will be wired in accordance with the TIA/EIA-568-B.2 standard. All modular jacks are to be labeled in accordance with TD number schema.

Appendix 7 -- Standard Switches Inside the Department

Any switches in the following Cisco series are acceptable (Vendors will consult with the Technology Department (TD) to determine the appropriate switch configuration at the time of proposal submission):

- Cisco 3000 series – low capacity Cisco
- 4000 series – medium capacity Cisco
- 6000 series – high capacity
- Cisco Nexus 7000 series – high capacity

Appendix 8 -- Workstation and Lateral Cable Identification Management

WORKSTATION AND LATERAL CABLE IDENTIFICATION/MANAGEMENT (Facility)

All lateral cabling installed to workstations at the Port Authority Facilities must be designated in accordance with the Port Authority's workstation and lateral cable identification code: This code consists of two elements, as follows:

- 1 - Room number or department name (acronyms are acceptable).
- 2 - Workstations (3 numeric digits)

The cable identification code for Workstation 10 in room 3801 at LGA CTB is 3801-010. The cable identification code for Workstation 15 in PA Automotive shop is Auto-015

Appendix 9 – Fiber Optic Specification for Network Services - PAWANET

General Scope of Work

1. Conduct a walk thru based on the specific Scope of Work for the job in question.
2. Note that all diagrams and or sketches that may be provided are approximates and not to scale.
3. All fiber optic cable is to be installed in rigid conduit or, where applicable, in plenum rated flexible inner duct.
4. Contractor shall furnish and install fiber optic cable as designated in the specific Scope of Work.
5. Fiber optic cable type for interoffice use shall be loose tube, with aramid yarn water block:

- Singlemode Fiber – 8.3/125/250 micron diameter (core/cladding/coating) manufactured by General Cable or approved equal.
6. Fiber optic cable attenuation from the factory, before installation, shall not exceed:
 - Singlemode – 4db per km @ 1310nm/.3 db per km @ 1550nm
 7. All fiber optic cable is to be labeled on each end and at any junction or patch panel with, 28 gauge, 2” wide embossed with ¼” high letters. The labels are to be fastened to the fiber optic cable using sealed wrap around labels or pliable Velcro ties.
 8. Fiber optic cable shall be installed in accordance with the manufacturer’s specifications. Any portion of the cable damaged during installation will be repaired or replaced by the contractor without any additional cost to the Port Authority of New York New Jersey.

Fiber Optic Terminations

1. Fiber optic terminations will use **SC** connectors unless otherwise specified in the Scope of Work.
2. Fiber optic terminations shall not yield more than 1db per mated (at the bulkhead) connector

Fiber Optic Testing

1. Fiber optic testing shall be performed by the contractor and certified fiber optic technicians.

Fiber optic technicians will be prepared to complete test procedures with the following equipment:

- Source and power meter testing to provide optical loss measurements.
 - Reference test cables and mating adapters that match the cables to be tested.
 - Cleaning materials – lint free cleaning wipes and pure alcohol.
 - OTDR test set with the proper launch cables and adapter types.
 - Power loss testing from both ends.
2. Fiber optic technicians will perform OTDR test on all terminated fibers unless otherwise noted in the Scope of Work.
 3. Fiber optic test results shall be recorded, and reports provided to the PA in hardcopy and via a readable txt file (PDF or RTF is acceptable).

Appendix 10 -- Public Telephone Ordering Guidelines

Technology Department (TD) staff is responsible for the management of the permit for public telephone service are available to answer any questions and provide direction for any matter relating to public telephones.

General Guidelines

All public telephone requests – that is both coin and non coin in any Port Authority space or any area of the tenant space – both “public” and “club” locations will be coordinated by the Port Authority to cover both New York and New Jersey.

Process

When the Facility, Property Manager, tenant or their representative (e.g., designer, architect, general contractor) has a public telephone requirement, they will contact the Technology Department (TD) whom will review the request and provide coordination with the appropriate service provider.

**ATTACHMENT O – INTELLIGENT TRANSPORTATION SYSTEMS DESIGN
GUIDELINES**
