

THE PORT AUTHORITY OF NY & NJ

PROCUREMENT DEPARTMENT
ATTN: BID/PROPOSAL CUSTODIAN

2 MONTGOMERY STREET
3RD FLOOR
JERSEY CITY, NJ 07302

REQUEST FOR PROPOSALS (RFP)

TITLE: DEVELOPMENT & MAINTENANCE OF AN AVIATION FACILITIES
MAPPING SYSTEM (FMS)

NUMBER: 29362

RESPONSE DUE DATE: Monday March 11, 2013 TIME: 2:00 PM

QUESTION DUE DATE: Wednesday February 20, 2013 TIME: 3:00 PM

BUYERS NAMES: ISABEL AMADO

PHONE#: (201) 395-3435

EMAIL: iamado@panynj.gov

STACEY WILLNER

PHONE#: (201) 395-3343

EMAIL: Swillner@panynj.gov

SUBJECT: REQUEST FOR PROPOSALS FOR PERFORMANCE OF EXPERT PROFESSIONAL SERVICES - DEVELOPMENT AND MAINTENANCE OF AN AVIATION FACILITIES MAPPING SYSTEM (RFP #29362)

The Port Authority of New York and New Jersey (hereinafter referred to as the “Authority”) is seeking Proposals in response to this Request for Proposals (RFP) for performance of expert professional services as required to design, develop, and maintain a Facilities Mapping System (FMS) comprised of subsurface utility and surface assets for John F. Kennedy International Airport (JFK), LaGuardia Airport (LGA), Newark Liberty International Airport (EWR), Stewart International Airport (SWF), and Teterboro Airport (TEB), and to include ongoing source document data entry. Work shall also include tasks related to the migration of the existing Utility Management System (UMS), as more fully described herein, to the FMS as well as ongoing field services and UMS document data entry until cutover to the FMS.

The selected Proposer shall enter into an agreement with the Authority for two (2) years, with two (2), one (1) year renewal options, at the Authority’s discretion. The scope of the tasks to be performed by the Consultant are set forth in Attachment A (including Appendices thereto) to the Authority’s Standard Agreement (the “Agreement”), included herewith. You should carefully review this Agreement as it is the form of agreement that the Authority intends that you sign in the event of acceptance of your Proposal and forms the basis for the submission of Proposals.

Proposers are advised to read the solicitation document carefully as solicitation structure and requirements vary from prior solicitations for similar services.

I. PROPOSER PREREQUISITES

The Authority will consider Proposals only from those firms able to demonstrate a minimum of five (5) years of continuous experience immediately prior to the date of the submission of its Proposal that they are:

- A. maintaining utility and base map data, and surveying using commercially available geographic information systems (GIS); and
- B. providing services complying with the Federal Aviation Administration (FAA) Office of Airports, Airport Surveying-GIS Program and the following FAA initiatives, including at least one project specifically demonstrating compliance with one or more of the following four (4) initiatives:
 - 1. Advisory Circular 150/5300-16A “General Guidance and Specifications for Aeronautical Surveys: Establishment of Geodetic Control and Submission to the National Geodetic Survey”
 - 2. Advisory Circular 150/5300-17B “General Guidance and Specifications for Aeronautical Survey: Airport Imagery Acquisition and Submission to the National Geodetic Survey”
 - 3. Advisory Circular 150/5300-18B “General Guidance and Specifications for Submission of Aeronautical Surveys to NGS: Field Data Collection and Geographic Information System (GIS) Standards”
 - 4. Advisory Circular 150/5300-13 or 150/5300-13A, “Airport Design”

A determination that a Proposer meets the foregoing requirements is no assurance that the Proposer will be selected for performance of the subject services. Firms that do not meet the requirements shall not be further considered.

II. PROPOSAL FORMAT REQUIREMENTS:

To respond to this RFP, the Proposer shall submit a concise Proposal complying with the following format requirements:

- A. To be acceptable, the Proposal shall be twelve (12) point or greater font size. Each resume shall be two (2) pages maximum, single-sided. Product brochures and other sales literature will not be accepted as substitutes for written responses to this RFP. Proposal pages shall be numbered and bound, or in a 3-ring binder, with “Your Legal Firm Name” and “**RFP Number 29362**” clearly indicated on the cover.
- B. Separate each section of the Proposal with a tab divider labeled in accordance with the section letter of the Submission Requirements specified below.
- C. All Proposals must be delivered in sealed envelopes and/or packages addressed to: The Port Authority of New York and New Jersey, 2 Montgomery Street, 3rd Floor, Jersey City, NY 07302, Attention: RFP Custodian, by the Response Due Date set forth in Section II.F below Proposer shall provide:
 1. One (1) reproducible original Proposal (containing original signatures and clearly designated as such);
 2. Eleven (11) double-sided copies of the Proposal;
 3. Twelve (12) compact discs (CDs) containing a digital file version of the Proposal; and
 4. In a separate sealed envelope clearly marked “Cost Proposal”, include one (1) reproducible original, eleven (11) completed copies of Attachment D, and twelve CD copies, with a digital file containing an unlocked version of the Cost Proposal in Microsoft Excel format. The Cost Proposal and associated material/documentation shall only be provided in said separately sealed and marked envelope, and nowhere else in the Proposal.

Failure to separate and seal Attachment D “Cost Proposal” information within your Proposal may deem your entire submission non-responsive.

- D. Notwithstanding retention of the CDs, in case of conflict, the reproducible original of the Proposals and the written hard copy Agreement, if awarded, shall take precedence over material on the CDs.

Consistent with environmentally preferable procurement practices, the Authority requests all documents submitted to be in a form that can be easily recycled and to provide only supporting literature, which directly relates to the Proposal being submitted.

- E. To ensure the appropriate handling of your submission, the Proposer shall use its **FULL LEGAL NAME WITHOUT ABBREVIATIONS** on any return address, and on any information submitted on the CD, as well as on the reproducible original and each copy

of its Proposal. Failure to comply with this requirement may lead to a delay in consideration of your Proposal, and thereby delay contract awards. Any such delays will be the responsibility of the Proposer.

F. Your Proposal shall be sent in sufficient time so that the Authority receives it **no later than 2:00 p.m. on the date specified on the cover sheet (Response Due Date).** **The outermost cover of your submittal, as well as the outside package, must include the RFP Number, full legal Firm name, and the RFP title clearly indicated.** The Authority assumes no responsibility for delays caused by any delivery services.

G. If your Proposal is to be hand delivered, please note that only individuals with proper identification (e.g., photo identification) will be permitted access to the Authority's offices. Individuals without proper identification will be turned away and their packages not accepted. The Authority assumes no responsibility for delays caused by any delivery service.

III. PROPOSAL SUBMITTAL REQUIREMENTS:

To respond to this RFP, provide the following information:

A. In the front of your Proposal, a copy of Attachment B, "Agreement on Terms of Discussion," signed by an officer of your company. Any modifications or change to this document will preclude your Proposal from the evaluation process.

B. Each Proposer shall submit a transmittal letter on its letterhead, signed by an authorized representative, demonstrating compliance with the "Proposer Requirements" stipulated in Section I above.

1. If the Proposer intends to utilize subcontractors, the Authority will consider the relevant demonstrated experience of each subcontractor in determining whether the Proposer has met the prerequisites set forth herein. Any decision that a Proposer has met the prerequisites that is based on the experience of a subcontractor will be reconsidered if the proposed subcontractor arrangement is withdrawn by the Proposer.

2. If the Proposer is a joint venture, the Authority will consider the experience of each of the joint venture partners in determining whether the Proposer has met the prerequisites set forth herein.

Note: In the event a joint venture submits prequalification information, the foregoing standards should be met as follows:

a. If the joint venture is a legal entity, the entity should meet the experience standards; if it is a common law joint venture, at least one member should meet them.

C. Complete a copy of Attachment C - Company Profile.

D. Technical Proposal - The Proposer shall submit a Proposal that details and clearly describes its experience and capability to develop and support a FMS system inclusive of ongoing source data entry and other related tasks as described in this RFP. At a minimum, the technical proposal shall address the following:

1. FMS Solution - The Proposer shall describe in detail the approach it plans to employ to satisfy the requirements as more fully specified herein. . This shall include the formal processes/methodologies in place for solution development and implementation that will allow the design and development of a stable GIS rooted solution (able to be relied on for mission critical functions in an active 24 x 7 environment). This discussion shall clearly delineate, in table format, the list of ALL products that will form the basis of the solution along with what functionality the product will perform. Include notes describing how the proposed products will work together with special mention of any custom codes, scripts, utilities, etc. that will be required.

The technical solution description shall also include:

- a. An overall pictorial schematic of the proposed solution;
 - b. A technical schema that delineates what hardware configuration and ALL associated software products (including version) that are required for implementation of the FMS solution;
 - c. A high level system implementation plan detailing the time frame for all key tasks including any assumptions that will be used to satisfy the requirements. The implementation plan shall be inclusive of all stages (installation, analysis, development/configuration, QA testing, migration to production) and should clearly indicate system go live date.. If the solution requires a phased approach, this shall be highlighted and explained.
 - d. Description of proposed end user training program. This shall include, but not be limited to, a discussion of the nature and type of training required, estimated duration, method of delivery, timeframes for refresher training, etc.
 - e. Description of the system and confirmation that the system complies with the Standards and Guidelines for Port Authority Technology (Attachment E), Technical Requirements (Attachment F), Audit Controls Checklists (Attachment G), and the Authority’s “Information Security Handbook” available on the web at: <http://www.panynj.gov/business-opportunities/pdf/Corporate-Information-Security-Handbook.pdf>.
2. Data Conversion/Loading of data from legacy UMS: Describe in detail the proposed methods to be employed to ensure data from existing UMS is carried over. The data is currently in an Oracle database (Oracle 9i Enterprise Edition). Include an explanation of how the Proposer is able to detect and correct corrupt records from tables and fields at the database level and associated reconciliation/verification tasks.
 3. On-going Field Construction Coordination Work: Describe the proposed approach for performing this work.

4. On-going Application Maintenance & Administration of FMS: Describe in detail the proposed on-going maintenance plan. What resources will be required? How will 24 x 7 support be provided? Include the following:
 - a. Identify the tools, and the application that comprises the FMS solution, as well as tasks associated with application maintenance and administration.
 - b. Tasks associated with the on-going source document data entry
5. Confirm the formal maintenance processes and methodologies to be adhered to, and identify prior engagements in which Proposer successfully employed these processes and methodologies, including, but not limited to:
 - a. detecting and correcting defects (including twenty four (24) hour on-call availability);
 - b. enhancing existing functionality and adding new functionality;
 - c. applying legally or contractually mandated application changes, such as FAA regulations, etc;
 - d. applying version upgrades, releases and fixes (including report generation/updates);
 - e. change management;
 - f. answering users' questions;
 - g. participating in disaster recovery tests;
 - h. providing a quality assurance review/methodology for maintenance activities; and
 - i. enforcing installation standards.

The Proposer shall indicate, for the Authority's sole consideration, which, if any services, can be provided off site and the benefit to the Authority for such an arrangement.

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

E. Firm Qualifications and Experience

1. Firm Qualifications and Experience – Identify specific firm experience, during the last three (3) years, where your firm (including subconsultants), provided services on projects of similar size and scope to that contemplated in Attachment A. It is desirable that Proposers demonstrate the following firm experience:
 - a. certified geographic information systems professionals (GISP), and demonstrated experience with ESRI/AutoDesk product suites;
 - b. migrating legacy information using extract/transform/load procedures into Commercial Off the Shelf (COTS) maintenance system software products:

- i. Aviation GIS experience, including, but not limited to obtaining and processing Airport Operations Area (AOA) data and providing the data in compliance with the FAA NEXTGEN initiatives;
- ii. Consolidating GIS viewers to integrate to CMMS/Asset Management/Maintenance Management Systems (i.e.: Maximo, SAP, etc.) with utility infrastructure; and
- iii. On-going data entry – on-going efforts to take data from as-builts and other projects highlighting requisite skill sets.

Present this information in a Table, to include but not be limited to the following for each project:

- Project Title
- Project Manager
- Duration of Project (Dates Started/Completed)
- Contract value (total value of services performed by your firm)
- Indicate whether said projects were completed on schedule and within budget
- Client Name
- A brief project description summary. Identify your specific scope of work. Highlight any unique challenges or obstacles and how they were handled. Identify any similarities to this project.
- Client contact name, phone number, and email address (project reference). The Authority reserves the right to contact such references at anytime.

2. Description of security certifications (SSAE16)

The Proposer shall produce an “Independent Service Auditor’s Report on a Description of a Service Organization’s System and the Suitability of the Design of Controls” in accordance with the American Institute of Certified Public Accountants (AICPA) Statement on Standards for Attestation Engagements 16 (SSAE 16) specific to the services to be provided in this Agreement. *[Note - Any auditor’s report produced after 6/15/2011 previously under SAS 70 standard, must conform to the SSAE 16 standard which superseded the SAS 70 standard on that date.]*

Furthermore, the selected Proposer shall remain “SSAE 16 Compliant” throughout the term of the Agreement. A copy of the final report, and all subsequent updates, shall be submitted to the designated Authority contact throughout the term of this Agreement within four (4) months of each report’s expiration date, confirming continued compliance.

3. Company certifications and/or description of relationships with relevant software products; industry leadership, etc.

4. Proposed Team/Proposed Staffing - provide a one (1) page organization chart that identifies key individuals, their firm and reporting relationships. Following this chart

shall be a summary sheet indicating the qualifications and experience of technical, managerial and supervisory personnel (and their respective firm(s)) to be assigned to the project. For each individual, indicate his/her proposed role on this engagement, whether on-site or remote and whether full or part time. (If part time, indicate number of hours/week). For each individual identified include the following:

- a. their length of service with the firm;
- b. their anticipated function;
- c. any relevant certifications if any; and
- d. a summary of the relevant experience (Resumes) of the individuals.

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

F. Submit a Consultant Identity Check/Background Screening Plan. This Plan shall be applicable to all years of the Agreement and shall include, but not be limited to, the following:

1. Describe how the Plan will ensure that only employees that were successfully prescreened and properly credentialed perform the services;
2. For new hires, indicate how many years prior to the identity check/background screening the investigation shall consider (as a minimum) ten (10) years of employment history and verification of what the new hire documented they have done in the last ten (10) years preceding the date of the investigation;
3. resources utilized to perform this research; and
4. the frequency at which it is performed on current employees.

G. Business Risk - Identify the five biggest risks as it relates to contract performance, internally and externally, and your proposed plan to mitigate such risks.

H. Sealed Cost Proposal

Submit a Sealed Cost Proposal indicating the compensation expected. The Cost Proposal should be complete and address all services referenced herein. The Cost Proposal shall be submitted on Attachment D – Cost Proposal Form. **Submit all Cost Proposal related material in a separately marked sealed envelope entitled "Cost Proposal".** The Cost Proposal and associated material and documentation (including the CDs of the Cost Proposal) shall appear only in the separately marked sealed envelope and not anywhere else in the Proposal.

I. Subconsultants

A complete list of your proposed subconsultant(s), including their M/WBE status, as applicable.

J. M/WBE Participation

Your attention is directed to paragraph 16 of the Authority's Standard Agreement in which the Director has stated the goals for Minority/Women Business Enterprise participation in this project. Submit details on how you intend to meet these goals.

K. Affiliates

Include a complete list of your firm's affiliates. Affiliates shall be as defined in paragraph 26 of the attached Standard Agreement.

L. Conflict of Interest

If the Proposer or any employee, agent or subconsultants of the Proposer may have, 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 Authority reserves the right to require a mitigation plan, disqualify the Proposer if, in its sole discretion, any interest disclosed from any source could create, or give the appearance of, a conflict of interest. The Authority's determination regarding any question(s) of conflict of interest shall be final.

M. Agreement Exceptions

The Proposer is expected to agree with the Standard Agreement and its terms and conditions. Make no changes to the Standard Agreement, and do not restate any of its provisions in your Proposal or supporting material. *However, if the Proposer has any specific exceptions, such exceptions should be set forth in a letter included with its response to this RFP.* The Authority is under no obligation to entertain or accept any such specific exceptions. Failure to raise issues at the time of Proposal submission shall preclude the raising of such issues at a later date.

IV. ORAL PRESENTATIONS

After review of all Proposal submissions, an oral presentation to the selection committee and others, as appropriate, may be requested. Firms selected to make presentations may be given only short advance notice. Your staff providing the presentation shall be led by the proposed Project Manager, who may be supported by no more than four (4) other senior staff members who are proposed to work on this project. Notification of presentation scheduling will be made via e-mail. **Provide the name and e-mail address of the person who should be contacted for presentation scheduling**, if applicable, as well as an alternate in the event that person is unavailable.

V. SELECTION PROCESS

The Authority will review all Proposals to determine if they adhere to the format required, if they contain all required submissions, and if the Proposal satisfies the prerequisites stated herein.

Proposals shall be reviewed employing a two (2) phased review process, as follows:

Phase 1 shall consist of a detailed review and evaluation according to the following criteria, listed in order of importance:

<p>Technical Solution</p>	<ul style="list-style-type: none"> • The methods, practices, tools and techniques to be employed by the Proposer to satisfy or exceed the requirements described in “Attachment A, Scope of Work (SOW)” and all related attachments, appendices and requirements. • The technical approach to be used to assure consistently high quality service, and provide for flexibility and controlled migrations in the face of rapidly changing technologies.
<p>Firm and Management Team Experience</p>	<ul style="list-style-type: none"> • Staff experience and demonstrated knowledge of the technologies, and configuration needed to design, implement and support a FMS inclusive of the technical resources required for ongoing FMS source data entry. • Firm experience, including <ul style="list-style-type: none"> - demonstrated ability to manage the functional and technical components of the application in an environment comparable to the Authority’s; - demonstrated experience performing Aviation and GIS projects similar to the requirements in this scope of work; - the Proposer’s financial stability; - demonstrated ability, through relationships with software vendors, the Aviation industry, and others to provide strategic advisory services, introduce alternative technology solutions and to assess the value and applicability of upgrades and new functionality. <p>The Proposer’s M/WBE plan, background screen plan, and business risk will also be evaluated.</p>

Phase 2

Upon completion of Phase 1, Cost Proposals of those Proposers that the Authority, in its sole determination, has identified as best qualified to provide effective solutions to the requirements stated herein shall be opened and evaluated. Cost-based scores will be added to the technical scores from Phase 1 for an overall comprehensive score.

VI. ADDITIONAL INFORMATION

- A. “Certification of No Investigation (Criminal Or Civil Anti-Trust), Indictment, Conviction, Debarment, Suspension, Disqualification and Disclosure Of Other Information” And “Non-Collusive Proposing And Code Of Ethics Certification; Certification Of No Solicitation Based On Commission, Percentage, Brokerage, Contingent Or Other Fees.”

If your firm is selected for performance of the subject services, the agreement you will be asked to sign will include clauses entitled “Certification of No Investigation (Criminal Or

Civil Anti-Trust), Indictment, Conviction, Debarment, Suspension, Disqualification and Disclosure Of Other Information” and “Non-Collusive Proposing, And Code Of Ethics Certification; Certification Of No Solicitation Based On Commission, Percentage, Brokerage, Contingent Or Other Fees.” By submitting a proposal, the Consultant shall be deemed to have made the certifications contained therein unless said Consultant submits a statement with its proposal explaining why any such certification(s) cannot be made. Such a submission shall be submitted in a separate envelope along with your proposal, clearly marked “CERTIFICATION STATEMENT.”

B. State of New York, State of New Jersey Requirements

It is the Authority’s policy that its consultants, contractors and vendors comply with the legal requirements of the States of New York and New Jersey. Your attention is therefore called to New York State's requirements that certain contractors, affiliates, subcontractors and subcontractors' affiliates register with the New York State Department of Taxation and Finance for the purpose of collection and remittance of sales and use taxes. Similarly, New Jersey State requires business organizations to obtain appropriate Business Registration Certificates from the Division of Revenue of the State's Department of Treasury.

Your attention is directed to Paragraph 16 of the Authority’s Standard Agreement in which the Port Authority’s goals for Minority Business Enterprise participation are set forth. A listing of certified MBE/WBE firms is available at: <http://www.panynj.gov/business-opportunities/sd-mini-profile.html>.

Proposers are advised that additional vendor information, including, but not limited to forms, documents and other related information may be found on the Authority website at www.panynj.gov.

Should you have any questions, please e-mail them to BOTH Ms. Isabel Amado, at iamado@panynj.gov and Ms. Stacey Willner at swillner@panynj.gov.

All such emails must have “**RFP #29362**” in the subject line. All questions must be received at least five (5) working days prior to the Proposal due date. Neither Ms. Amado, Ms. Willner nor any other employee of the Authority is authorized to interpret the provisions of this RFP or accompanying documents or give additional information as to their requirements. If interpretation or additional information is required, it will be communicated by written addendum issued by the undersigned, and such writing shall form a part of this RFP, or the accompanying documents, as appropriate. Addenda to the RFP, if any, will be posted at <http://www.panynj.gov/business-opportunities/bid-proposal-advertisements.html?tabnum=6>.

You should therefore monitor the advertisement on said website, as appropriate, to ensure you are aware of changes, if any.

Proposal preparation and presentation costs are not reimbursable by the Authority.

No rights accrue to any Proposer except under a duly authorized agreement for performance of the specified services.

The Authority reserves the unqualified right, in its sole and absolute discretion, to reject all Proposals, to undertake discussions and modifications with one or more Consultants and to

proceed with that Proposal or modified Proposal, if any, which in its judgment will, under all the circumstances, best serve the public interest.

Attachments:

The Authority's Standard Agreement will include, but not be limited to, the following attachments, as required:

Contract Specific Terms and Conditions

Appendix 1 – Port Authority Facilities

Attachment A – Scope of Work

Appendix A1 – FMS System Abstract

Appendix A2 - Current System Metrics

Attachment B – Agreement on Terms of Discussion

Attachment C – Company Profile

Attachment D – Cost Proposal

Attachment E – Technology Standards and Guidelines

Attachment F - Technical requirements for computer hardware software and networking equipment

Attachment G – Audit Controls Checklists

ATTACHMENT A

PERFORMANCE OF EXPERT PROFESSIONAL SERVICES DEVELOPMENT AND MAINTENANCE OF AN AVIATION FACILITIES MAPPING SYSTEM

I. BACKGROUND

The Port Authority of New York and New Jersey (the “Authority”) is a municipal corporate instrumentality and political subdivision 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 seventeen counties, in the two States. The Authority manages and/or operates all of the region’s major commercial airports (Newark Liberty International (EWR), John F. Kennedy International (JFK), Teterboro (TEB), LaGuardia (LGA) and Stewart International Airports (SWF)); marine terminals in both New Jersey and New York (Port Newark and Elizabeth, 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.”

II. SCOPE OF WORK

The services of the Consultant shall generally consist of developing a Facilities Mapping System (“FMS”) (computer application) that adheres to FAA Part 139 Inspection Compliance Initiatives, including all of its tasks related to the migration of the current Utilities Management System (“UMS”). The Consultant’s services shall include, but are not limited to: application design and development; configuration; query development; user training; data conversion and migration, and development and execution of appropriate unit/component, integration and user acceptance test plans; data entry and field construction coordination support services; maintaining the existing legacy UMS prior to migration and conversion to the new FMS; and operating, maintaining, and updating the FMS.

The UMS shall be considered the system of record as of the contract commencement. The FMS shall be considered complete and the system of record only with the Authority’s acceptance of completed full system acceptance plans, which shall not be unreasonably withheld.

- a. Performance of the Consultant’s FMS support services shall begin upon the Authority’s acceptance of the FMS as detailed below [TASK A & B].
- b. Performance of the Consultant’s data gathering and data entry into the existing UMS, and all related field construction coordination, services shall begin at Contract commencement. [Task C].

III. DESCRIPTION OF CONSULTANT'S TASKS

The Consultant's tasks shall include, but are not limited to, the following:

TASK A. DESIGN CRITERIA SUMMARY

Prepare and submit a written draft Design Criteria Summary ("DCS") identifying all criteria to be used in developing the new FMS. Incorporate Authority comments as required, and resubmit the DCS as Final.

The FMS as designed by the Consultant, and as approved by the Authority, shall comply with the following requirements:

1. While the scope of the current UMS is limited to Aviation facilities and associated FAA requirements, the replacement FMS as contemplated under this Contract shall be scalable and flexible enough to include and incorporate FMS data from other non-aviation Authority facilities.
2. The FMS is a corporate system that will exist in a corporate data center with shared resources, as referenced in:
 - a. Appendix A (Overall System Abstract) details the appropriate roles and demarcation points.
 - b. Appendix B (Current System Metrics) details the existing UMS constructs.
3. Efficiently allow for the rapid update of existing plans and associated data
4. Eliminate redundant data entry
5. Improve utility location accuracy
6. Increase efficiency in data gathering and analysis
7. Standardize mapping presentation for universal interpretation
8. Automate applications for data manipulation
9. Increase effectiveness to emergency response
10. Distribute standardized, current, data to end users for analysis and decision-making
11. Track on-going and proposed projects
12. Be built using off-the-shelf software that can integrate with both ESRI and Autodesk products as defined more fully elsewhere in this document. Off-the-shelf software components shall be used wherever possible. All system components shall be easily configurable, nonproprietary, and shall comply with all applicable Port Authority standards. The solution shall provide a consistent user interface and interface with external systems through an open systems architecture. The system shall be accessed through a secure interface, accessible only by authorized personnel.
13. Maintain data as required to comply with the Federal Aviation Administration (FAA) Office of Airports, Airport Surveying - GIS Program requirements, and the following FAA initiatives (FAA part 139 inspection compliance initiatives) as same may be amended, from time to time:

- a. Advisory Circular 150/5300-16A - “General Guidance and Specifications for Aeronautical Surveys: Establishment of Geodetic Control and Submission to the National Geodetic Survey”
 - b. Advisory Circular 150/5300-17B - “General Guidance and Specifications for Aeronautical Survey Airport Imagery Acquisition and Submission to the National Geodetic Survey”
 - c. Advisory Circular 150/5300-18B - “General Guidance and Specifications for Submission of Aeronautical Surveys to NGS: Field Data Collection and Geographic Information System (GIS) Standards”
 - d. Advisory Circular 150/5300-13A - “Airport Design”
14. Provide the Authority with a web based map viewer to view and query the utility and FAA data. The map viewer shall provide the ability to:
- a. View a legend of the data layers
 - b. Use Standard pan and zoom functionality
 - c. Print the current map extent with user specified layout features (title of map, date, legend etc.)
 - d. Copy the map and save the image as either a pdf or standard image format to allow the user to include the image in a document or e-mail message
 - e. Select map features options that include select by point, polygon, distance, etc.
 - f. Identify features with Authority defined fields
 - g. Access documents/files hyperlinked to a feature
 - h. Query features that meet a set of user-defined expressions
 - i. Trace functionality that will allow the user to perform upstream/downstream and isolation traces (i.e. allowing the user to identify valves to shut off to isolate a broken pipe)
 - j. Allow users to request features in the map viewer (i.e. if a user wants the features of a specific data layer(s) the user would select the area on the map viewer)
 - k. Create and update spatial data from a variety of digital and non-digital sources; maintain and update existing spatial data; convert both non-GIS or non-digital data; provide Data modeling and spatial database design services; create and maintain Metadata; and provide for transformation and publishing (WFS, WMS)
15. Construct with the required capabilities for integration with commercial maintenance management system(s) and three dimensional (3D) project design initiatives.
- Note – While the FMS shall be constructed for ease of integration to the initiatives above, the specific integration is NOT part of the FMS effort. Specific integration requirements shall be transmitted as standalone “as-needed” task order(s), when required.
16. Support mobile and handheld applications that allow approved users to access, (view and or update) information remotely, from the field.

17. Enable the Authority to create, edit, and maintain current and accurate records of the location of surface and subsurface utilities, as well as, to store and readily retrieve information related to the maintenance and operation of the utilities and other relevant components.
18. Provide for secured, controlled, and auditable access to current, accurate utility locations, and provide for a single, integrated and updated store of information about utilities.
 - a. The FMS shall include subsurface and above ground utilities as per Federal Aviation Regulation (FAR) part 139 data. This would include fuel farms, aircraft rescue and fire fighting (“ARFF”) – more information can be found at: http://www.faa.gov/airports/airport_safety/part139_cert/.
 - b. The data must align to/overlay with, Aviation’s Electronic Airport Layout Plan (eALP) data layer (which contains the buildings and runways).
19. Provide for an integrated reporting and querying toolset for authorized users. Reports are defined as both standard and ad hoc and shall be defined as part of the design stage. Reports can be business / data focused, or management focused. These reports / queries shall be maintained and new reports created as part of normal support duties. Reports / queries can be one shot – in response to a particular request, or on-going. On-going reports shall be structured and available for subsequent execution.
20. Provide for user access commensurate with function specific security requirements.
21. Provide for end user training to Authority defined staff. The Consultant shall provide all training development inclusive of the preparation and printing of manuals, quick aids, or screen shots and the required test data and/or training simulations that are required to effectively communicate system usage. The Consultant shall use current best practices in Adult Education to prepare and deliver this training. The Consultant shall maintain and update training materials, as changes are made to the system. (It shall be noted that the Authority will handle student identification, classroom registration, and scheduling).
22. Conversion of all required data from the legacy system to the new FMS.

It shall be noted that this is not simply the loading of data from current Oracle version; but requires the conversion from the original data attribute schema to the proposed system, which inherently has differences (fields, etc.). **TASK B. FMS IMPLEMENTATION**

This task includes all services as required to plan, develop implement and migrate to production the FMS as it was fully designed and approved by the Authority in task A above. This task also includes the actual conversion, validation and integration of all existing UMS data. . This task shall generally include:

1. All required application design, development, and scripting;
2. All required product configuration including the creation of user roles and security profiles as required;
3. All Required query, list and report development;
4. All initial user training – objective to train the current user base in effective usage of the new FMS functions and features. Training shall be instructor led and include, at a minimum, a handout; instructor demonstrations; screen shots and include test data

examples. A component of the training course shall include a delta wherein users are cross walked from the old to the new. Precise length and composition of training course shall be determined during the TASK A;

5. All data conversion, validation and migration efforts; (inclusive of scripts and reconciliation reports highlighting quality and effectiveness of data conversion efforts). Given the large volume of data currently existing and the fact that UMS is a 24 x 7 system, it is assumed that the data conversion methodology shall be done in a manner consistent with 24 x 7 operations.
6. Development and execution (upon Authority approval) of appropriate unit/component, integration and user acceptance test plans inclusive of all required test data and test cases. It shall be noted that this task includes all required reprogramming or related efforts to correct errors found during testing. Agreement as to the appropriate number of test cycles and any required parallel processing cycles and reconciliation efforts will be part of Task A efforts.
7. Development and execution of required 'go live' planning efforts including; but not limited to – timelines for data & system cutover; developing timelines and agreement for user downtime during cutover; agreement as to data entry and related system freezes, back out plans; reconciliation plans; success factor determination etc.
8. Ongoing FMS Core Support – While Task A and B are generally considered one time efforts; commencing upon Contract start and ending when the FMS is accepted as the system of record, it shall be noted that one component of Task B shall be considered to be ongoing. The continual 'care and feeding' core support tasks to ensure the FMS is up and running; patched and operates as per the stipulated service levels and requirements detailed herein inclusive of responding to end user questions. For ease of documentation and task close out, with the Authority's prior approval, the Consultant may consider Core FMS support to be either under Task C ongoing efforts or as a work order task falling under Task D detailed below. Regardless of placement however, it shall be noted that the ongoing support and maintenance is considered a mandatory task that forms the basis of this agreement.

TASK C. DATA ENTRY/DATA MAINTENANCE, AND FIELD CONSTRUCTION COORDINATION SERVICES

The Consultant shall provide the following Solution Support, Data Entry, and Field Construction Coordination Services:

It shall be noted that Data entry/data maintenance and, field construction and coordination services shall be performed in the existing UMS as of Contract commencement with input efforts switched to the FMS upon FMS acceptance by the Authority. (Details specific to the conversion process shall be addressed in Task B, above.)

1. The services of a supervisor, and data maintenance technician as required to perform Data Entry/Data Maintenance services which includes, but are not limited to:
 - a. Collecting and disseminating utility related data.
 - b. Submitting the appropriate data conversion prioritization to be employed, to the Authority for review and approval. Modifying the prioritization as required by the Authority.

- c. Preparing memoranda, technical correspondence, and activity reports.
 - d. Performing data scrubbing.
 - e. Performing related work, as required.
 - f. Assisting the Authority in the deployment of field personnel responsible for utility inventories to ensure timely tracking and updating of utility locations.
 - g. Inputting data in the FMS.
 - h. Performing data scrubbing activities.
 - i. Preparing and revising working drawings, maps, and diagrams.
 - j. Performing related work as required.
2. Field/Construction Coordination
- a. Review as-built drawings.
 - b. Review Electrical, Mechanical, Plumbing, Fire Alarm, Communications, and Civil work design drawings.
 - c. Coordinate all trades work.
 - d. Coordinate obtaining Electrical Permits.
 - e. Coordinate testing and tie-ins of public and tenant utilities systems.
 - f. Coordinate work between the Authority, Contractors, and Aviation Facilities Tenants.
 - g. Perform field assessments for operational correctness.
 - h. Monitor construction activity for contract and operational compliance.
3. Performance of data entry services to keep FMS up to date, and field construction coordination services, as required, shall be as directed by the Authority based on construction and maintenance activities at the Airports.
4. On-going system support (for both proprietary and third party components) includes on-going system administration of the application and front end products inclusive of system updates, fixes and all similar maintenance and support activities to assure the Solution remains in a current updated state with respect to version and releases, temporary fixes and on-going technical support; maintenance, problem solving, report and query support and maintenance; developing and implementing Quality Assurance/Quality Control (“QA/QC”) procedures, and for providing system related training on an “as-needed” basis.

TASK D - AS-NEEDED TASK ORDER ASSIGNMENTS

The Consultant shall perform work on simultaneous task order assignments (e.g. implementing new functionality), as requested by the Authority, on an “as-needed” basis.

Each ‘as needed’ task order shall be managed via written task order and shall include all information necessary for effective management thereof, including at a minimum; task description; timeline/timeframe for implementation; estimate as to number of hours and skill set required; cost; special notes as required and a place for authorized signatures. Invoicing for task orders (as well as all Tasks) shall be detailed enough and provide sufficient information that the Authority can easily cross reference invoice to projects.

Procurement of Hardware/Software - The Authority may purchase hardware and software for this project. The Consultant shall perform those services required to install the hardware and/or software as further detailed in a task order.

IV. CONDITIONS AND PRECAUTIONS

A. General Requirements

1. The Consultant shall work in harmony with the Authority’s third party Contractors and service providers in areas such as, but not limited to, problem diagnosis and resolution; application enhancements, coordination activities related to implementation of new releases, or other associated maintenance fixes or releases.
2. All Consultant staff must be capable of receiving Airside Operations Area (“AOA”) identification, which includes fingerprinting and an FBI background check.
3. The Consultant shall provide all safety equipment (e.g. reflective vests) necessary to conduct fieldwork. The Consultant shall immediately inform the Authority of any unsafe condition discovered at any time during the course of this work.
4. Hours of Work, and Location of Operation
 - a. Except as otherwise required during the term of this Agreement, on-site services shall be performed Monday through Friday during normal business hours.
 - b. In any case, no work shall be performed at the site on a Holiday unless otherwise required by the Director.
 - c. Given the operational nature of this work, off-hour support is not generally expected, but may be required and shall be compensated at the same rates as standard hours, unless otherwise authorized in advance by the Director in writing.

The Consultant’s services shall include 24 x 7: “on call” operational support; preventative maintenance, remedial maintenance; telephone support; application of appropriate bug fixes; ensuring the UMS/FMS continues to run effectively after operating system, data base or other third party patches are applied. Also included are capacity monitoring, performance monitoring, troubleshooting, change management testing, and associated administration.

The Authority shall give as much reasonable advance notice for performance by the Consultant of off-hour services, however, the Consultant’s services include maintaining an operational system in use 24 hours a day, 7 days a week, in

support of airport facilities that are operational 24 x 7. Appropriate response and support are required.

- d. While subject to change at the direction of the Authority, the anticipated work locations shall be office locations at the Authority's airports. All work is anticipated to be performed on-site unless otherwise agreed by the Authority. All individuals working on this effort shall be subject to security requirements, as stipulated herein (see Standard Agreement, Section 17. Notification of Security Requirements").

B. SSAE 16 CERTIFICATION

The Consultant shall remain "SSAE 16 Compliant" throughout the term of the Agreement. A copy of the final report, and all subsequent updates, shall be submitted to the designated Authority contact throughout the term of this Agreement within four (4) months of each report's expiration date, confirming compliance.

C. Work Areas

1. The Consultant shall limit its fieldwork to the areas necessary for the performance of such services and shall not interfere with the operation of the Airport. No fieldwork shall be done without first obtaining specific approval from the Authority.
2. During all periods of time when not performing operations at the work site, the Consultant shall store all equipment in areas designated by the Authority, and shall provide all security required for such equipment.
3. The Consultant shall not permit any objects or pieces of equipment to lie unattended on sidewalks, roadways or structures at any time.
4. Vehicular traffic on all airport roadways shall always have priority over any, and all of the Consultant's operations.

D. Service Levels

The Consultant's obligation for the performance and completion of the work within the time or times provided for in this Agreement are the essence of the Agreement. In the event the Consultant fails to satisfactorily perform all or any part of the work required hereunder in accordance with the requirements set forth, and inasmuch as the damage(s) and loss to the Authority for such failure (to perform) includes items of loss whose amount will be incapable, or very difficult, to accurately estimate, the damages to the Authority shall be liquidated in the following amount(s):

1. Regular scheduled maintenance approved by the Authority is excluded from service level calculations.
2. Emergency maintenance, however, is unscheduled maintenance, as it affects service availability, and is measured as part of service availability unless otherwise agreed to by the Authority.
3. Total dollars of liquidated damage(s) for non-performance for the month shall not exceed the Consultant's compensation for that month.

Service	Service Level	Associated Liquidated Damage for Non- Performance
FMS System	<ul style="list-style-type: none"> • Application Software, Database and any other tools or products shall always be no more than two versions below the current general release version available • All support requests or user queries shall be responded to within 48 hours of notification. All responses shall be inclusive of projected deadlines. All deadlines once approved must be met. • Application shall maintain 99.9% online availability. 	\$500 per each instance of non-compliance for each Service Level. As defined here in an instance can be either more than 2 versions below current release; response is over the 48 hour timeframe or less than 99.9% online availability.
Construction Coordination Data Entry & Maintenance	Throughout the course of the agreement all construction coordination & data entry & maintenance tasks shall be given target dates assigned and mutually agreed between the Consultant and the Authority. Failure of Consultant to meet the accepted target dates; especially without prior discussion with the Authority; can result in a determination of non-coordination. Repeated failure of Consultant to meet deadlines may be considered a material breach of the Contract.	\$1,000 per instance of non-coordination
General	<ol style="list-style-type: none"> 1) All billing auditing must be accurate and include all detail and backup material. 2) All tasks must have target dates and backup information presented that effectively demonstrates satisfactory work completion as indicated by Authority signature. 	\$500 per instance of non-compliance

As Need Task Order Assignments	Unless otherwise agreed in advance, all task order requests shall be responded to within one (1) calendar week from receipt of complete information from the Authority. Response shall be inclusive of details and backup material as well as datelines. Unless otherwise agreed to in advance, and allowing for a 10% grace period, target completion dates shall not be missed.	\$500 per instance of non-compliance
Adherence to Audit Controls Checklists and Technology Standard and Guidelines	Satisfy 100% of all applicable sections and requirements	\$500 per each material instance of failure to meet checklists and standards

Computation of online availability, problem resolution, etc., is limited to, and refers specifically to, services covered by the Agreement that are the Consultant's responsibility. For example, time spent by other Consultants to repair hardware would not be included in the calculation of the Consultant's service level performance.

E. General Requirements

1. The FMS shall -
 - a. provide for complete logging of system activity;
 - b. provide redundancy – the servers shall be configured to provide for continuous operation of the system;
 - c. provide for fault tolerance – so the system will continue to run upon detection of any type of failure;
 - d. be in a 'state of common usage' or industry standard, and shall be an open architecture;
 - e. be capable of being shutdown in an orderly fashion, and in a fashion that causes no anomalies in other system components; and
 - f. be installed sequentially in client environments (development, test, staging, production and disaster recovery).
2. The Consultant shall -
 - a. establish and maintain an organizational and operational structure appropriate to the services to be performed under this Agreement;
 - b. furnish sufficient trained staff to provide the services required, with all such personnel subject to review and approval by the Authority; (the Authority maintains the right of first refusal – to approve or disapprove, at the Authority's

sole discretion, with or without cause, any employee who directly services the Authority's account as well as the right of Replacement.)

- c. appoint a member(s) of its organization to oversee the management of the services;
 - d. employ a proven project management methodology that addresses the scope of services described herein;
 - e. schedule and conduct regular status meetings with the Authority at an Authority selected site. Details of frequency, nature and content of such meetings shall be developed during project start up;
 - f. maintain a list of Consultant employees authorized for physical security as well as those employees authorized by the Authority to access the system;
 - g. Assist with Disaster Recovery and Business Resumption Planning, and direct participation in periodic testing efforts and exercises.
 - h. Work with the Authority to prepare all required management processes including, but not limited to: workload tracking, escalation procedures, QA processes, problem and incident tracking, etc.
 - i. Establish and document a system library inclusive of system documentation and technical descriptions of the solution, hardware, software, and communications architecture. The system documentation library shall follow best industry practices and include function description, graphic system architecture plans, describe failure handling and recovery, Operating instructions; Start up and Shut down procedures.
3. The Authority maintains the right to review and approve all proposed approaches and work products.

* * *

Appendix A1 (to Attachment A) – Overall System Abstract

The Authority is seeking proposals to create and maintain a comprehensive Facility Utility Subsurface and Surface Asset Management System to be named Facilities Mapping System (“FMS”) at various Authority locations, with initial focus on LGA, JFK and SWF airports and the associated FAA requirements.

The selected solution is anticipated to be robust, incorporating as much out of the box functionality inherent in existing geospatial and CAD/engineering software, with easy to use intuitive views of utility subsurface and surface asset data, flexibility to respond to new technologies, and end user requirements for viewing and accessing the core data elements. (By way of example, it is assumed that the proposed solution will capture elevation as an attribute in the database to allow future use of 3D related product features). The proposed solution shall highlight the Consultant’s expertise in working with the proposed tools to their fullest, and shall showcase how services will be built to be sharable. In addition, the selected Consultant shall have familiarity with applicable FAA requirements, as detailed more fully in Attachment A, such that the proposed solution, from the data element level through viewer level, shall be created and maintained consistent with FAA requirements.

The Consultant shall recommend a proposed solution inclusive of hardware infrastructure and software tools based on information provided by the Authority in this solicitation document and consistent with the Authority’s Technology Standards and Guidelines, Technical Requirements for Computer Hardware, Software and Networking Equipment, and Audit Control Checklists included herewith (see Attachments E, F, and G).

To meet stated requirements, the proposed solution shall incorporate the latest versions of ESRI and Autodesk products using either Oracle Spatial or the equivalent SQL product as the underlying database. However, Proposals using alternative toolsets consistent with the above-mentioned Authority standards shall be considered and evaluated consistent with the criteria disclosed elsewhere in the solicitation document.

At the Authority’s discretion, the Authority will procure the required hardware & software for the proposed solution using existing Authority processes. The Consultant will not generally be expected to procure or install any Authority standard hardware or software unless otherwise explicitly defined. Furthermore, the Authority will be responsible for any Authority standard hardware and software required for the system that includes operating systems, database systems (Oracle/SQL) and Authority standard GIS software (ESRI/Autodesk products). The Authority will install, configure to Agency standards, maintain and upgrade, for the duration of the Agreement, these Authority standard hardware and software products on both the server and PC level inclusive of the entire system landscape – production, test/QA/training as detailed and agreed to consistent with the Consultant’s stated approach. Database support provided by the Authority includes the back-end database (Oracle, SQL) and the core ESRI infrastructure. The Consultant shall be responsible for maintaining the data within the databases, as directed by the Authority.

Upon turnover of the installed equipment, the Consultant shall be responsible for scripting, configuring the software and performing all tasks required to produce and maintain a functioning FMS on the provided hardware and with the provided toolsets and approach identified in their proposal. Utilizing structured methodologies and best practices consistent with the Authority’s guidelines and standards, the Consultant shall be responsible for all application level support and upgrades, testing, Disaster Recovery and Business Resumption planning, documentation, and

shall work with the Authority and /or its third party providers to ensure a secure, patched and supported environment, all end-user support as well as required training and coaching.

The selected Consultant shall be responsible for supporting the existing legacy Utility Management System's (UMS) environment and for the phased and validated conversion and migration of all data in the existing system to the proposed system structure, constructs, tools and functionality. Furthermore, consistent with service levels and parameters defined elsewhere in this document, the selected Consultant shall be responsible for the ongoing validation & data entry of FMS "updates", and as presented to the Consultant from as built drawings, surveys, or other communications with Authority or third parties as it relates to the FMS. These 'updates' reflect changes in the actual physical environment that need to be recorded in FMS to ensure accurate and up to date data is presented. This ongoing data entry is a critical maintenance task.

During FMS development, the existing UMS shall be considered the system of record and all required 'production' services shall be performed on it. Upon acceptance by the Authority, the FMS shall become the system of record and the basis for the remainder of services provided for herein.

* * *

Appendix A2 (to Attachment A) - Current System Metrics

The Authority operates and maintains a Utility Management System (“UMS”) that tracks, maintains and monitors subsurface utility information.

The Authority’s Aviation Department (“Aviation”) is the primary beneficiary, principal user, and owner of the data housed in the UMS. JFK and LGA are the primary facilities that have data tracked in UMS. Others throughout the Authority also use UMS. The UMS is used to locate underground systems and to appropriately plan construction and maintenance activities so that service disruptions are avoided, displaying locations and types of major utilities including: chilled water, thermal distribution, communications, electric, fuel, natural gas, sanitary, storm, and water.

The current UMS is a custom-designed system that integrates the following software applications and databases:

1. Visual Basic Scripts
2. Autodesk Map 2004
3. Autodesk Land Desktop 2004
4. Oracle 9i Enterprise Edition
5. MapGuide Control 6.5 ActiveX plug-in
6. Crystal Reports
7. IIS
8. AutoCad 3D Civil 2010

Customized Visual Basic scripts have been implemented to enable users to insert features into an AutoCAD drawing, housing all relevant data information in the Oracle database. MapGuide is then used to provide access to these drawings and their elements via web pages through the use of IIS over the Authority’s Wide Area Network (“PAWANET”). In addition, reports using Crystal Reports are prepared as requested and associated Queries are used to identify database or application/front end issues.

There are three types of UMS users:

1. **Data Maintainers** – those responsible for adding, editing, and ensuring the quality of stored data.
2. **Data Viewers** – the ultimate end-users who browse, query, and retrieve data.
3. **System Administrator** – approves access to system and handles data requests.

Two separate software tools were developed to serve the data maintainers and viewers:

1. **The Data Maintenance Tool (DMT)** - a set of data construction tools to manage, modify, and select AutoCAD Map drawings, and associated attributes, by trained CAD personnel with knowledge of various utilities; and
2. **The Data Viewing Tool** - a read-only web-based data viewing software residing on a Microsoft application server and accessed by users over the Authority’s intranet.

The UMS is presently residing on Authority servers off-site from JFK and LGA. The workstations consist of IBM desktops. The system is available and operational 24 hours a day, 7 days a week.

A. Current UMS System Metrics

Note – All metrics are approximate and accurate as of year-end 2012.

- 1) 130 System Users
- 2) Database B Size -
JFK 7 GB; LGA 4 GB
- 3) Points -
JFK 96,000 Points, 55,000 Lines, 224,000 Survey Points
LGA 14,000 Points, 14,000 Lines, 26,000 Survey Points
- 4) Images –
JFK 16,000 images; LGA 1,000 images
- 5) Basic miles of utilities -
JFK 1,100 miles; LGA 300 miles
- 6) Changes per year lines (define line) average 10%
- 7) Attributes -
JFK 240,000 pieces of data; 10% a year Changes
LGA 34,360 pieces of data; 10% a year Changes

* * *

ATTACHMENT B

**REQUEST FOR PROPOSALS FOR PERFORMANCE OF
EXPERT PROFESSIONAL SERVICES – DEVELOPMENT AND MAINTENANCE OF
AN AVIATION FACILITIES MAPPING SYSTEM (RFP #29362)**

AGREEMENT ON TERMS OF DISCUSSION

The Port Authority’s receipt or discussion of any information (including information contained in any proposal, vendor qualification, 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. The foregoing applies to any information, whether or not given at the invitation of the Authority.

Notwithstanding the above, and without assuming any legal obligation, the Port Authority will employ reasonable efforts, subject to the provisions of the Port Authority Freedom of Information Code and Procedure adopted by the Port Authority’s Board of Commissioners on March 29, 2012, which may be found on the Port Authority website at: <http://www.panynj.gov/corporate-information/pdf/foi-code.pdf>, not to disclose to any competitor of the undersigned, information submitted which are trade secrets or is maintained for the regulation or supervision of commercial enterprise which, if disclosed, would cause injury to the competitive position of the enterprise, and which information is identified by the Proposer as proprietary, as more fully set forth in the FOI Code, which may be disclosed by the undersigned to the Port Authority as part of or in connection with the submission of a proposal.

(Company)

(Signature)

(Title)

(Date)

ORIGINAL AND PHOTOCOPIES OF THIS PAGE ONLY. DO NOT RETYPE.

ATTACHMENT C
COMPANY PROFILE

**REQUEST FOR PROPOSALS FOR PERFORMANCE OF EXPERT PROFESSIONAL
SERVICES – DEVELOPMENT AND MAINTENANCE OF AN AVIATION
FACILITIES MAPPING SYSTEM (RFP #29362)**

1. Company Name (print or type):

2. Business Address (to receive mail for this RFP):

3. Business Telephone Number: _____

4. Business Fax Number: _____

5. Firm website: _____

6. Federal Employer Identification Number (EIN): _____

7. Date (MM/DD/YYYY) Firm was Established: ____/____/____

8. Name, Address and EIN of Affiliates or Subsidiaries (use a separate sheet if necessary):

9. Officer or Principal of Firm and Title:

10. Name, telephone number, and email address of contact for questions:

11. Is your firm certified by the Authority as a Minority-owned, Woman-owned or Small Business Enterprise (M/W/SBE)? Yes No

If yes, please attach a copy of your **Port Authority** certification as a part of this profile.

If your firm is an M/WBE not currently certified by the Authority, see the Authority's web site – <http://www.panynj.gov/business-opportunities/supplier-diversity.html>, to receive information and apply for certification.

Attachment D – Cost Proposal

REMINDER – Consistent with RFP instructions, this Cost Proposal and all associated material/documentation shall only be provided in a separately sealed and marked envelope, and the cost information shall not be contained anywhere else in the Proposal. Failure to separate and seal Attachment D “Cost Proposal” information within your Proposal may deem your entire submission non-responsive.

This sheet represents the direct compensation to the selected Firm.

It is anticipated that solution offered may require the Authority’s investment in hardware, software etc. separate and apart from the direct compensation to the selected Firm. Evaluation of the relative merits of the anticipated total cost of ownership to the Authority, separate and apart from direct compensation to the selected Firm for the proposed solution, shall be incorporated as part of the Authority’s technical solution evaluation.

I. FMS DEVELOPMENT EFFORTS

This category consists of all costs required to design, implement, configure, build, program, test, and populate the FMS.

I.A ALL FMS IMPLEMENTATION EFFORTS EXCLUDING DATA CONVERSION

Compensation shall be based on hourly billable rates for actual services provided, however, the figures here represent “Not to Exceed” prices for the solution offered.

Firms are required to include as an attachment, clearly labeled Attachment D – Cost Proposal item I.A a breakdown that details the number of resources and costs by task/phase consistent with implementation timelines.

Note – Final total of attachment I.A breakdown SHALL agree with figures provided in Attachment **D** below.

Total Estimated Number of hours (all skill sets) _____

Total not to exceed price using billing rates \$ _____

I.B UMS to FMS DATA CONVERSION EFFORTS

Compensation shall be based on hourly billable rates for actual services provided, however, the figures here represent “Not to Exceed” prices for the solution offered.

Firms are required to include as an attachment, clearly labeled Attachment D – Cost Proposal item I.B a breakdown that details the number of resources and costs by task/phase consistent with implementation timelines.

Note – Final total of attachment IB breakdown SHALL agree with figures provided in Attachment **D** below.

Estimated Number of hours (all skill sets) _____

Total not to exceed price using billing rates: \$ _____

I.C END USER TRAINING (firm fixed price per class)

Number of classes anticipated is listed for evaluation purposes only. Compensation shall be based on the actual number of classes offered and shall be invoiced upon demonstrated class delivery completion.

Price per CLASS – inclusive of development & delivery \$ _____

Number of CLASSES anticipated x 8

END USER TRAINING: \$ _____

Note - Once the FMS is live, on-going training is not anticipated to be significant; therefore, price per class shall remain constant for the duration of the Contract. However it shall be noted that as part of system support efforts, training material shall be kept up to date and inclusive of modifications, upgrades, enhancements etc. so that whenever offered, the class accurately depicts the then current system.

TOTAL (I.A + I.B + I.C): \$ _____

III. ESTIMATED TOTAL (I + II): \$ _____

IV. NET COST WORK (10% Figure in III above): \$ _____

ESTIMATED GRAND TOTAL (III + IV) = \$ _____

V. ASSUMPTIONS

Please list any and all assumptions made in the above calculations.

Attach additional sheets, clearly labeled, as necessary.

<u>ITEM</u>	<u>DISCUSSION</u>

General Position Descriptions

Programmer / Analyst – Experience writing application software, data analysis, data access, data structures, data manipulation, databases, programming, testing and implementation, technical and user documentation, software conversions; environments include but are not limited to mainframe, mid range, personal computers, laptop; Sr. position available to assist and/or lead in the design of program specifications and the implementation of software solutions.

Project Manager - Experience in overseeing medium to large scaled projects comprised of sub-projects and distinct deliverables; typically coordinates and delegates the assignments for the consultant project staff. Focal point of contact regarding project status, meetings, reporting requirements, scope changes/extensions, and financial, administrative, and technical issues and business / administrative concerns.

Specialist - Experience in a particular technical and/or business application, which is beyond the requirements addressed in the Programmer/Analyst discussed above. Examples include but are not limited to: Certified Network Engineer (CNE); Lotus Notes Certified Application Developer; Microsoft Certified Systems Engineer (MCSE); Web Master

Mechanical Utility Coordinator – Demonstrated field experience related to mechanical/civil utilities (i.e. hthw, chw, chrp functions, sanitary, storm, hydrant fueling, water, gas, etc.) related to airports. Thorough understanding of how systems operate, how to construct new and repair existing. Thorough understanding of industry standard practices, and testing and commissioning.

Electrical Utility Coordinator – Demonstrated field experience related to electrical & electronics related to airports (including thorough understanding of how systems operate, how to construct new and repair existing). Thorough understanding of aviation airside lighting/signage and power systems, FAA equipment, buildings, roadways, etc. and their industry standard practices, including testing and commissioning.

Administrative Data Entry - Seasoned Administrator with demonstrated experience utilizing Microsoft Office products. Must have the ability to type and be well spoken and written. Experience with time keeping, billing, auditing, and procurement of equipment.



THE PORT AUTHORITY OF NY & NJ

Standards & Guidelines for Port Authority Technology

Technology Services Department

Version 8.3
August 30, 2011

Introduction	1
1.0 The Port Authority Wide Area Network (PAWANET)	2
1.1 PAWANET Overview	2
1.2 PAWANET Circuit Diagram	3
1.3 Inter-site Services Providers	3
1.4 PAWANET Functions	3
1.5 Features of PAWANET	4
1.6 Supported Protocols	4
1.7 PAWANET Switches and Routers	4
1.8 Approved Servers	5
1.9 Enterprise Addressing Scheme (including IP addressing)	5
1.10 Enterprise Network Monitoring Software	5
2.0 Network Resources	5
2.1 Network Overview	5
2.2 Enterprise Network Architecture	6
2.2.1 Operating System and Software	7
2.2.2 Configuration	7
2.2.3 Network Resources Security	9
2.2.4 Network Access and User Account Security	10
2.2.5 Remote Access System	12
2.2.6 Network Resources Hardware Standards	13
2.3 Network Naming Conventions	14
2.3.1 Server Names	14
2.4 Directory Services and Structure	14
2.4.1 File Storage Guidelines	14
2.5 System Management	15
2.5.1 Technology Services Department and Departmental Business System Manager Responsibilities	15
2.5.2 Change Management	17
2.5.3 Turning Over a New LAN Resource to the System Administrator	18
2.6 System Backup and Recovery	18
2.6.1 Backup Logs	19
2.6.2 Backup Scheduling	19
2.7 Business Resumption Plan	19

2.8	Telecommunications Standards for Enterprise Network Resources	19
2.8.1	Closet and Telecommunications Room Access.....	20
2.8.2	Telecommunications Installation Contractor's Responsibilities	21
2.8.3	Electrical Requirements	21
2.8.4	Telephone Company Interface	21
2.9	Documentation	22
3.0	Virus Scanning & Management.....	23
3.1	Overview.....	23
3.2	Background	23
3.3	Standards	23
3.4	Virus Detection and Response.....	23
3.4.1	Preventing Virus Outbreaks	24
3.5	Virus Protection Stand Alone PCs and Laptops	25
3.6	Acquisition and Installation.....	25
4.0	Electronic Mail.....	26
4.1	E-Mail Overview	26
4.2	Policy on Use of E-Mail: Highlights.....	26
4.3	E-Mail Etiquette.....	27
4.4	E-Mail System Architecture	27
4.4.1	Public Folders in the Exchange Organization	27
4.5	E-Mail Environment: Design Considerations and Infrastructure.....	28
4.6	Remote Access to E-Mail	29
5.0	Intranet.....	30
5.1	Intranet Overview	30
5.2	Direction of eNet Development.....	30
5.3	eNet Software Infrastructure Standards & Guidelines	30
5.3.1	Design Guidelines	31
5.3.2	Accessibility Guidelines.....	34
6.0	Workstation and Workstation Operating System.....	35
6.1	Overview	35
6.2	Workstation Inventory	35
6.3	Workstation Operating System Standard	35
6.4	Workstation Configuration	35
6.4.1	Workstation Naming Conventions	35

6.4.2	Workstation User Accounts	35
6.4.3	Remote Workstation Management	36
6.4.4	Drive Mappings	36
6.4.5	Standard Workstation Hardware Configurations.....	36
6.5	Standard Department Workstation Software	36
6.5.1	Standard Workstation Software.....	36
6.6	Enterprise Software.....	36
6.6.1	PeopleSoft	37
6.6.2	SAP.....	37
6.6.3	Other Business Applications	37
6.7	Workstation Security	37
6.7.1	Physical Security.....	37
6.7.2	Logical Security.....	38
6.8	Customer Support Desk.....	38
6.8.1	Functions	38
6.8.2	Hours of Staffing	39
6.8.3	Escalation Procedures	39
6.9	Administrative Rights Procedure	39
6.10	Computing Resources Policy	40
6.11	Use of Port Authority Owned Computer Equipment at Home	40
6.12	Software Licensing Guidelines	41
7.0	Distributed Systems Environment.....	44
7.1	Overview.....	44
7.2	Microsoft Windows Servers.....	44
7.2.1	<i>Virtual Environment</i>	44
7.2.2	Windows Data Encryption	44
7.3	Unix.....	44
7.3.1	Unix Security.....	45
7.3.2	Backup.....	45
7.4	z/OS.....	45
7.5	Databases.....	45
7.6	Application Security.....	45
7.7	Server Physical Security	45
7.8	Load Balancing – Failover Architecture.....	46

8.0	Voice Network	46
8.1	Voice Network (Telephone) Services	46
8.1.1	Port Authority Telephone Network.....	46
8.1.2	Local Service	47
8.1.3	Long Distance	48
8.1.4	Tie Line Network	48
8.1.5	Voice Mail	49
8.1.6	Telephone Help Desk.....	49
8.1.7	Telephone Moves, Adds and Changes (MAC)	50
8.1.8	Installation and Use of Home Telephone Lines for PA Business	50
8.1.9	Installation of Modem Lines for PA Business.....	50
8.1.10	PA Calling Cards.....	50
8.1.11	Toll Free (800) Services	50
8.1.12	Audio Conference Call Services (Voice).....	51
8.1.13	SL100 Meet-me Conference Call Service (Voice)	52
9.0	Vendor Provided Dedicated Systems.....	53
9.1	Overview	53
9.2	Physical Security Technology Standards	54
9.2.1	Agency Standard for Digital Video Recording and Access Control and Alarm Monitoring.....	54
9.3	Communications Infrastructure Standards.....	55
9.4	Server Infrastructure Standard	55
10.0	Wireless Technologies	57
10.1	Wireless Guidelines	57
10.1.1	Purpose and Scope.....	57
10.1.2	General Policy.....	57
10.1.3	Personal Area Networks - PAN	57
10.1.4	Wireless Local Area Networks - WLANs	57
10.1.5	Portable Electronic Devices (PEDs) – Cell Phones, PDAs, messaging devices, laptops and tablets.	64
10.1.6	Cellular and Wireless Email	65
10.1.7	Synchronization.....	65
10.1.8	Responsibilities of Technology Services Department	65
10.1.9	Responsibilities of Technology Services Voice Networks Group	66

10.1.10	Responsibilities of Wireless and Handheld Device Users.....	66
10.2	Paging Device Policy And Procedures	66
10.2.1	Policy	66
10.2.2	Procedures.....	67
10.3	Cellular And Nextel Phone & Wireless Modem Policy And Procedures ..	67
10.3.1	Policy	67
10.3.2	Procedures.....	68
10.4	Technology Services Personal Digital Assistant (PDA) Policy	70
10.4.1	Introduction	70
10.4.2	Hardware – Hyper Link.....	70
10.4.3	Software.....	70
10.4.4	Support	70
10.4.5	Training.....	71
10.4.6	Acquisition.....	71
10.4.7	Criteria To Qualify For A PDA Device.....	71
10.4.8	Personal Acquisition.....	71
10.4.9	Breakage And Loss.....	71
10.4.10	Data Security Considerations.....	71
10.4.11	Data Backup	72
10.4.12	Personal Digital Assistant (PDA) Policy.....	72
10.5	BlackBerry Device Policy & Procedure.....	72
10.6	BlackBerry Guidelines	73
10.6.1	Introduction	73
10.6.2	Recommendation for Essential Staff and First Responders.....	73
10.6.3	Support	73
10.6.4	Breakage And Loss.....	73
10.6.5	Data Security Considerations	73
10.6.6	Data Backup	73
Appendices	74
	Appendix 2 -- Business Resumption Plan Document Format.....	74
	Appendix 3 -- Communication Rooms/Closets Standards.....	76
	Appendix 4 -- Cabling	77
	Appendix 5 -- Port Authority Unified Wiring Plan.....	77
	Appendix 6 -- Telephone Closet / IDF Termination Blocks	79

Appendix 7 -- Workstation Jacks.....	79
Appendix 8 -- Standard Switches Inside the Department	79
Appendix 9 -- Desktop and Lateral Cable Identification Management	79
Appendix 10 – PA TELEPHONE NETWORK 5/08	81
Appendix 11 -- Fiber Optic Specifications for Network Services - PAWANET	82
Appendix 12 -- Public Telephone Ordering Guidelines.....	83
Appendix 13 -- PAWANET Services Connection Policy	85
PAWANET “Rules of Connections”	87
Appendix 14 -- PAWANET Services Summary	89

Introduction

The purpose of this document is to communicate the standards established by the Technology Services Department and provide managers and technical staff with guidance in managing the Port Authority's (PA) Information Technology (IT) resources in the most effective way. Managers and technical staff should consult this document when making decisions about how to acquire or evolve their computing systems, platforms, networks and applications. Port Authority department managers and staff need to ensure that changes in their department's Information Technology are compatible with the current Enterprise computing and telecommunications infrastructure. This is crucial to connect and exchange information with other Port Authority departments, as well as with individuals and organizations outside the Port Authority. To that end, these guidelines are intended to help departments do the following:

Implement computing and networking solutions that ensure the utmost reliability, availability and security.

Procure hardware and software that advances current and mandated business needs and enables departments to work with other departments/offices more effectively.

Easily and efficiently communicate and exchange information throughout the agency.

Achieve greater systems integration through leveraging and building upon standardized infrastructure and facilitating systems management.

Adherence to these standards ensures that IT investments achieve Enterprise connectivity, interoperability, consistency, and will enhance performance in a cost-effective way.

How to Use This Document

Throughout this document you will find cross-references, also called hyperlinks, to other documents which provide more specific and detailed information. For example, the very latest standard PC desktop and server configurations are listed on a linked page. Because the computer industry is dynamic and change is frequent, this time-sensitive information will be maintained on the PA's Intranet (eNet) so that it can be monitored and easily updated, assuring you of the most current information. This document will also be available on the eNet, so that when viewing it online, you can click on the underlined hyperlink to immediately access that information. If you are reading a paper copy of this document, you will need to access eNet to obtain the cross-referenced information.

The Technology Services Department welcomes your feedback/comments on these standards and guidelines. Please address your e-mail to: jgrant@panynj.gov.

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, CADD, Lease Image, Closed Circuit Television (CCTV) surveillance systems, and in the future, videoconferencing, and more.

PAWANET consist of a Managed Fiber Optic SONET network, provided by Verizon Select Services. This network consists of two dual OC48 SONET Rings that connect key Port Authority facilities, and intersects the Port Authority's two Data Centers. High-speed DS1, DS3, and Resilience Packet Ring (RPR) links are allocated on this network to form PAWANET's Wide Area Network (WAN) topology. Additional high-speed Ethernet Private Lines (EPL) has been deployed to support Key Port Authority's off-ring facilities.

Remote nodes are linked using high-speed dedicated communication lines. Alternate high speed dedicated communications lines and high-speed dial up communication links (ISDN Lines), provide back up paths should the primary links fail.

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 Cisco Systems SMARTnet hardware/software maintenance services, and Cisco's Technical Assistance Center (TAC) to support and maintain the network

Voice	The network provides the hardware capabilities for voice and VoIP transmission.
Videoconferencing	The network switches and transmission lines are capable of handling videoconferencing to support the agency's future needs.
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
- High performance Catalyst 3000, 4000 and 6500 series switches at Port Authority facilities.
- Cisco high performance 2000, 3000, 7200 and 7507 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:	Transmission Control Protocol Internet Protocol (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:

- Cisco's 15454 High-speed SONET multiplexers connecting the Verizon's OC48 Rings to key Port Authority facilities and data centers.
- Cisco High performance 3000, 4000, and 6000 series switches
- 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.
- Cisco 7500 series high-capacity redundant routers
Serve as the -network backbone core router that provides high speed routing functions between Teleport, Port Authority Technical Center, and all PAWANET

connected facilities, as well as, the IBM mainframe. Also provide high-speed connection and routing capabilities to the disaster site for data recovery in case of a catastrophic event.

1.8 *Approved Servers*

Only IBM File & Print and Application servers may be connected to PAWANET. The link to the CTO's memo on server infrastructure standards is shown below.

[Memo on Server Infrastructure Standards](#)

This includes turnkey and distributed systems where File & Print or Application servers are being 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 are 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).

1.10 *Enterprise Network Monitoring Software*

The Port Authority continually monitors its WAN and the availability of its links. To provide for real time monitoring, the following software utilities are used:

- HP Open View Network Management software
- Cisco Works for Switched Internetworks

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 which 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
- LAN Devices
 - Desktop PCs
 - Workstations
 - Laptops
 - Local Printers
 - Scanners
 - Copiers
 - PC Peripherals

The purpose of the following subsections is to:

- Define the policies and standards governing Enterprise and LAN resources throughout the Port Authority.
- Delineate the duties and responsibilities of the Enterprise System Administrators, the Technology Services Department (TSD), and the Departmental System or Application Manager.

See the [Guide to Systems Administration](#) for detailed information on system requirements and procedures.

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 departments to manage their systems, applications and data in a way that best

meets their business needs while maintaining interoperability and safeguarding Port Authority's information assets.

2.2.1 Operating System and Software

All Enterprise file & print services in the Port Authority are based on the Novell Netware operating system. We are currently moving to a Microsoft Windows file & print environment. Microsoft Windows servers and Sun Solaris are supported as application servers when required for functionality.

In addition to the base operating system, all Enterprise servers must include or provide access to the following components:

- Virus Protection
- Network Security
- Remote Monitoring and Management
- Intrusion Detection
- Mainframe Systems Backup
- Uninterrupted Power Supply (If central UPS is not installed at the location)
- Current Service Packs and security patches

To see the current standard, click below.

[PA Server](#)

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 Novell and Windows operating systems. All Novell servers must be configured using the following parameters:

- Minimum Size of DOS Partition: 5GB
- IP Protocol
- Volume Names: SYS, DATA, APPS

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 the Novell NetWare Login Script. The following drive letters are reserved for Novell installations:

Pointer	Volume or Folder
H:	Novell login (first network drive)
M:	Reserved
P:	Public Applications
Q:	Installation and Upgrade Utilities

S:	Departmental shared directories and files
T:	Reserved
U:	Users Private Home Directory
Z:	Novell system files (Search mapping)

- Public (Shared) application software installed on a NetWare file and print Server, or server cluster must reside on a separate volume named "APPS".

Example: P:\APPS

- Each software application installed on the NetWare file and print server, or server cluster, must have its own sub-folder.

Examples: P:\APPS\EXCEL
P\APPS\WORD

- SYS volume must be used for operating system and support software only.
- Shared Data stored on a NetWare file and print Server, or server cluster, shall reside in a volume named Data, and shall be mapped to the "S:\" drive pointer.

Example <Server_name>:\DATA\SHARE on a single server
<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.
- The Projects folder is provided for storage of project related files. All departmental projects will be kept in a sub-folder under the Projects folder and the folder will be named using the same name as the project. User rights will be assigned by a group having the same name as the project folder. Only staff requiring access to the project files should be granted rights to that project folder.
- 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 identify a project as being completed, the project folder will be moved to the "Completed" folder and all rights, except for "Read" and "FileScan" 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 Director, 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 Novell 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 staff in each department are required to approve these requests.
- A user “U” drive will be assigned to each standard Novell 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 except for “Access Control” and “Supervisory”. 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 Services Department 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)

To see the current standard software needed for connecting LAN devices to the Enterprise Network, click below.

[PA Server](#)

2.2.3 Network Resources Security

2.2.3.1 Server Physical Security

All network equipment must be physically secured in a locked room.

2.2.3.2 Server Logical Security

To safeguard the Port Authority's Information Technology (IT) systems and data, TSD has implemented a number of processes and procedures, including the requirement that all users accessing the Port Authority's networks authenticate to the Novell NetWare Directory Service (e-Directory). The e-Directory Service is a database containing descriptions of all network devices including servers, printers, shared drives 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 Novell NetWare 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 Novell authentication grants you access to network resources, such as shared data volumes, software applications and network printers you use in performing your assigned tasks.

TSD, or its contracted vendor, is responsible for providing all Enterprise servers with the following protection of their logical resources:

- Guard against unauthorized access by making sure that servers cannot be booted from a floppy.
- Scan all workstations for viruses daily.
- Scan all laptops for viruses at log-in.
- Scan all incoming data from users, server peripherals, diskette, CD-ROM, tape drives, other servers, and the Internet for viruses
- Perform daily incremental backups 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 Suite software.
- Perform deleted file purges immediately or no later than 6 days after file deletion.

Control all remote access using the Port Authority's Remote Access System.

2.2.4 Network Access and User Account Security

2.2.4.1 Account Creation

User accounts are created and managed in e-Directory for both the Novell and Windows network resources. The Novell Username must be unique. Individual user accounts are established based on a manager's approval and are inactivated and/or removed as appropriate. Documentation for the creation of user accounts and authority for access is maintained by the System Administrator.

The Novell Username is determined by combining the first initial of the user's first name and the complete last name.

Example:	User's Name	Novell Login ID
	Tony Robinson	trobenson

When the Novell Login ID is already in use, see the [Guide to Systems Administration](#) for additional examples of alternative account names to use.

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 Novell File & Print servers. All staff may access their Novell account 24 X 7.

2.2.4.3 Concurrent Logins

Login sessions should 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 should 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 should have passwords conforming to the following standards:

- Minimum length is six (6) characters.
- 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

Staff are prohibited from connecting dial-up modems to workstations that are simultaneously connected to PAWANET or another internal communication network unless approved by Technology Services.

Where modems have been approved, users must not leave modems connected to personal computers in autoanswer 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 PA network is prohibited. Exceptions to this policy require the approval of the Technology Services Department's IT General Manager, Network & Operations.

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. The system also provides access to IBM enterprise server ("mainframe") applications. 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.

To obtain Remote Access Authorization, see the *Remote Access Authorization* procedure in the public folders on the Exchange server.

The Port Authority also supports corporate site-to-site VPN connections and utilizes Cisco equipment for these connections.

2.2.6 Network Resources Hardware Standards

2.2.6.1 Standard Servers

To see the current Port Authority standards for servers, see the Technology Services Department web page on eNet, or click below.

[PA Server](#)

2.2.6.2 Printers

To see the current standard, see Technology Services Department web page on the eNet. If you are already viewing this document on the eNet, click below.

[PA Printer](#)

2.3 Network Naming Conventions

2.3.1 Server Names

All server names should conform to the standard 8-digit code, with the first four characters indicating the facility. Click below for a listing of facility codes.

[Facility Codes](#)

The second two characters represent the type of server, i.e. file storage, infrastructure, backup, application or database. The link below contains valid server functionality codes.

[Server Functionality Codes](#)

The final two characters contain a unique sequential two-digit identification number.

Static IP addresses for servers, printers and faxes must be within the address range of 201 to 234 of the respective subnet. All information regarding the name and address configuration should be forwarded to the Server Design Group, to ensure that duplicate names are not used.

2.4 Directory Services and Structure

The Port Authority uses Novell e-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 as e-Directory objects. IPrint should be utilized.

Applications are distributed using Novell's ZENworks. Applications are distributed based on the type of workstation and user definitions. Scheduling of distributions is done in conjunction with client departments.

2.4.1 File Storage Guidelines

All business related files should be saved to a shared drive or the user's home directory (U:). Non-business related files may be stored locally (C:) and backed up to removable media such as CD/DVD-ROM, etc if needed.

When saving files to network storage, whether on the U:\ drive, S:\ drive or any other network storage location, it is important to remember not to exceed a maximum of 255 characters for the file name **and its full path**. The length of a file name consists of: the full directory path including the server name, directory name, names of all sub-directories and the name of the file. This also includes special characters such as slashes and dots. The 255 characters limit is a known issue in both the NetWare and Windows environments as well as with data backup software.

Some of the problems that may result when full file names exceed the 255 character limit may include: inability to backup files, inability to restore files, errors when copying files or deleting files, and other problems with file utilities such as Hierarchical Storage Management (HSM), archiving and backup utilities.

To prevent the types of problems described it is highly recommended that the following guidelines be observed:

Abbreviate file and folder names to keep them as short as possible

Avoid many levels of sub-directories with long names

Don't move or copy existing directories, and the files they contain, to other directories. This only adds their names to the existing file name and path.

Avoid exotic and "wild-card" characters such as:

underscore at the beginning of directory and file names " _ "

blanks at the beginning of directory and file names

asterisk " * "

question mark "?"

semi-colon " ; "

An example of a full file name is as follows:

\\1MADCLUST\DATA\TSD\share\projects\PATH\ExpressRail\file123.doc

The format is: \\<server name>\<volume>\<department>\<directory1>\.....\<directoryX>\<file name>

In the above example the full file name is 64 characters, including spaces and all special characters.

2.5 System Management

All computing at the Port Authority is performed on workstations connected to PAWANET. Port Authority departments receive support for their network from the Technology Services Department and the authorized Enterprise vendor. There is a division of responsibility between Technology Services Department and those responsible for the management of departmental network resources.

The department is responsible for selecting a Business System Manager who will manage the departmental network resources. Technology Services Department will oversee the System Administrator(s). The System Administrator provides day-to-day operational support. The following chart delineates the major responsibilities of Technology Services Department System Administrators and the Departmental Business System Managers. Click below for detailed information concerning System Administrator duties:

[Guide to Systems Administration](#)

2.5.1 Technology Services Department and Departmental Business System Manager Responsibilities

Technology Services Department Responsibilities	Business System Manager Responsibilities (May be carried out by department staff, contract with TSD or third party)
Select and install: Servers Desktop PCs CAD Workstations	Select and Manage: Business Applications Software

<p align="center">Technology Services Department Responsibilities</p>	<p align="center">Business System Manager Responsibilities (May be carried out by department staff, contract with TSD or third party)</p>
<p>Network & Local Printers PC Peripherals Routers and switches Cabling Wiring closet hardware</p>	
<p>Promulgate Port Authority Standards for, install and maintain: Workstation OS and configuration Network OS and configuration Physical and logical security for: Network Servers Workstations PC Peripheral Devices User Accounts Databases Virus Protection Back up and Recovery Hardware Software Addressing/ Naming Conventions for Network devices</p>	<p>Review and Verify Port Authority Standards for installation and maintenance of: Current Workstation OS Current Network OS Physical and logical security for: Network Servers Workstations PC Peripheral Devices User Accounts Databases Virus Protection Download and install current virus protection software and data files. Back up and Recovery Maintain tape library</p>
<p>Establish and monitor Performance and Capacity Standards</p>	<p>Review and verify Performance and Capacity reports</p>
<p>Set standards for, and provide database administration</p>	<p>Monitor database performance</p>
<p>Establish requirements for Business Resumption Plan</p>	<p>Develop, validate and document Business Resumption Plan Implement Business Resumption Plan if necessary</p>

Technology Services Department Responsibilities	Business System Manager Responsibilities (May be carried out by department staff, contract with TSD or third party)
<p>Conduct Change Management Meetings: Establish version control procedures Create a forum to insure good communication in the agency.</p>	<p>Review and monitor Change Management tasks: Verify version control Document changes in department devices Inform Technology Services Department of all significant changes — hardware and software.</p>
<p>Maintain Documentation Library containing, for example: Suppliers' manuals on all software and Hardware Configurations of all servers and workstations Physical media, such as back up tapes.</p>	
<p>Select, configure and deploy software distribution tools.</p>	<p>Monitor and review software distributions.</p>
<p>Electronic Messaging to include e-Mail, calendaring and message-enabled applications.</p>	<p>Supply users e-mail setup information as needed</p>
<p>Provide direct support to end users on the use of workstation and applications running on the department's network resources.</p>	
<p>Select and provide virus protection software and data files. Maintain a log of all virus scan activity for daily review.</p>	<p>Report all suspected instances of computer viruses immediately to the Customer Support Desk in accordance with established IT security procedures</p>
	<p>Maintain and control software licenses</p>

Note: System Administrators do not create patches or upgrades.

To see a more detailed description of System Administrator responsibilities, see the Guide to System Administration, or click below.

[Guide to Systems Administration](#)

2.5.2 Change Management

System Administrators are responsible for reporting to the Technology Services Department all changes pertaining to:

Departmental hardware:

All network connected devices, such as:

- Printers
- Print servers
- Scanners
- Network Interface Cards

Software:

- Non-standard operating systems
- Non-standard applications

System administrators are responsible for participating in Change Management meetings or for making sure that a representative participates.

2.5.3 Turning Over a New LAN Resource to the System Administrator

Whenever a new departmental network resource goes into production, the installation team or vendor is responsible for turning over to the System Administrator of the new departmental network resource all of the items on the *Information and Documentation Transition List*. To see this list, see the Technology Services Department Web page, or click below.

[Information and Documentation Transition List](#)

2.6 System Backup and Recovery

There are two Port Authority approved standard software products used to perform scheduled server backups:

- FDR Upstream and Mainframe based tools are used to create data backups that will be stored remotely and managed automatically. The use of these backups is required to assure off-site data storage at a secure facility.
- The System Administrator is responsible for verifying that system backups, both local and remote can be used to restore the data. Tests of the ability to successfully restore from both backup systems will be performed annually. . See section 2.7 – Business Resumption Plan to establish and test recovery processes It is recommended that the test data restore be performed on a single non-critical directory only, not the entire server. Tests of the ability to restore system and application files will be performed on a non-production server in the Lab. 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.
- Testing a full restore should only be performed on a non-production server.

The product used will depend on the criticality of the data and the need for redundancy. For the current standard versions click below:

[PA Server](#)

All backup media and records must be treated with the same level of security and confidentiality as the original data.

2.6.1 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.

2.6.2 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.

2.7 Business Resumption Plan

The Departmental Business System Manager should work with Technology Services to develop a disaster recovery and contingency plan. The System Administrator should participate in the planning, design, implementation, testing, updating and documentation of the plan. [Appendix 2](#) shows a recommended outline for such a plan. The Business Resumption Plan should be updated quarterly and tested at least annually.

2.8 Telecommunications Standards for Enterprise Network Resources

To see the standards and guidelines for the following telecommunications components, please see the Appendix.

[Appendix 3](#) -- Standards for Setting up Closets & Communication Rooms

[Appendix 4](#) -- Standard Cabling Schemes

[Appendix 5](#) -- Unified Wiring Specifications

[Appendix 6](#) -- Telephone Closet / IDF Termination Blocks

[Appendix 7](#) -- Workstation Jacks

[Appendix 8](#) -- Standard Switches

[Appendix 9](#) -- Workstation and Lateral Cable Identification Management

[Appendix 11](#) – Fiber Optics Specifications for Network Services - PAWANET

2.8.1 Closet and Telecommunications Room Access

The following standards need to 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, the System Administrator must submit a TSD Service Request (TSR) Form.

[TSD Service Request \(TSR\) Form](#)

2.8.2 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, so as 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.

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. Access to this room will be reserved to TSD staff and an agreed upon member 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.

2.8.3 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 5L-30P 208/220 volt 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.

2.8.4 Telephone Company Interface

The following items are needed for the telephone company interface. If your department has contracted with the Technology Services Department (TSD) to provide internal telecommunications for the department's network, TSD will provide them. If the department is designing and procuring its own network resources, then the department will be responsible for providing them, depending on the requirement of the department's network.

- a) Install a dedicated wallboard for Telco demarcs
- 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

2.9 Documentation

It is the responsibility of the System Administrator to establish and maintain a library of all documentation designated as standard by the Port Authority. These include archived system files and system backups. System Administrators should refer to the [Guide to System Administration](#) for a list of standard/required documentation.

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. To that end, the Technology Services Department has established a procedure with the **Customer Support Desk** to provide an expedited response for quick containment. The phone number is **212-435-7469**, and the Support Desk is staffed 24 hours a day, seven days a week.

3.2 Background

A computer virus, in its simplest form, is a software program written to alter the way a computer operates--without the permission or knowledge of the user. The virus enters a PC desktop or a departmental network server when the user executes an infected program or data file. Computer viruses can spread via removable media, or from files downloaded from online services or the Internet, or through electronic mail attachments. Multiple infections can occur on the desktop as these files are used or copied across the network.

Computer viruses can destroy or alter valuable data and program files. If not detected and eradicated, they can spread to other PC desktops causing serious disruption in business operations and considerable loss of staff time and valuable data.

3.3 Standards

Standard virus protection software must be installed on all network servers and personal computers, and updated on a regular basis. Departments are required to implement appropriate procedures to ensure adherence to this standard and to promptly report all virus incidents to the Customer Support Desk.

All users must leave the current version of virus scanning software installed on their desktops. For the current standards on virus protection software, click below:

[Workstation Software for Windows XP](#)

[Workstation Software for Windows XP 64 bit](#)

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)

3.4.1 Preventing Virus Outbreaks

The following tips will help end-users prevent virus outbreaks:

- Ensure that your computing devices, especially laptops, have antivirus installed and running. (McAfee displays a shield with a "V" in it, in the lower right-hand corner of the computer screen.)
- Ensure that your virus DAT files are up to date. (For McAfee, "right-click" the shield and select "About VirusScan...". DATs are updated daily. If your DATs are more than 2 two days old, update them by "right-clicking" the shield and selecting "Update Now".) Then,

- contact the Customer Support Desk to determine why your DATs are not updating automatically.
- When copying data from removable media, (floppy disks, CDs, DVDs); be sure you are getting them from a trusted source. Ask if the media has already been scanned for viruses.
 - When downloading data from the Internet, only do so from known / trusted sites.

3.5 Virus Protection Stand Alone PCs and Laptops

Users of stand-alone PCs and laptops are responsible for ensuring that virus protection is running and up to date on these devices. Users of such devices should contact the Customer Support Desk if they need assistance.

3.6 Acquisition and Installation

The Technology Services 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. Staff should contact the Customer Support Desk for assistance.

4.0 Electronic Mail

4.1 E-Mail Overview

The PA's Electronic Mail System (E-Mail) is designed to facilitate Port Authority 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 Policy on Use of E-Mail: Highlights

The Computing Resources Policy provides guidance on the appropriate use of e-mail. This policy applies to any person who has access to the E-Mail system. For a complete copy of the policy, click on the link below.

[Computing Resources Policy](#)

Highlights of the policy are:

- The E-Mail system is not intended to transmit sensitive materials, such as personnel decisions and other similar information.
- All e-mail messages and attachments are property of the Port Authority. The system is not to be used for employee personal gain or in support of any purposes not related to Port Authority business.
- An e-mail message should not be used for disseminating information that is critical and/or needs to be retained longer than 120 days. Such information should only be transmitted as an attachment, for example a Microsoft Word document. The attachment must be filed outside the E-Mail system for retention and security in accordance with the Port Authority Records Retention Program if appropriate.
- The Port Authority reserves the right to review the contents of any e-mail communication when necessary for Port Authority business purposes.
- Employees and other users may not intentionally intercept in any way another person's e-mail messages without prior authorization.
- E-mail may not be used for the solicitation of funds or for messages that are political, harassing, threatening abusive, defamatory, obscene, religious, sexually explicit or unlawful or that infringes on copyrights. Use of e-mail for employee organization business other than communication with management representatives is also prohibited.
- Each message is automatically deleted from a user's mailbox on the Exchange server and from backup media a total of 120 days from the date of receipt or creation. It may be deleted without notice.
- E-mail messages or attachments that you delete may remain active on other recipients' accounts or on backup media, but for no more than thirty days on back up media.
- Contractors and other third-party users who are in violation of this e-mail policy may be denied access to the system and legal remedies may be pursued.

- Employees who violate the e-mail policy may be subject to disciplinary action, including dismissal from employment. In addition, misuse of e-mail may be referred for criminal prosecution.
- Passwords should be difficult to guess and changed every 90 days to ensure security of the e-mail messages. Users should not share their password with anyone else. Users are accountable for messages sent from their accounts.

4.3 E-Mail Etiquette

Since e-mail is different from paper-based messages, e-mail messages require certain conventions to ensure effective communication. For information on E-mail Etiquette click on the link below to view the document stored on eNet :

[E-Mail](#)

4.4 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 USinternetworking data center and network to the Port Authority network.

4.4.1 Public Folders in the Exchange Organization

Public Folders on a Microsoft Exchange server provide a public forum where authorized users can share information, such as project information. In general, Public Folders should be used for dynamic--that is, frequently changing--information--or, for files or e-mails that are being worked on collaboratively by a workgroup. Static documents, such as corporate policy statements, should be placed on the corporate Intranet (eNet) and not on the Public Folders. Documents to be stored long-term should be stored outside of the E-Mail system such as on a Novell file server and in accordance with the Computing Resources policy and Records Retention program if appropriate.

All Public Folders reside on the Public Folder servers. Such Public Folders are created, and then supported, by the Technology Services Department at the request of a department. When a request is received, TSD reviews it to determine whether it is an appropriate use of a Public Folder; or, if it is not, whether some other mechanism for communication or collaboration is needed such as EmployeeNet. The criteria used for determining the appropriate use of Public Folders are as follows:

- Information must be dynamic.

- Public Folders should not be used to replace storage on a workgroup's shared network directory.

4.5 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 2003 servers.
- E-mail is protected by TrendMicro's InterScan and ScanMail 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:
 - MAPI (Microsoft's Messaging Mail protocol)
 - Internally for X.400 mail protocol (which Exchange servers use)
- IMAP4 and POP3 mail protocols, NNTP news protocol, and LDAP directory protocol are disabled.
- Front-end Exchange servers running TrendMicro's Internet 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.
- The two supported forms of SMTP addresses are:
 - Primary form: FLastname@panynj.gov
FLastname where F is the first initial of the user's first name and Lastname is the last name, and FLastname conforms to the corporate standards for a unique Novell user's username (also known as Novell ID). FLastname is also used as the Alias for a user in the Global Address List. Note that an earlier format with truncating the above to a maximum of eight characters is still in use for accounts created prior to Sept. 2001 (example: Flastnam@panynj.gov).
 - Secondary form: Firstname.Lastname@panynj.gov
- Exceptions are governed by Novell directory structure and user account requirements.
- Each individual e-mail message and its file attachments has a combined limit of 10MB.
- Each regular user mailbox has the following size limits:
 - 45 MB - user receives warning notice
 - 55 MB - user is prohibited from sending
 - 85 MB - user is prohibited from sending or receiving

- When we upgrade to Exchange 2007, later this year, the mailbox storage limits will be increased as follows:
 - 80 MB – user receives warning notice
 - 90 MB – user is prohibited from sending
 - 100 MB – user is prohibited from sending or receiving
 -
- 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 Novell file servers.

4.6 Remote Access to E-Mail

We provide a secure Internet-based web browser access to corporate e-mail utilizing Microsoft's Outlook Web Access (<https://email.panynj.gov>). In addition, we have wireless e-mail access utilizing RIM's Blackberry Enterprise Server and Blackberry handheld devices.

Also, remote access to the Port Authority E-Mail system is available through the Agency's Remote Access System. Please refer to the section on Remote Access System in this document.

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

Category	Software Name	Minimum Version
	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:	Macromedia ColdFusion MX	7.0
Development and Design Tools:	Macromedia Dreamweaver MX	9.0
	Macromedia Fireworks MX	9.0
	Macromedia Flash MX	9.0
	Adobe Photoshop	9.0
Database	Oracle Database	9i
	Microsoft Access	2007
Programming Language/Scripts	ColdFusion MX	7.0
	Java	2.0
	PERL for Windows	5.0
	JavaScript	1.0
Search Engine Software:	UltraSeek	5.7
Bulletin Board/Discussion:	Chatspace WebBoard	6.0
Web Performance Monitoring:	WebTrends Marketing Lab 2	2.0
Content Management:	Stellent	7.5

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.

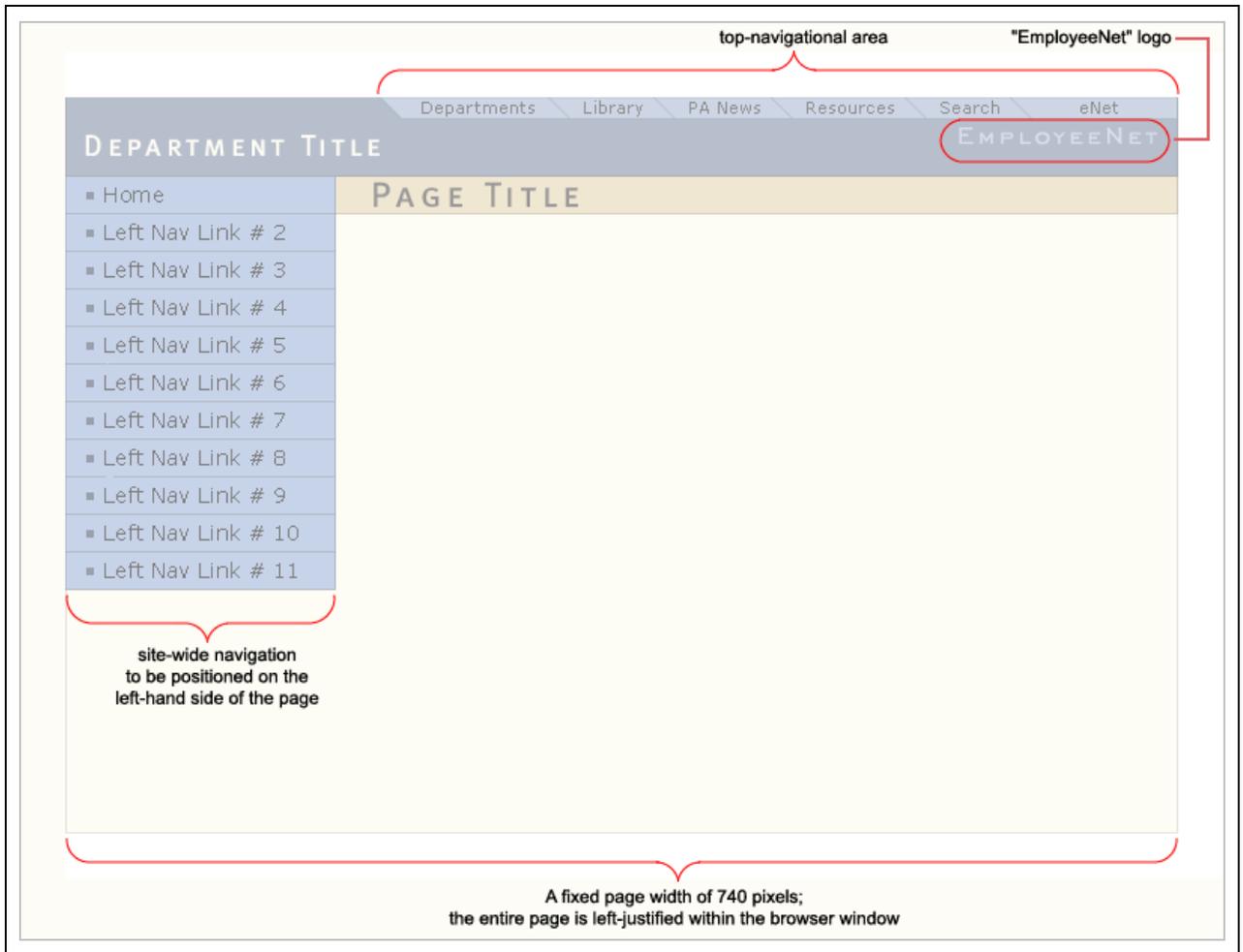
Departmental Web Site Standards and Guidelines

Prescribed standards are assigned to only the following items:

<i>Page Width:</i>	A fixed page width of 740 pixels
<i>Page Justification:</i>	The entire page is left-justified within the browser window
<i>Global Navigation:</i>	A top-navigational area, which provides for global links within eNet
<i>eNet Logo:</i>	The top-navigational area includes an accompanying "EmployeeNet" logo whose position is fixed
<i>Resolution:</i>	Pages will be designed for optimal viewing at the 800x600 setting.
<i>Site Navigation:</i>	<p>Site-wide navigation shall be positioned on the left-hand side of each page, except for the home page, where navigational links may be positioned anywhere on the page.</p> <p>All efforts should be made to present the entire navigational scheme without the need to scroll.</p> <p>Positioning of each navigational link must be consistent throughout the entire site.</p>
<i>Masthead - Heading and Subheading:</i>	The design for the masthead area, which included the page heading and sub-heading, shall be flexible and will be developed with the customer department.
<i>Body:</i>	The design for the body area shall be flexible and will be developed with the customer department.

The Departmental Web Site Standards are Illustrated Below:

A. Basic Page



B. Home Page



5.3.2 Accessibility Guidelines

TSD'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 and Workstation Operating System

6.1 Overview

The Port Authority makes extensive use of workstations networked into an Enterprise Wide Area Network to accomplish its business objectives. 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 Inventory

All computer related hardware, including printers must be maintained in the Port Authority's (PA) PC inventory. Tivoli Asset Management for IT (TAMIT) is the system of record for all managed PC assets within the PA. The data obtained from this system is used for PC inventory reconciliation purposes and report generation. Users requesting changes to their PC inventory – including the decommissioning of assets, reassignment of equipment to another person within the same department/organizational unit, etc - should contact their Departmental IT Coordinator. The Departmental IT Coordinator should send the request to: jgrant@panynj.gov for processing. This e-Mail notification should include, at a minimum; the Serial Number of the PC, the user name, department number, organizational unit number and the type of change required. This information must be received by the 20th of each month (or previous business day) to be reflected in the subsequent month's report.

6.3 Workstation Operating System Standard

The Port Authority's standard operating system for workstations is Microsoft's Windows XP Professional. The current versions of workstation software for Windows XP are contained in the links below:

[Workstation Software for Windows XP](#)

[Workstation Software for Windows XP 64 bit](#)

6.4 Workstation Configuration

6.4.1 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.

6.4.2 Workstation User Accounts

Windows workstations must have user accounts that correspond to the user's network user identification. All workstations should include at least two login accounts, the local Administrator account and at least one user account. The local Administrator account should be used only by the System Administrator for workstation installations and maintenance.

6.4.3 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.

6.4.4 Drive Mappings

Drive mappings for workstations should be accomplished only through the Novell login script and should conform to the standard outlined. Locally configured drive mappings to network volumes are discouraged and should not be used. See Section 2.2.2.1 for drive mapping conventions.

6.4.5 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 current workstation standard can be accessed using the link below:

[Workstation](#)

6.5 Standard Department Workstation Software

The following software is the standard Port Authority software for departmental workstations. New computer installations should conform to the existing standard. Previous installations may use the alternate standard until they are replaced or upgraded.

6.5.1 Standard Workstation Software

- Windows XP, Professional Edition
- Novell NetWare Client
- Novell LAN Workplace Pro
- McAfee Antivirus
- Internet Explorer
- Microsoft Office Professional
- WinZip

Because technology is rapidly changing, the links below should be consulted to obtain the most recent versions of standard software.

[Workstation Software for Windows XP](#)

[Workstation Software for Windows XP 64 bit](#)

[Approved and Supported Software](#)

6.6 Enterprise Software

The sections below describe the standard Enterprise software.

6.6.1 PeopleSoft

Users requiring access to the Port Authority's Human Resources – Payroll System (PeopleSoft) must enter the link to the PeopleSoft application in their browser.

6.6.2 SAP

Users requiring access to the Port Authority's Financial and Procurement system (SAP) must have the current client installed on their workstation. System Administrators are responsible for installing appropriate components on the user's workstation as well as maintaining current application files on the network server for use. System Administrators must also work with the Customer Support Desk to install and configure IP addressable printers for use with SAP.

6.6.3 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 Services Department.

For the current list of Enterprise applications, click on the link below:

[Enterprise Applications](#)

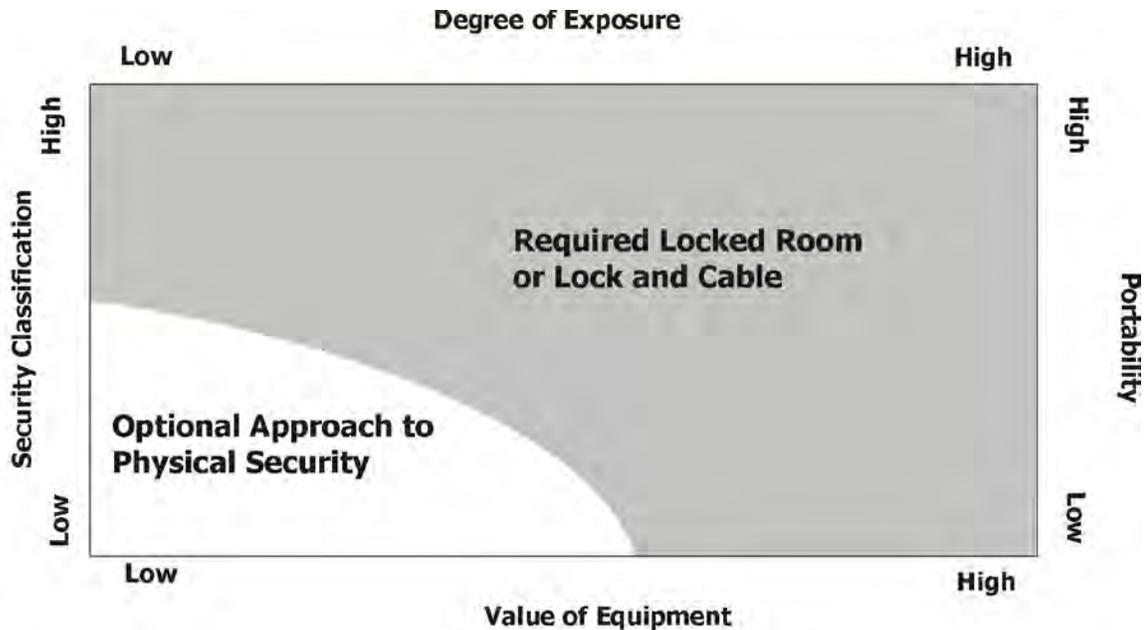
6.7 Workstation Security

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.

6.7.1 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 Systems Manager should make the appropriate determination of physical security required based on their best business judgment. In addition, it is recommended that workstations be assigned a coded theft recovery ID.

The graph below provides general guidance to Business Systems Managers in determining the level of physical security required.



6.7.2 Logical Security

Port Authority departments are responsible for providing for the security of computer resources and devices:

- Workstations should be protected with a boot-up password during power on.
- Screen saver passwords should be implemented with a maximum of a fifteen (15) minute time-out.
- All critical data should be backed up nightly onto either external media or a network drive.

6.8 Customer Support Desk

6.8.1 Functions

The Customer Support Desk's primary role is to provide assistance, troubleshooting, and first resolution of the problem. When necessary, problems are referred to the appropriate party. Customer Support Desk Agents are equipped to answer questions pertaining to vendor-packaged software, hardware problems, resetting of passwords, etc. Incoming calls are evaluated and a determination made as to whether the call can be handled by Customer Support Desk Agents or referred. Customer Support Desk staff maintains records and collects information, including listings of appropriate contacts, to ensure that all calls are handled properly.

Using problem ticketing and referral software, each call is assigned a problem number, and then forwarded to one of the following: the System Administrator, a desktop technician, a Port Authority staff member responsible for that particular problem, or an outside contractor. A ticket is opened and an email submitted with the ticket information to the customer. When the problem is fixed, the Customer Support Desk Agent closes the trouble ticket and a closure email is also submitted to the customer. When special issues arise within the Agency, Customer Support Desk staff is alerted. They plan a strategy to resolve the problem and handle incoming calls related to the issue. Reports of outstanding ticketed

problems are generated daily by the Customer Support Desk ticketing system for management review.

6.8.2 Hours of Staffing

The Customer Support Desk is staffed 24 hours a day, seven days a week. Desktop support technicians are onsite at major facilities from 7:00 AM to 6:00 PM, Monday through Friday, and on call as needed from 6:00 PM to 7:00 AM.

6.8.3 Escalation Procedures

Generally, when major issues are anticipated, the Customer Support Desk Supervisor is notified in advance of the issue. The Supervisor immediately alerts the IT Manager Customer Services of the problem and the proper response. When the Customer Support Desk staff encounters problems, they immediately notify the Customer Support Desk Supervisor who helps them resolve the problem. If the issue is urgent and requires additional attention, the Customer Support Desk Supervisor notifies the IT Manager Customer Services. The IT Manager Customer Services then escalates to the Assistant Director, Technology Infrastructure and others, as appropriate.

6.9 Administrative Rights Procedure

Technology Infrastructure & Service Delivery (TISD):

A PA3624A form is submitted to the TISD Customer Services Group.

The form is reviewed for accuracy and sent via email to the TISD-AD for approval.

TISD AD reviews and approves request with start and end dates.

If no start and end date, the form is reviewed with the CTO for approval.

Pomeroy:

Request for administrative rights received on approved PA3624A form from TISD Customer Services Group.

For Server:

Email is sent to the Server Team with approved PA3624A form attached.

Administrative Rights spreadsheet is updated with the following information: Ticket #, Date Opened, Department, Last Name, First Name, Description of Request, Date Completed, and Time Limit.

If no time limit specified: Marked on spreadsheet as "NO TIME LIMIT SPECIFIED"

Time limit specified: Noted in spreadsheet and marked on calendar to send removal request to server team on the day of removal.

Email is sent to End User 3 days prior, notifying them of impending removal of rights on server.

On day of removal: Email is sent to the Server team to remove rights.

Rights removed by Server Team, confirmed via email.

Spreadsheet is updated.

For PC:

PA3624A form is processed with the Support Desk team to grant administrative rights to End User until specified date.

Administrative rights spreadsheet is updated with the following information: Ticket #, Date Opened, Department, Last Name, First Name, Description of Request, Date Completed, and Time Limit.

If no time limit specified: Marked on spreadsheet as "NO TIME LIMIT SPECIFIED"

Time limit specified: Noted in spreadsheet and marked on calendar to contact the End User on the day of removal.

Email is sent to End User 3 days prior, notifying them of impending removal of rights on PC.

On day of removal: Systems Administrator contacts End User via phone and/or email to remove administrative rights.

Rights removed by Systems Administrator.

Spreadsheet is updated.

TISD Assistant Director & CTO:

Review Administrative Rights spreadsheets once a month.

6.10 *Computing Resources Policy*

Computing resources are intended solely for the Port Authority's business. Resources are not intended for personal gain or in support of any purposes not related to the Port Authority's business. The Port Authority's policy on computing resources is provided at the link below.

[Computing Resources Policy](#)

6.11 *Use of Port Authority Owned Computer Equipment at Home*

The Port Authority's computer equipment may be authorized where the benefit to the organization can be clearly demonstrated and the employee's intended use cannot be accomplished in the workplace during normal business hours. The Port Authority's policy on computer equipment at home is provided at the link below.

[Port Authority-Owned Computer Equipment at Home](#)

To safeguard the Port Authority's equipment and data, all authorized users must adhere to all applicable standards as if the equipment was in use at a Port Authority site. This includes physical security of equipment and virus scanning. In addition, where persistent Internet connections are in place, an approved firewall configuration and software must be in place.

6.12 Software Licensing Guidelines

SOFTWARE LICENSE GUIDELINES

All software installed or running on Port Authority equipment must be licensed with a proof of purchase available for verification. Employees, Consultants or Vendors of the Port Authority must not install, upload, download, or use any unlicensed and unapproved software. Employees, Consultants or Vendors who acquire or use unlicensed copies of computer software are subject to disciplinary action up to and including suspension or dismissal. Copyrighted and licensed software may not be copied or duplicated, or installed on non-agency computers, unless such use is permitted by the software's license agreement.

The proper licensing of software is both a legal requirement and an ethical imperative. Software vendors and industry watchdog organizations regularly survey organizations for software license compliance and can assess substantive penalties for noncompliance.

Using non-licensed (copied or counterfeit) software has other risks:

- Greater exposure to viruses and corrupt or defective software.
- Inadequate or non-existent documentation and warranties
- Lack of technical support for the software
- Ineligibility for software upgrades and fixes

We must manage our software assets in a way that respects copyrights and software licenses, in order to protect confidential information and provide maximum benefit to the Agency, as well as to ensure the ongoing maintenance and operation of a safe computing environment while avoiding penalties and monetary fines.

GENERAL RESPONSIBILITIES FOR MANAGING SOFTWARE LICENSES

Procurement and Technology Services Department (TSD) will continue to work closely together to ensure that enterprise software supported by TSD, purchased through an Agency-wide agreement, and software purchased by Departments directly through

Procurement is licensed appropriately. The Audit Department will periodically perform audits in the area of software license compliance.

Appropriate documentation required to ensure software license compliance must include:

- software inventories with user counts or installation counts (including user name and machine name as appropriate)
- valid license agreements/license confirmations
- proof of purchase/email confirmation of purchase

These documents must be kept up to date and must be readily available for audit verification.

For enterprise software with agency agreements, TSD will oversee the management of these products to ensure the usage of software is within the contractual and license requirements. TSD will be responsible for addressing the documentation requirements listed above for these software products. The use of these licenses will be monitored and reviewed on an annual basis. The current list of enterprise software includes:

AutoCAD

BudgetPRO

Cognos Client Software

Livelink

PeopleSoft

Primavera

SAP

Schedulesoft

TRIM

BlackBerry

HIDS

Lumension (Patchlink)

McAfee Virus Scan

Microsoft Office 2007

Microsoft Server

MS SQL

Oracle

Record Now/Roxio

WinZip

For all other software, each department, through their business managers and IT coordinators, are responsible for assuring that software running on all computers utilized by that department's employees, vendors and contractors is appropriately licensed. The Department is responsible for maintaining and producing the required documentation listed above for this software. Departments should validate software in use against their inventory listing and purchases on a regular basis. These documents must be kept up to date and made readily available for audit verification.

Only the system administrators designated by the Technology Services Department for installation and maintenance will perform the installation of all computer software. Individuals are prohibited from installing free-ware or any software on their computers.

In situations where the presence of a given software application on an Agency computer represents a violation of copyright, license agreement, or a violation of security, privacy, or other Agency policy, remedies may include removal of the software application or, in some cases, complete review of the system on which the software is installed.

PURCHASING DESKTOP SOFTWARE

Before requesting purchase or installation of any software, the requestor should check the list of approved software available on the TSD ENET web page. This web page also provides a mechanism for requesting the review/approval of software not already on the list. Only software on the approved software list may be installed on Agency computers. This includes free downloadable utilities, browser plug-ins, freeware or shareware. No employee shall download such software to his or her computer. Only the system administrators designated by the Technology Services Department for installation and maintenance will perform the installation of all computer software, including free software.

As of July 2011, the purchase of desktop software has been centralized within TSD and is initiated by filling out a "Desktop Software Request" form #3694, available on ENET. You will be notified if your request is approved and you will also receive the license-key information. You will not receive any software media(CD/DVD). When you receive your license-key information, you should contact the Support Desk (10-7469) to arrange for installation of the software. You must provide the system administrators designated by the Technology Services Department with the valid license-key information and confirmation email to complete the install.

As stated in the General Responsibilities for Software Licenses, you should retain all information associated with the software licenses purchase. Department business manager and IT coordinators should also be provided with copies of all license information that you receive when purchasing software licenses.

7.0 Distributed Systems Environment

7.1 Overview

A number of department and 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 (Standard and 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 requirements mandate a dedicated ESX host.

7.2.2 Windows Data Encryption

For those applications that require additional data security measures, TSD 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. Prior to implementation, the Business System Manager should consult with the Technology Services Department to implement the Encrypting File System feature on Windows XP, 2003 and 2008 Servers (See <http://technet.microsoft.com/en-us/library/cc700811.aspx>).

7.3 Unix

Sun's Solaris is the currently supported UNIX operating system for infrastructure and corporate servers.

7.3.1 Unix Security

Unix servers must be physically and logically secured from unauthorized access. The following document should be used to secure your Sun Solaris server. Click on the link below to view the document:

[Unix System Security Policy](#)

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 should be kept offsite for disaster recovery purposes if required.

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.

7.5 Databases

Oracle 10.2.0.4 or higher and MS/SQL 2005 Server or higher are the supported database platforms for Port Authority systems. Auditing trail must be enabled for all database accounts with administrator privileges.

7.6 Application Security

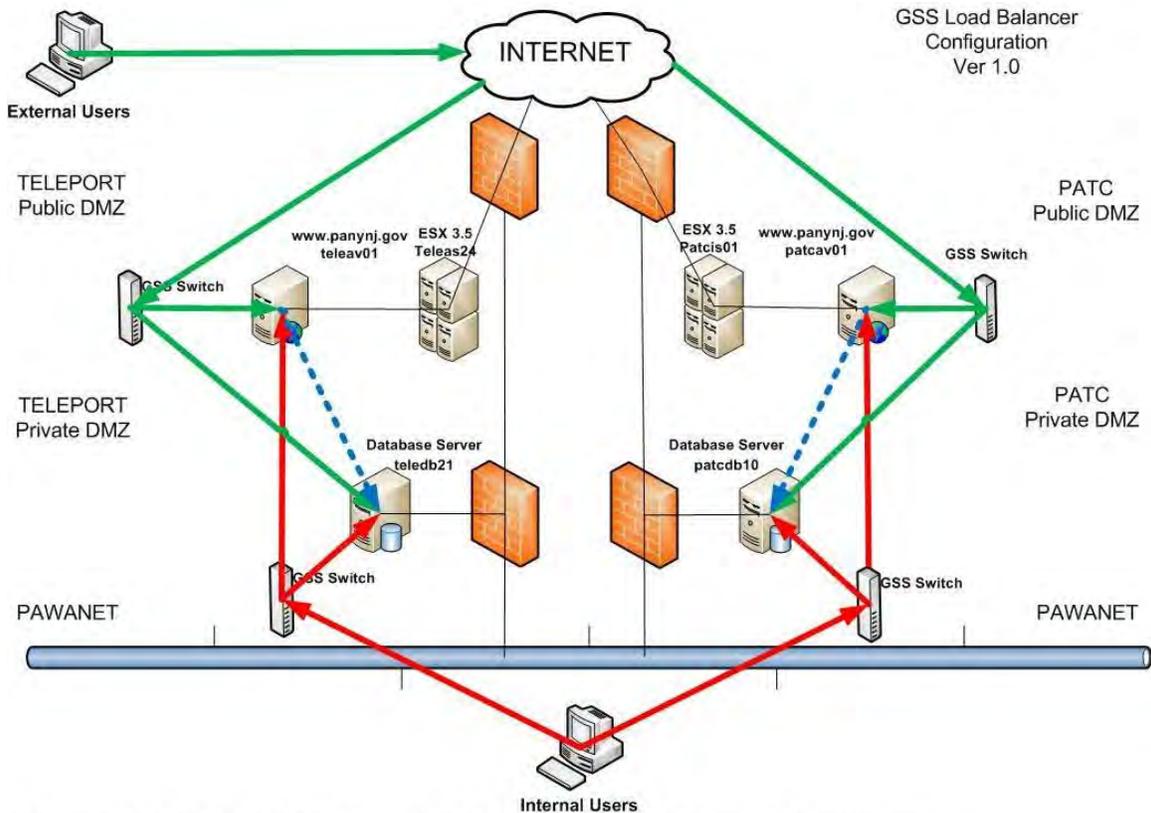
Depending on the application residing on the server, security may be administered at the application, database, module, screen, data field, and/or transaction level in addition to network authentication. Prior to implementation, the departmental manager who owns the application (Business System Manager) should review the capabilities of the application and consult with Technology Services Department staff to ensure implementation of the appropriate security levels. When in production, the administrator responsible for day-to-day administration of the application (Application Administrator) is responsible for maintaining the selected security profiles. At a minimum, all applications must require authentication to Novell Directory Services by way of a network login.

7.7 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.) He/she must also maintain a list of persons authorized to enter secured areas. Technology Services Department staff is available to provide technical assistance in making this determination.

7.8 Load Balancing – Failover Architecture

Depending on the requirements of the application, load balancing and failover architectures are supported. Below is a typical diagram of the load balancing/failover architecture.



There are a total of four load balancers, two are used for internal users and the other two are used for external users. Cisco GSS devices support load balancing or failover configuration

8.0 Voice Network

8.1 Voice Network (Telephone) Services

8.1.1 Port Authority Telephone Network

Most of the Port Authority's telephone services are provided by a Nortel SL100 (CS2100) Private Branch Exchange (PBX) network (approx. 11, 000 lines) with a host switch at **JFK International Airport (JFK)** and remote switches at **Newark International Airport (EWR)**, **LaGuardia Airport (LGA)**, the **George Washington Bridge and Bus Station (GWB/BS)**, **Lincoln Tunnel (LT)**, **PATH /Journal Square Transportation Center (PATH/JSTC)**, **PA Bus Terminal (PABT)**, **Gateway Plaza** in Newark, NJ, **225/233 Park Ave South** which serves **115 Broadway** and the **WTC site, 1 Madison Ave.** and the **NJ Leased Properties (NJLP)** which serves the PA Technical Center (PATC), the Jersey Ave. Maintenance Facility (JAMS), and the Holland Tunnel. Additional networked PBXs include a Nortel Meridian One PBX (130 lines) with Call Pilot serving **Port Newark** and a Nortel CS1000M switch (250 lines) serving the **Staten**

Island Bridges, with voice mail off the Call Pilot at JFK. **The PA Tech Center** also has a Meridian 1 System (300 lines) with Call Pilot for the Public Safety headquarters operation. Several of the above remote locations may also have Nortel adjuncts, such as 9150 or Norstar systems for secondary sites or special applications. Additionally, there are other PA sites (e.g., Brooklyn Piers, EWR Redevelopment, Harrison Car Shop, and Stewart International Airport) that have PBXs or service from other vendors that are maintained by the facility under separate maintenance contracts. See [Appendix 10](#) — Voice Network Diagram.

The SL100 remote switches are tied to the JFK host via Telco T-1 links, which serve as intermachine trunks. Most of these have been transitioned to our new Sonet network from Verizon. . If the intermachine trunks are lost, the remote switches function independently in Emergency Stand Alone (ESA) mode, but only with basic “Plain Old Telephone (POTs)” features (i.e., the more sophisticated features from the host switch are not available.)

Voice Over Internet Protocol (VOIP) is in the process of being implemented at a number of Port Authority facilities. VOIP is based upon a Cisco product line of Call Manager Appliances which also include Voice Mail, Call Center, Emergency Stand Alone, along with other features and functionality that will be introduced as the installed base of VOIP phones increases. As of the 2nd Quarter of 2010, VOIP has been implemented at: Teterboro Airport, Telecenter, Journal Square Transportation Center, PATH Waldo Yards, Lincoln Tunnel, George Washington Bridge, Lincoln Tunnel, and selected buildings at Newark Liberty International Airport and JFK International Airport. Work is continuing at PATH, GWB and LT to convert Analog and Customer Service phones to IP, while VOIP implementation for Harrison Car Shop and LaGuardia Airport is in its final stages. To date, approximately 1000 lines have been converted to VOIP.

This section will be updated on a quarterly basis to track the VOIP deployment.

As of August 1, 2008, AT&T is the vendor that maintains the Port Authority’s telephone network. .

Note: Most facilities also utilize some auxiliary business Centrex lines or private lines supplied directly from Verizon. These auxiliary lines often serve as back-ups to the above PBX systems. They are typically ordered from Verizon directly by the facility.

8.1.2 Local Service

At most Port Authority sites, Verizon provides local service. However, we utilize local service from AT&T Local Services at several New York sites. AT&T Local Services handles outgoing service on the JFK, LGA and PABT switches and both incoming and outgoing on the 225 Park Avenue South and 1 Madison systems.

8.1.3 Long Distance

The Authority's primary long distance carrier is currently AT&T under the NY State contract. Dedicated service is aggregated at the host PBX, where the SL100 routes long distance calls over the dedicated T-1's as a first choice: if these T-1's fail, the SL100 will route the calls over "PIC'd" service to Verizon, thus providing a redundant path and service for all SL100 long distance traffic.

8.1.4 Tie Line Network

Most facilities enjoy the convenience of our corporate dialing plan, which typically consists of a 2-digit access (tie line) code, followed by the 4-digit end user extension. This is done by connecting our main SL100 telephone hub at JFK to facilities via the intermachine links or tie lines that are leased from the local telephone company. Moreover, we avoid the usage charges associated with making intra-Agency calls over the public switched network.

Port Authority Access (Tie Line) Codes

- 03 - Stewart International Airport (Follow with 3-digit Stewart extension number)*
- 04 - Gateway
- 06 - Brooklyn Piers**
- 07 - Port Newark/Elizabeth
- 08 - Teleport Office Park***
- 10 - Park Avenue South, One Madison Avenue, 115 Broadway, WTC Command Post PAPD
- 11 - PATC, JAMS (NJLP), Public Safety at PATC and the Holland Tunnel
- 12 - JSTC/HCMF
- 13 - LGA
- 14 - EWR, 5 Marine View Plaza
- 15 - JFK, Bldg. 9, Vertical Control Bldg.
- 16 - Lincoln Tunnel, Teterboro Airport (Mgr.'s Office/REO)
- 17 - GWB/GWBBS
- 18 - Staten Island Bridges
- 19 - Port Authority Bus Terminal

**Users at Stewart International airport must dial "8" button in advance of the tie line access code. Note: When dialing Stewart using access code "03" from other PA facilities, you will experience 5-6 seconds of silence before you hear the Stewart greeting and can enter the desired Stewart 3-digit extension.*

***Users at Brooklyn Piers must use their access button in advance of the tie line access code.*

****Users at Teleport Office Park must dial "606" in advance of the tie line access code.*

8.1.5 Voice Mail

The primary voice mail system that serves the SL100 system is a Nortel Call Pilot system. It is located at JFK and serves approximately 4300 mailboxes. Independent Call Pilot systems that are networked to JFK's Call Pilot serve Port Newark and Public Safety at PATC (3rd floor). SIB obtains its voice mail from the main JFK host. Other vendor-specific voice mail systems that serve the non-Nortel sites include a Lucent Audix system at Harrison Car Shop and a Toshiba voice mail system at Brooklyn Piers.

Voice mailbox access is restricted by a unique password entered via the touchtone pad. Passwords must be changed every 90 days and must adhere to the password standard outlined in Section 2.2.4.5. Users should call the Telephone Help Desk at 212-435-4357 (HELP) for assistance with resetting passwords.

As indicated in Section 8.1.1, where VOIP has been deployed, Voice Mail is now provided via the Cisco based Unity Voice Mail system.

8.1.6 Telephone Help Desk

All trouble calls for lines and telephones on the PA telephone network should be directed to the **Telephone Help Desk at 435-4357 (HELP)**. Outside of normal business hours, the call is forwarded to the AT&T 24X7 Help Desk for repair on the next business day. Phone numbers on each facility's Critical Line List will have a 1-hour response time. Note: Extra charges will apply if the line/phone you are reporting is not on your facility's Critical Line List, so use judgment if requesting to override the Critical Line List for an immediate repair. Telco lines that are billed directly to the facilities should be reported directly to Verizon, as follows:

Verizon NY Repairs: 866-804-2640

Verizon NJ Repairs: 800-540-6960

Note: on an interim basis, trouble calls for VOIP will also go the Telephone Help Desk. Operational procedures are being worked to migrate VOIP Help Desk functions to the

Customer Support Desk and additional information will be forthcoming when those arrangements have been finalized.

8.1.7 Telephone Moves, Adds and Changes (MAC)

Orders for new or modified SL100 and Meridian One telephone network services are coordinated by the Voice Networks Telephone Help Desk at 212-435-3257 (HELP) using the attached form (Form PA3753 on ENET.)

[SL100](#)

8.1.8 Installation and Use of Home Telephone Lines for PA Business

Installation of a local "Telco" line from Verizon in the home for PA business purposes can be arranged via a request by the Department Director and approval by the Chief Administrative Officer (See AP30-4.01-Telephone Charges). Contact Will Lassalle at 212-435-3221.

8.1.9 Installation of Modem Lines for PA Business

Installation of modem lines in the office is discouraged due to network security issues, but if a PA business reason justifies a modem line, the attached form must be completed (in addition to the SL100 Telephone Service Request form referenced in Section 8.1.7). Contact Will Lassalle at 212-435-3221.

[Request for Modem](#)

8.1.10 PA Calling Cards

AT&T calling cards for PA business use may be obtained by submitting a request to the Manager, Voice and Data Networks that explains the intended use and business justification for the card and signed by the requesting unit manager. Contact Will Lassalle at 212-435-3221.

8.1.11 Toll Free (800) Services

Toll Free Services can be obtained via dedicated Megacom circuits or Readyline Service, where AT&T redirects calls from your Toll Free number to an existing local line. To obtain assistance with arranging for Toll Free service, call Will Lassalle at 212-435-3221.

8.1.12 Audio Conference Call Services (Voice)

To take advantage of AT&T's discounted New York State/City rates for Conference Call Services to the Port Authority,

New Users must call:

Robert G Taylor

AT&T Operations, Inc.

toll free 888-478-0374

efax 512-646-3696

Existing Accounts may call: AT&T Teleconference Center at 1-888-NYS-CONF (888-697-2663) (or, use your dedicated dial-in number to set up AT&T Reservationless conference call anytime – day or night – without making a reservation in advance!)

Instructions for New Users/Accounts:

Coordinators can begin the process of establishing a new TeleConference account by simply emailing the above Sales Consultant with the following information **5 days in advance of your first conference call:**

- Verify you are with New York City account: 12516422 (Note: The PA obtains the discounted service under this NYC account.)
- Bill Name (PORT AUTHORITY, plus Dept. Abbr., plus Unit Name)
- Host Name
- Host Phone Number
- Email Address
- Billing Address
- Cost Center (3-digit unit code, plus 3 digit program/facility code; Examples. 123G01 or 123A04)

When processing new accounts, the Sales Consultant will set up:

- A “**Billing Site**” account for each PA Unit based on your Cost Center code (3-digit Org. code, plus 3-digit Program or Facility code – Examples 123GO1 or 123A04) that will be used to pay for the service.
- A TeleConference “**Folder ID**” will also be created to identify each host (specific user); Folders sit under the umbrella of each Unit’s Billing Site account.

Once a Billing Site has been established, your Sales Consultant will have a Reservationless Folder ID created on your behalf. AT&T Reservationless Service provides the host with dedicated dial-in numbers and access and host codes. This enables the host to make conference calls without making a reservation in advance!

IMPORTANT: Each Unit is responsible for their own conference call account administration and billing obligations!

Please [click here](#) for more information on AT&T conference call services.

For AT&T discounted rates, open this attachment:

[ATT Discounted Rates](#)

8.1.13 SL100 Meet-me Conference Call Service (Voice)

PA staff can utilize a basic Meet-Me Conference Call service from our SL100 system that allows staff to reserve a special “435” number that allows up to 30 conference attendees (internal or external) to participate in a conference call. Each attendee dials in at the time predetermined by the organizer. The first party to call the number will continue to hear the line ring until a second party joins the call. Note: This is not a secure conference bridge, so anyone can dial in at any time. If you need a secure conference, use the AT&T service described in 8.1.13. Contact the Telephone Help Desk at 212-435-4357 to schedule an SL100 Meet-Me Conference Call.

Revised 12/22/08

9.0 Vendor Provided Dedicated Systems

9.1 Overview

Vendor Provided Dedicated Systems refers to the Information Technology software, hardware and infrastructure furnished and installed through a contract with an external provider. Generally, this refers to systems that are designed to support a large Capital Project, where the Information Technology Systems are either provided based upon detailed functional and technical requirements as outlined in a Request For Proposal (RFP); or, are an integral part of a detailed design and set of specifications prepared by an outside Engineering firm in the preparation of “Low Bid” contracts. These Capital Projects 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

The uniqueness of the Capital Projects is further reflected in the organizational structure within the Port Authority. Typically, a Line Department identifies a specific need that will require a Capital Project. The Line Department identifies the functional and operational requirements of the endeavor and solicits Project funds to support the initiative. On all technology related projects a representative from the Technology Services Department (TSD) 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 Chief Technology Officer (CTO) and is expected by our client departments. The Line Department or their representative shall submit a Technology Service Request (TSR) via the online form PA 3937 found on eNet, to solicit TSD support on these projects.

To ensure a successful project, and honor our responsibility to our customers and the Agency, one of the steps undertaken by TSD is to provide guidance with, 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 the large discounts negotiated in the various requirements contracts, ensures that the equipment can be gracefully integrated with other existing systems, and ensures that long term maintenance and systems administration contracts will be focused on the same product lines. Ensuring 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 is the first step. Responses to RFP’s should be reviewed for their compliance with the Standards and Guidelines. Deployment, integration and testing should be monitored by TSD to ensure that equipment or infrastructure is not duplicated, that the integration and migration plan will not adversely impact 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 should be directed to work with TSD in exploring all options, and if an exception is deemed required, the vendor should work with TSD to prepare the necessary Business Case to receive written concurrence from the Chief Technology Officer for this deviation from the Port Authority Technology Standards and Guidelines.

9.2 *Physical Security Technology Standards*

9.2.1 *Agency Standard for Digital Video Recording and Access Control and Alarm Monitoring*

Based upon the Agency's investment in and positive experience with Lenel's access control and alarm monitoring and Loronix's CCTV and Digital Video recording technologies, these product sets are the Agency's standard (please see below 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 compatible technologies agency-wide. September 11th reinforced the need to maximize the Port Authority's investment while providing for redundancy. 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.

A standard will also improve:

- The capabilities of an Emergency Operations Center and other facilities;
- 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;
- Access to and the sharing of information;
- Single learning curve;
- Minimization of maintenance and system administration costs.

Guidelines for using the Loronix standard include:

1. If the camera system needs to be recorded
2. When an upgraded or new system is being installed at a PA facility or at a tenant facility monitored or reviewed by Agency personnel or contractors
3. When rule based intelligence is to be added like motion detection and other related algorithm processes
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 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. Discuss bandwidth issues with Technology Services Department before proposing alternate solutions
9. On all new projects where Loronix is the site base system now.
10. When the OEM department needs override capabilities in the event of an incident.

Guidelines for using the Lenel standard include:

1. On all new or upgrade projects that need card access and / or alarm monitoring
2. On projects that will have security that needs to be monitored by PA personnel or contractors (airports are monitored by contractors)
3. On all new projects where Lenel is the site base system now
4. Where access is required to work with ID cards that exist and are compatible with Lenel
5. When the OEM department needs override capabilities in the event of an incident.

9.3 *Communications Infrastructure Standards*

The Port Authority Standard for Communications Infrastructure is Cisco. The link to the CTO's memo on communications infrastructure standards is shown below.

[Memo on Communications Infrastructure Standards](#)

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 should be purchased through the Cisco Requirements contract, which is administered by TSD 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.

9.4 *Server Infrastructure Standard*

The Port Authority's standard platform for File & Print and Application servers is IBM. The link to the CTO's memo on server infrastructure standards is shown below.

[Memo on Server Infrastructure Standards](#)

Technology Services has contracted discounted pricing with IBM 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. 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.

10.0 Wireless Technologies

10.1 Wireless Guidelines

10.1.1 Purpose and Scope

Applies to: all wireless devices and technologies including voice and data capabilities that store, process, transmit or access data.

Includes but is not limited to commercial and unlicensed wireless networks and laptops, cellular devices, scanning devices, messaging devices (2-way pagers and email devices) and PDAs.

10.1.2 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.

10.1.3 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

10.1.4 Wireless Local Area Networks - WLANs

I- OVERVIEW

Business requirements have arisen throughout various Port Authority locations for the improved use of Wireless LAN technology to facilitate local user mobility. Research has been done on the different technologies supported via 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.

This document from the desk of TSD's Senior Network Specialist is targeted for an agency wide audience of network designing and implementations for deploying wireless LANs 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.

II- SCOPE

The scope of this document shall present some standards for the Agency Wireless LAN and the specification of all devices and configurations.

III- 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.**

IV- OWNERSHIP

This document is under the ownership of Bill McPherson the Port Authority's IT Senior Network Specialist.

V- COMPLIANCE, REQUIREMENTS

All specifications defined in this document may be effective upon approval of and complete concurrence with TSD's CTO & Senior IT Architecture, to update wireless standards and policies as per IEEE and Wi-Fi Alliance std.

VI- DEVICE SPECIFICATIONS

The following sections will detail the various hardware components, and related firmware versions, that are specified for use in the Port Authority's WLAN solution.

6.1 Access Point Standard

Standards Details:

- **1250** 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. 1242 for light-weight AP's for WLAN controller.
- 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.
- Physically the device models (1242 & 1230) by default when AP connects to controller automatically becomes an access point.
- All autonomous, IOS APs must be upgraded to LWAPP, Note: LWAPP Upgrade requires AP to run at least IOS version 12.3.7. WAP2 with AES / CCMP for unique authentication deployments.
- **AP 350 is no longer supported.**
- **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:
 - v4.0.217.0 or above
 - 1242 & 1310 usage were spectrum analyzer testing warrents.
 - 1200 IOS AP must be LWAPP capatible.

- d. AP fallback enabled
- e. 3 SSIDs-each on separate VLAN's as per radio configurations.
Note: "guest" SSIDs must anchor on management string.
- f. 15 users per AP
- g. AP ratio-4:1
- h. Auto RF channel changes via configuration settings. Roaming rule consideration for extended service area (ESA), prevents interference between two overlapping APs with the same SSID. These types of APs must be configured on different channels or frequency ranges that do not overlap. This process will prevent co-channel interference.
- i. DTIM=2
- j. 800 APs per Mobility Group (or 8 '4404' controllers per mobility group)
- k. Use DNS to 'load-balance' AP' connections between controllers in same mobility group.
- l. If wireless is primary connection-'load-balance' AP' cabling connection to two different network switches

6.2 Antennae Standard

Cisco's AP1310 have both internal & external antennae while AP1242 have external antennae.

1200 AP series with multiple antennae supporting 2.4 & 5 GHz bands.

6.3 WLAN Controller Standard

The Cisco 4400 Series Wireless LAN Controllers is available in two models (4404, 4402) depending upon the number of AP's to be supported at each location. When roaming via settings on a controller for clients, the primary interest must be mobility group deployment. Mobility domains are for extended controllers ONLY.

4404 Controller Standard

- * 4 front Distribution System ports (gig only). Has fiber connections but can use SFP connector if copper is required.
- * Dual power supplies
- * One single out-of-band management service port
- * Handles to 100 AP's

4402 Controller

use (2 front Distribution system ports (gig only). Has fiber connections but can use SFP connector if copper is required)

- Dual power supplies
- One single out-of-band management service port
- Handles 12, 25, and 50 AP's

Controller Standards Summary:

- **4404-100 v4.0.217.0 (supports up 100 APs)**
- **4402-12 v4.0.217.0 (supports 12, 25 or 50 APs)**
- **Ports must be hard-coded to 1000-duplex**
- **Controller's location (connection):**

:

Controllers must connect to user block aggregation router

- i For sites with multiple core routers, connect each additional Controller to DIFFERENT user block aggregation router on DIFFERENT core.
- ii. For sites without multiple core routers, connect each additional controller to DIFFERENT user block aggregation router.
- iii For sites without aggregation routers or gig ports access switch, a Catalyst 4948 (**WS-C4948-S**) can be purchased to accommodate wireless controller.

For both 4404 and 4402, physical connections must include ports #1 & #2 in LAG (Link Aggregation) mode.

Data Site (dedicated) controllers:

1. Each location must have their own centralized WLAN controllers
2. **Two 4404-100** controllers (one in each WLAN) must be designated as failover for sites with **one** local controllers. APs connect directly to their local controller as their primary connection. For secondary & tertiary controllers-point APs to WLAN controllers.
3. **Two 4404-100 controllers** (one in each WLAN) will be designated for sites **without** any controllers. APs connect directly to these controllers as their primary, secondary and tertiary connections for failover

4. **Two 4402-12** controllers for guest access in DMZ

4404 and 4402 controllers, “service” and “virtual” ports are not used

3 SSIDs per controller with each SSID having independent security and QoS policy (e.g., **SSID #1 WLAN; SSID #2 QUEST-VPN; SSID #3 QUEST-PROXY**).

8 Controllers per Mobility group

5. **Note:** There is a 24 controller’s limitation per mobility group but to limit the chattiness of mobility messages between controllers belonging to same mobility group, there should be only 8 controllers per mobility group. Create new mobility group for 9th or more controllers

Management and AP-Manger interfaces reside on same VLAN. Mainain range of encryption cipher suites with algorithms under SSLv2 or SSLv3. Maintain authentication framework with Extensible Authentication Protocol (EAP). Disable all unnecessary services that the controlled AP’s are shipped with. Add controllers to WCS (Wireless Control System)for management.

VII CONTROLLER PLACEMENT

Following is a guideline for controller placements. Controller’s placement depends on a few important criteria such as size, WAN latency, local resources, mobility, scalability, cost and redundancy. Four separate scenarios are defined to meet these different requirements. PA considers these four placement types ...

Single local controller

Two or more local controllers

No local controller

Guest controllers

VIII OVERVIEW FOR NETWORK & SUBNETTING

- No Multicast on wireless
- Radius ACS v3.2 or higher
- 802.11 family of specifications developed by IEEE for wireless LAN technology.
- IP Lease = 1 hour as per static IP wireless device assignments.
- **DHCP server** for non-static IP wireless devices.
- MANAGEMENT VLAN ... Each controller needs 2 IP addresses for management and AP management interfaces. Two IP addresses must be on same VLAN
- USER VLANs

6. For sites with 10 or more APs on each controller use **/24 (510 IPs) for each SSID**
7. Each SSID is on different VLAN
8. Increase subnet size if more IPs are needed later for LWAPP.
9. **Note:** For non-FW controllers, there's **no need** for guest VLANs. Guests are terminated at guest controllers. It is at guest-LWAPP controllers that IP addresses for clients are handed out. The only VLAN needed at non-FW controllers is for SSID WLAN.
10. For sites with less than 10 APs for each controller, use /26 (62 IP) for each SSID

**THIS DOCUMENT IS FOR BEST PRACTICES WITH WIRELESS
HARDWARE IMPLEMENTATION AGENCY-WIDE SITE
DEPLOYMENTS ... NOT FOR WIRELESS DEVICE
CONFIGURATION PRACTICES.**

Appendix A

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. Deploying the use of WGB (autonomous workgroup bridging) topology with IOS AP version 12.4(3G)JA.
11. Maintain cryptographic strength range from 128-bits to 256-bits with matching symmetric algorithms AES-128 to AES-256

Appendix B

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 (config. 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

10.1.5 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.

10.1.6 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.

10.1.7 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", 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

10.1.8 Responsibilities of Technology Services 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.

10.1.9 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.

10.1.10 Responsibilities of Wireless and Handheld Device Users

Coordinate all requests through Technology Services 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.

10.2 Paging Device Policy And Procedures

10.2.1 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 contracts must be sent to the Chief Technology Officer. If approved, the requesting department is responsible for obtaining necessary authorizations and preparing a contract and/or purchase order.

10.2.2 Procedures

Specific models of paging devices and service pricing plans have been selected by Technology Services Networks Division, E-Mail Group, as agency standard models and plans, and will be used for all staff. The E-Mail Group will review all requests for alternate models or plans to ensure that the request is appropriate for the work need indicated.

All requests for paging devices should be sent via e-mail to Marion Resnick, E-Mail Group, mresnick@panynj.gov using the unified Wireless Device Approval form available by clicking on the link below:

[Wireless Device Approval Form PA 3943](#)

The request must be approved by the department director. Concurrence via e-mail is acceptable. Once the request form is reviewed, it will be forwarded to the service provider who will deliver the paging device directly to the requestor.

All service and equipment problems should be reported to Marion Resnick, E-Mail Group, ONEMAD 152TSD (for PA mail) or call 212-435-3251.

The service provider will send all invoices directly to the customer department. Each customer department will be responsible for reviewing, approving and processing the payment of the invoices. Each department is required to maintain an inventory list of assigned paging devices for use in verifying the invoice. Inconsistencies should be reported to the service provider for resolution.

Responsibility for keeping accounts current with the service provider will rest with the customer department. Prompt payment of invoices is critical as delinquency may result in termination of service.

Annually, the E-Mail Group will send each department director and their respective Chief, a listing of assigned paging devices for review. Each department must review the list, perform a physical inventory and reconcile any discrepancies. The reviewed inventory list must be returned to the E-Mail Group for update of the master list.

When the use of a paging device is no longer required, or upon termination of employment, the paging device is to be returned by the department to the service provider, and the completed [Pager Change Form](#) requesting the disconnection (available on ENET) is sent to Marion Resnick, the E-Mail Group. Please click on the link below for the form:

[Pager Change Form](#)

Staff below director level are allowed only one of the following devices, cellular phone, Nextel radio/phone or pager, unless approved in writing by the department director. BlackBerry devices are excluded from this restriction.

10.3 Cellular And Nextel Phone & Wireless Modem Policy And Procedures

10.3.1 Policy

The Port Authority obtains cellular and Nextel radio/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.

If approved, the requesting department is responsible for obtaining necessary authorizations and preparing a contract and/or purchase order.

10.3.2 Procedures

Specific models of cellular phones, wireless modems and service pricing plans have been selected by Technology Services, Voice Networks/Wireless, as agency standard models and plans and will be used for all staff. Voice Networks/Wireless will review all requests for alternate models or plans to ensure the model or plan requested is appropriate for the work need indicated.

All requests for cellular telephones, wireless modems and Nextel radio/cellular phones should be sent to Voice Networks/Wireless, One Madison Avenue, 7th floor, New York, NY, 10010, (212-435-8227 fax 212-435-3363), using PA form 3943, available online on Enet. The requesting director is responsible for determining whether there is sufficient business reason to authorize use of a cellular phone or wireless modem.

The request will be reviewed to ensure that a cellular telephone, wireless modem or Nextel radio/cellular phone is the best solution for the department's communications needs and that it meets the above criteria. Nextel should be considered only where substantial use of radio service is needed. Once approved the order will be sent to the contractor.

Once the order has been processed the contractor will ship the cellular telephone, wireless modem or Nextel radio/cellular phone to the customer.

When required, the installation of any cellular or Nextel telephone equipment in a PA vehicle, can be requested from Voice Networks/Wireless, and will be coordinated with the Central Automotive Division. Staff is advised that using a cellular or Nextel radio/cellular telephone while driving is dangerous and is restricted by law in both the states of New York and New Jersey.

Voice Networks/Wireless will arrange with the cellular or Nextel network service provider for the initial telephone number or wireless data service. Any subsequent number changes and/or disconnects will be processed by Voice Networks/Wireless upon receipt of a written request.

All charges for Verizon Wireless, ATT Wireless cellular service and Nextel radio/cellular service- including usage and equipment- are included on a consolidated invoice, which is processed under SAP by Voice Networks/Wireless. Courtesy statements are sent directly to the customer for review. Employees are responsible for reimbursement to the Port Authority for non-business calls (See AP 30-4.01, Non-Work Related Telephone Charges).

Annually, Voice Networks/Wireless sends each department director and their respective chief, a listing of assigned cellular, Nextel radio/cellular phones and modems for review (this listing can be provided to departments more frequently if required). Each department must review the list, perform a physical inventory and reconcile any discrepancies. The reviewed inventory list must be returned to Voice Networks/Wireless for update of the master list.

All service and equipment problems should be reported to Voice Networks/Wireless, One Madison Avenue, 7th floor, New York, NY 10010, 212.435.8227.

Staff below director level is allowed only one of the following devices, cellular phone, Nextel radio/phone or pager, unless approved in writing by the department director including specific business need for multiple devices. Blackberry devices are excluded from this restriction.

When the use of a cellular telephone, Nextel radio/cellular phone or wireless modem is no longer required, or upon termination of employment, the department must notify Voice Networks/Wireless which will issue the disconnect notice. The department is responsible for proper disposition of the cellular/radio equipment.

In accordance with PA environmental policies, all wireless equipment that is no longer needed must be returned to the vendor for appropriate handling and recycling.

All wireless phones and accessories that are old or not being used remain the property of the owner's department. Equipment in very good condition may be kept as spares. If the device is not needed or is not in good condition, select the appropriate procedure listed below for disposal. Contact Chuck Levinson via email or at 212-435-8227 to discuss disposal. Do **not** send devices to the Technology Services Department, unless you have received approval to do so.

For large numbers of wireless phones, fill out a Property Disposition Report, noting that you will be sending the unused phones back to the vendor for recycling. PA form 2331A -Property Disposition Report is available on eNet.

Send the Property Disposition Report form only to Margaret D'Emic in Procurement.

Nextel equipment must be sent to Michael Mistretta, Nextel, 59 Maiden Lane, 21st Floor, New York, NY 10038. Send only when you have a full box of phones. Accessories may also be returned to the above location, but must be packaged separately.

Verizon Wireless and other cellular equipment must be sent to a Verizon Wireless Warehouse, using labels provided by Voice Networks/Wireless. Contact Chuck Levinson, Technology Services Department, One Madison Ave. 7th floor, via email at clevinso@panynj.gov or call 212-435-8227.

Please include a note listing the contents (number of phones, etc.), indicate they came from our agency and the date and send a copy to Chuck Levinson, Technology Services Department, One Madison Ave. 7th floor.

Users should delete all stored numbers, names, caller ID lists and messages prior to returning equipment to the vendors. Use the phone menu or check the operating manual for instructions on how to do a "Master Clear" or "Reset" or "Erase". These are usually found in the "security" section and require the use of an access code, which is usually set to all zeros.

We suggest administrators verify that all stored information is erased on receipt of the equipment since it may be hard to do so after they are collected.

Assistance is also available by contacting the vendors' customer service support lines at the numbers listed below:

Sprint/Nextel: 800-390-7545

Verizon Wireless: 800-922-0204.

10.4 Technology Services Personal Digital Assistant (PDA) Policy

10.4.1 Introduction

Personal Digital Assistants (PDAs) are a class of handheld computers that currently offer limited functionality with compact size and portability. PDAs 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 PDAs, with further enhancements predicted.

In order to better serve the PA, and to limit the expense of supporting a wide variety of PDA hardware and software, Technology Services will support the use of the Windows based devices.

With a PDA, 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 PDA.

Any questions related to this policy should be directed to the Customer Support Desk at 212-435-7469.

10.4.2 Hardware – Hyper Link

Specific manufacturers listed below and other models using the current Windows Pocket PC 2002 or more recent versions of Windows operating system are supported.

Compaq/HP

The list of supported hardware will be updated from time to time to reflect current standards.

10.4.3 Software

All versions of the Windows Pocket PC 2002 (Operating System) or more recent Windows versions are supported.

Microsoft ActiveSync

The list of supported software will be updated from time to time to reflect current standards.

Any software found to interfere with normal operation must be uninstalled in order to receive support from Technology Services.

10.4.4 Support

Support for PDA hardware and software is provided by Technology Services through the Customer Support Desk. TSD will support the physical hardware connection (PDA cradle to PC) and software to support this connection. No software can be added to company owned PDA devices without TSD's assistance and director approval.

10.4.5 Training

Training will be available covering basic PDA use and integration with Outlook at the time of installation of the equipment. Training classes for the PDA units may be provided in the future depending on user demands.

10.4.6 Acquisition

The PA will purchase PDA units for employees with a business need for the PDA device. Employees are responsible for obtaining management approval. TSD 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.

10.4.7 Criteria To Qualify For A PDA Device

It is recommended that the purchase of PDA devices be limited to employees who:

Have heavy meeting schedules

Travel frequently

Do not have access to their desktop computers for at least two entire workdays 12 hours per week

PDA requests must be approved by a director or above. After a director grants approval, the unit will be ordered and installed by Technology Services personnel.

10.4.8 Personal Acquisition

Employees, who purchase their own PDA 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 PDA devices.

10.4.9 Breakage And Loss

Be aware that the touch-sensitive screen used on a PDA device is very fragile. Dropping a PDA device from the height of a desktop, or applying too much pressure on the screen itself, often results in breakage of the glass. Once this happens, the PDA device is unusable. If a PDA screen is broken, it will be up to the user department to justify the cost of a replacement unit.

If a PDA device is lost, the employee is responsible for replacing it. As with all PA equipment, PDAs should be used for business purposes only.

10.4.10 Data Security Considerations

Since in most cases the data residing on a PDA 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 PDA. Extreme caution should be taken when using company confidential data on the PDA units.

At the present time, Technology Services is researching options for encrypting PDA data using a third-party application. Until a solution is found, great care should be taken to ensure that important or confidential information doesn't end up in the wrong hands.

10.4.11 Data Backup

Though it doesn't happen often, it is possible to lose, damage or duplicate the data that resides in the PDA and PC applications. Technology Services will provide assistance in attempting to recover files or data from data corruption.

10.4.12 Personal Digital Assistant (PDA) Policy

Instructions:

Send a copy of this completed form to Technology Services.

I have read, and agree to abide by, the terms of the Technology Services Personal Digital Assistant Policy.

Signature _____

Printed Name _____

Date _____

Approved By:

Director _____

Date _____

10.5 BlackBerry Device Policy & Procedure

The Port Authority provides corporate wireless e-mail services using the BlackBerry device from RIM.

To obtain a BlackBerry, you must have the approval of the department director using the Wireless Device Approval form PA 3943 which is available on eNet or by using the link below. It must be completed in its entirety including the appropriate account code.

The BlackBerry is a palm-sized device designed to synchronize with Outlook and other e-mail systems. The monthly cost for BlackBerry data service is approximately \$41 plus fees. Voice service through Verizon costs an additional \$30 per month. If radio service is required through Nextel, the cost would be \$40 for the voice/radio service. 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.

Forward the completed form to an authorized approver for their concurrence. He or she will then forward it via e-mail to Marion Resnick, Technology Services Department. If you have any questions regarding a BlackBerry device, please contact Marion Resnick at 212-435-3251.

[Wireless Device Approval Form PA 3943](#)

[For information about combined BlackBerry data and cell phone devices, see section 10.6 below.](#)

10.6 BlackBerry Guidelines

10.6.1 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.

10.6.2 Recommendation for Essential Staff and First Responders

Technology Services does not recommend use of the BlackBerry device combining e-mail and voice capabilities for essential staff or first responders as the device becomes a single point of failure for both modes of communications. The hybrid device relies on a single network for service connection, and in an emergency, this network could be overcrowded or otherwise unavailable, resulting in the loss of both voice and e-mail service.

10.6.3 Support

Support for BlackBerry devices is provided by Technology Services through the Customer Support Desk at 212-435-7469. The E-Mail Group provides additional support as needed.

10.6.4 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.

10.6.5 Data Security Considerations

Data residing on a BlackBerry device can be easily browsed by anyone having possession of the device. Users should activate the password security available on the device, and carefully consider what type of information they store on their devices. Extreme caution should be taken when using company confidential data on the devices.

10.6.6 Data Backup

Though it doesn't 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 2 -- 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)

12. Indicate time frames in which essential operational/business functions must be resumed.

13. 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

14. 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

responsibility for updating and communicating BRP changes

frequency of review/update

Appendix 3 -- 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 TSD 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 FM200.
- 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 19” W/72” H cabinets or 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 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 trouble-shooting and vendor support.
- m) All communications equipment and cabinets must have ample room for easy access and proper ventilation.

Appendix 4 -- Cabling

- a) Teflon-coated cables should 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 5 -- Port Authority Unified Wiring Plan

Original: 01/90
8th Revision: 03/02

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				
	Horizontal		Patch	
Frequency MHz	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)*
Conductor diameter-in. (mm)	.020 (0.52)	020 (0.52)	024 (0.61)
Cable diameter-in. (mm)	.195 (5.0)	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)	1.0 (25.4)	1.0 (25.4)	1.0 (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	72% nom. Non Plenum	72% nom.
Propagation	72% nom. Plenum	
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 degrees C
Pair 2	White/Orange	Orange	Operation	-10 degrees C to +60 degrees C
Pair 3	White/Green	Green		
Pair 4	White/Brown	Brown		

Appendix 6 -- Telephone Closet / IDF Termination Blocks

Lateral Data cabling serving each workstation will be terminated on a CAT5e patch panel (RJ45 face, 110 punch rear) in the telephone closet. For 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 the TIA/EIA-568-B.2 standard. The patch panel shall have a swing away faceplate or rack mountable.

NOTE: The Category 5e patch panel should be equivalent to the AMP SL series 110Connect Category 5e patch panel. The number of ports may vary.

Each workstation will be assigned a unique station identification number.

Appendix 7 -- Workstation Jacks

Workstations will be equipped with various components of the AMP Communications Outlet system (AMP equivalent can be used with TSD 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 and four modular data connectors, maintaining the integrity of category 5e 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 appropriately labeled.

Appendix 8 -- Standard Switches Inside the Department

Any switches in the following Cisco series are acceptable (Vendors will consult with the Technology Services Department (TSD) 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 4507 series – high capacity – New

Appendix 9 -- Desktop 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:

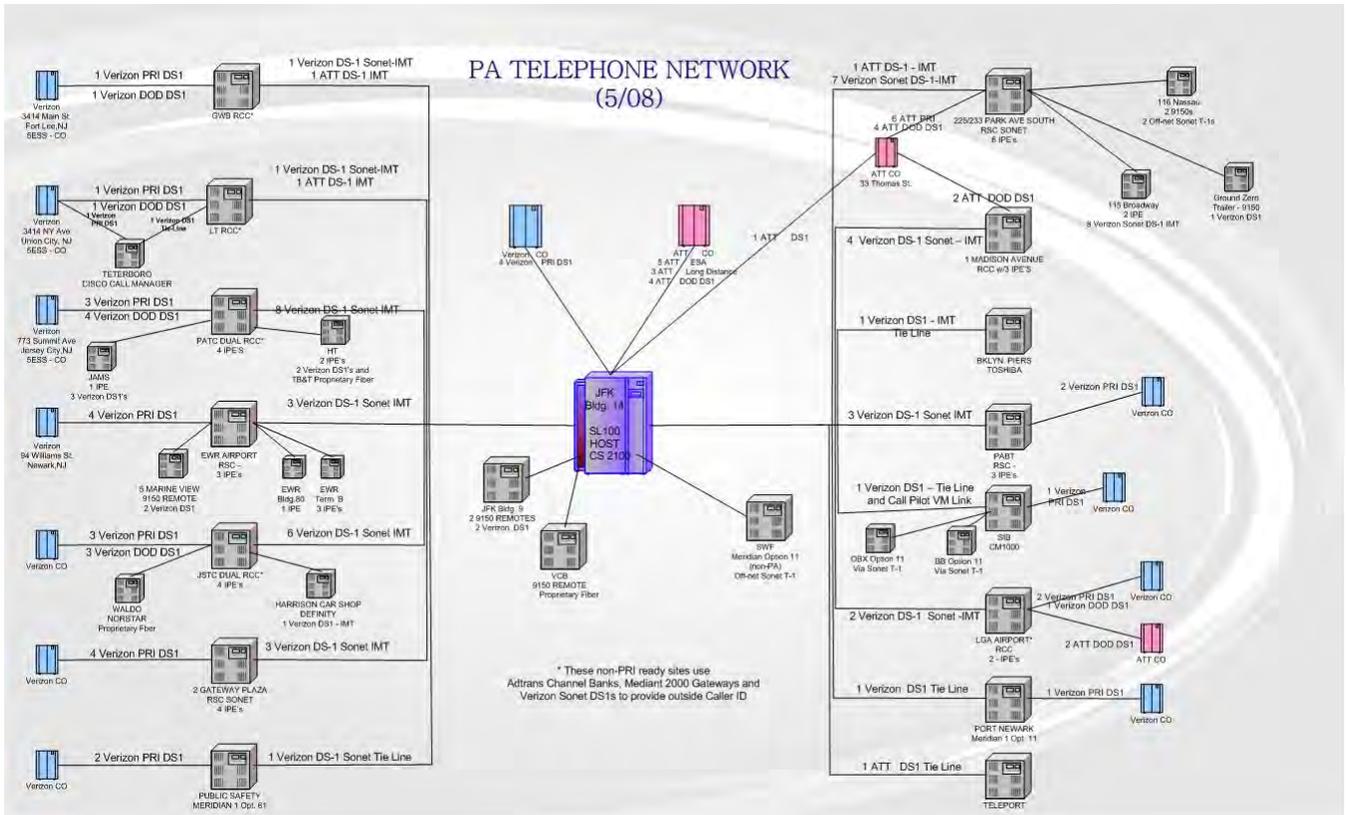
1 - Room number or department name (acronyms are acceptable).

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 10 – PA TELEPHONE NETWORK 5/08



Appendix 11 -- Fiber Optic Specifications 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 will be loose tube, gel filled, with aramid yarn water block:
 - a. Multimode Fiber – **50/125*** micron diameter. Manufacturer of cable TBD
6. Fiber optic cable attenuation from the factory, before installation, shall not exceed:
 - a. For multimode – 3.5 db per km @ 850nm / 1.0 db per km @ 1300nm
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.
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).

*50/125 micron fiber has been chosen over 62.5/125 micron fiber by Network Services:

1. Greater speeds achieved. 62.5/125 fiber will deliver 1 gigabit per second (Gbps). 50/125 fiber will deliver up to 10 Gbps. This allows for equipment upgradeability.
2. Greater distances. 62.5/125 fiber will go up to 275 meters from source. 50/125 will achieve up to 550 meters from source. We can cover greater distances in an installation without having to go to the more expensive single mode fiber installation.

****SC** connectors have been chosen over **ST** connectors by Network Services due to the fact that we utilize Cisco equipment, which come furnished with **SC** connectors on their fiber interface blades. It is more cost effective to use the standard **SC-SC** patch cable with Cisco equipment than to add the additional cost of having hybrid **SC-ST** cables made. **SC** connectors are also easier to work with and use less space in an installation.

Appendix 12 -- Public Telephone Ordering Guidelines

Technology Services (TSD) staff 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. The names and contact numbers are listed below

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 should be coordinated through Marion Resnick 212-435-3251 for sites in 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 contact Marion Resnick of Technology Services. She will review the request and coordinate with GTL-the public telephone permittee and the facility or the tenant.

Facility:	TSD
Contact:	Marion Resnick
Telephone #:	212-435-3251
Fax #:	212-435-3363

Facility: GTL
Contact: Lou Pasquarella
Telephone #: 732-566-7554
Fax #: 732-566-7449

Facility: GTL Operations
Contact: Ben Wurzel
Telephone #: 718-289-9775
Fax #: 718-289-9733

Facility: GTL Operations
Contact: Henry Penna
Telephone #: 718-289-9734
Fax #: 718-289-9733

Appendix 13 -- PAWANET Services Connection Policy

PAWANET SERVICES & REQUIREMENTS

POLICY:

All communications for access to the Port Authority's Agency wide resources will be conducted over the centrally managed and administered Port Authority Wide Area Network (PAWANET). This includes but is not limited to; access to SAP, People Soft, Outlook, Internet and file and print servers. In addition, any and all facility based or departmental systems that require email, Internet access, remote access or interdepartmental communications MUST use the Agency's Network, PAWANET.

BACKGROUND

The Port Authority has made and continues to make significant investments in a centralized communications network, PAWANET, which is designed around current Technology Industry best practices and employs well documented Standards and Guidelines to ensure continued good service and interoperability through future growth and changes. PAWANET is designed to accommodate all of the Agency's current and future services in a highly secure and cost effective fashion.

PAWANET offers high performance network architecture that Departmental Business Systems owners can use to provide access to applications within the Agency's network and also to outside users/business partners and organizations. Utilizing PAWANET provides the following services and benefits:

- Business Benefits of PAWANET
 - High network availability
 - Data availability
 - Network and application design and review
 - Business continuity planning and services
 - Remote Access methods for outside personnel
 - Messaging services
 - Hosting services for web enabled applications
 - Monitoring, logging and auditing services
 - Systems administration services
 - Software support services

- Professional staff organized for appropriate separation of duties
- Server and client maintenance services
- Flexibility for growth, enhanced applications and organizational change
- Capacity planning services (network, applications)
- 7x24 Help Desk
- Local Desktop Support
- Security Benefits of PAWANET
 - Centrally managed security architecture
 - Cyber security technology
 - Firewalls
 - Intrusion detection
 - Virus protection
 - Local and Wide Area Network security
 - Software patching and vulnerability detection
 - Spyware detection
 - Spam protection
 - Encryption technologies
 - Strong user authentication and identity management services
 - Single Sign-On
 - Role-Based authentication
 - Password Synchronization
 - User directory integration
 - Secure physical infrastructure
 - Monitoring, logging and auditing services

This architecture has been deployed because most application business owners cannot provide the equivalent level of security and services on an individual application basis.

SYSTEMS WHICH BENEFIT FROM A SINGLE NETWORK

All Business owners can utilize the services discussed above but Business Applications with the following characteristics derive significant benefits from a single network. Systems which:

- Are located in multiple facilities
- Can be configured for high-availability/redundancy
- Have End Users who are currently or expected in the future to be located in any of the PA facilities (examples would include users with viewing and reporting capabilities)
- Require Consolidated/Agency wide reporting
- Require significant physical security/backups of data
- Are likely to increase in size, number of users and have a number of facilities over time
- Require secure interfaces with outside organizations via dedicated lines or Internet connectivity
- Will be connecting to multiple outside parties via dedicated communication links or Internet connectivity (ex. Transcom, EZ-Pass)
- Are likely to have large increases in transmission requirements over time
- Require monitoring/alerting for system maintenance and operating personnel
- Are likely to benefit from automated software distribution and updating (ex. client machines which require software upgrades and are not web based)
- Are capable of running on a shared/consolidated server environment (application, database, web server)
- Require significant remote management from non-local vendors

COMPLIANCE PROCESS

Before connecting devices to PAWANET, Business Systems owners and end users must ensure that such devices are in compliance with the PA Standards and Guidelines found on eNet.

PAWANET “Rules of Connections”

1. Users must submit a Service Request Form to the Technology Services Department (TSD for connecting standard / authorized end-point devices such as desktops, notebooks, workstations, and printers.
2. Users must submit a Design Request Form to TSD for servers or devices designed to provide file & print, applications (including Web, Video), software or other types of access services.

3. Users may not extend or modify a secured network in any way by installing devices such as repeaters, bridges, switches, routers, gateways, wireless access points, or permanent hubs.
4. Users must use network services provided by TSD and not attempt to provision network services such as IP (Internet Protocol) address assignment (i.e. DHCP (Dynamic Host Communications Protocol) servers), DNS (Domain Naming System), or other IT (Information Technology) infrastructure and management services.
5. Any piece of equipment that is found in violation of this policy may be subject to immediate disconnection from the network and the owner/operator may be held liable for an infraction of the Computing Resource Policy.

Appendix 14 -- PAWANET Services Summary

Service Name

High availability network services

High bandwidth capacity for current and future applications

Route Diversification with multiple high-speed data communications between facilities

Real time Network monitoring and alerting - 7x24 - from network devices to end-point devices

Capacity planning

Network equipment purchasing and maintenance to agreed upon SLA (4 hour)

Network utilization reporting

High Availability Internet Services through multiple service provided on an "on-demand" basis

Dual Network Operations Centers in New York and New Jersey

Redundant electricity (Redundant N+1 design of uninterruptible power supplies)

Redundant stand-by generator power supplies, in the event of a power failure from commercial power

Data availability

High availability and capacity Data with cross facility data replication

File and print services to provide secure centralized storage of client machine data

Secure physical infrastructure

State of the Industry Data Center which provides 24x7 facility security, staffing, environmental controls

Fire Detection and Prevention Systems
Fire Suppression Systems
Video Surveillance (Indoor and Outdoor)
Environmental monitoring (humidity, temperature, smoke, fire)
Network equipment in locked cabinets with tamper switches
Application servers in locked cabinets with tamper switches
Proximity card access control

Network and application design and review

Pre-Requirements Design Assistance
Requirements and Selection Assistance
Pre-Implementation Review Services
Post-Implementation Review Services

Business continuity planning and services

Backup/Restore Services and Storage Area Networks for high capacity data storage ensuring enterprise-wide data and application availability at lower cost
Offsite Disaster Recovery services are available utilizing our existing relationship with an outsourced leader in disaster recovery
Battery Backup (UPS)

Centrally managed security services and architectures

Multi Layered Security Architecture - Security not compromised by single vulnerability
DMZ environment separating internet facing services from back office servers

Firewall and access control with separation of duties
Intrusion Detection (Network Based)
Intrusion Detection (Host based)
Virus Protection (Server and Client) with expedited and automated protection
Virus Protection (E-Mail) through Outsourced E-mail services and 3rd Party Virus Filtering Services
Spam Protection (E-Mail) through Outsourced E-mail services and 3rd Party Spam Filtering Services
Centralized auditing and logging of server/OS activity
Industry recognized operating system and application lock downs
OS Vulnerability testing
Intra-agency Encryption (VPN) services
Vulnerability scanning of network, servers and clients
Automated Patch management for Servers
Automated Patch management for client machines
Layered security methodology and technology which protects Agency assets and which relies on no single security control to defend against emerging threats
Secure encrypted transmissions to outside organizations
Network Time Stamp Services From National Atomic Time-Clocks
Coordinated and Timely responses to alerts, intrusion incidents
Directory Names Services (DNS) - Within PA Network
Network Security - Network Address Translation for masking the internal IP address from the Internet
Network Security - Access lists configured on all edge routers
Network Security - Project specific VLANs can be implemented

Strong user authentication and identity management services

Identity Management - Automated and expedited User Provisioning/Revocation of User Rights

Single sign-on Services

Directory services, integration and synchronization between Active Directory and Novell and a unified identity management repository

Password synchronization

Identity and Role Based Access Control

Multi-form factor authentication solutions (tokens, smart card, biometric) for high security, auditing and reporting

Remote access methods for outside personnel

Unified secure encrypted web portal access via I-Chain architecture

Remote access and secure support and tools via Citrix/VPN or other thin client methods

Messaging services

E-mail services and alert routing via corporate e-mail system and SNMP servers

Blackberry and other paging services available

Hosting Services for Web Enabled Applications

Intranet (E-Net) enabled applications

Extranet (I-Chain) enabled applications

Internet hosted environment through Outside Vendor

Domain name registration and management for the Internet

Monitoring, logging and auditing Services

Server monitoring with alert message creation

E-mail forwarding services to end users, systems administrators and outside parties

Centralized auditing control, logging and reporting services

Asset management and reporting

Systems Administration Services

Outsourced services which ensure SA availability at all times

Servers and desktops configured and maintained following industry best practices and following PA Standards and Guidelines and other recognized best practices methodologies

Servers configured with self diagnostic and automated reporting tools

All servers are properly secured and managed

Software Support Services

Hardware and Software Inventory services

Automated software upgrade and maintenance

Automated patch management services for operating system and application patches

In-depth and broad knowledge in major software products

Database Support and Security Services

Professional staff organized for appropriate separation of duties

Trained professionals who are expert in each area of network services

7x24 Help Desk support with agreed to Service Levels

Operational responsibility for networks separate from computer operations

Server and client maintenance services

Consolidated database servers
Consolidated web servers
Consolidated application servers

Flexibility for growth, enhanced applications and organizational change

Network Design Services - to optimize application performance and minimize Total Cost of Ownership to Business System Owner

Existing PAWANET presence at all facilities allows new systems to be attached at a lower incremental cost.

Total Number of Services Available = 91

General Index

Administrator, 18, 19, 23, 27, 28, 29, 31, 33, 34, 36, 46, 50, 53, 55
 AT&T, 9, 11, 56, 59, 70
 ATM Cisco View, 13
 ATMs, 9, 11, 12, 13, 78
 Browsers, 41
 Business Resumption Plan, 26, 29, 79
 Document Format, 79
 Cabling, 14, 25, 29, 82
 Change Management, 26, 27
 Cisco, 9, 12, 13, 21, 64, 85
 Cisco Strataview Plus, 13
 Cisco Works, 13
 Closed Circuit TV, 9, 11, 61
 ColdFusion, 42
 Communication Room, 29, 81
 Computer Aided Design, 25
 Computing Resources Policy, 37, 51
 Comsoft Telephone Reports, 58
 Databases, 25, 42, 55, 80
 Dreamweaver, 42
 Drive Mappings, 16, 47
 Electrical Requirements
 Telecommunications, 30
 Email, 37, 38, 39, 40
 Public Folders, 38, 39, 40
 Remote Access, 18, 20, 21, 40, 53
 eNet, 8, 21, 27, 32, 36, 38, 41, 42, 43, 70, 73
 Development, 41
 Software, 41
 Enterprise Software, 48
 Escalation Procedures, 50
 File Transfer Program, 53
 Hardware Configuration
 Workstations, 47
 Home Telephone Lines, 58
 HP Open View Network Management, 13
 IDF Termination Blocks, 29, 85
 Information System Security Officer, 33
 Internet Explorer, 41, 47
 Intranet, 8, 9, 38, 41
 Intruder Detection, 15, 19, 36
 Inventory
 Workstations, 46
 IP Addresses, 12, 15, 48, 55
 iPlanet, 42
 IPX Protocol, 15
 IPX/SPX, 12
 Jacks, 29, 85
 Java, 42
 LAN Devices, 14, 17
 Laptops, 14, 35, 64
 Local Service, 11, 56
 Logins, 16, 18, 19
 Concurrent, 19
 MAPI, 39
 Modem Lines, 58
 Modems, 20, 58
 Naming Conventions, 22, 25, 46
 Net8, 55
 Netware, 15
 Network Interface Card, 17, 27
 Networks, 9, 10, 11, 12, 13, 14, 15, 17, 18, 20, 21, 22, 25, 27, 29, 30, 31, 41, 46, 47, 52, 56, 57, 65, 78
 Access, 18
 Connecting LAN Devices, 17
 Enterprise Network, 12, 14, 15, 17, 29
 Intruder Detection, 19

- Logins, 19
- Monitoring Software, 12
- Naming Conventions, 22
- Operating Systems, 17, 52
- Security, 15
- Nodes, 9, 78
- Nortel SL100, 56, 57, 58, 86
- Operating Systems, 15, 17, 25, 46, 52, 55, 71
- Oracle, 42, 55
- OS/390, 55
- Paging, 68
- Paging Devices, 68
- Partition, 15
- Passwords, 19, 20, 38, 58
- PDA's, 35, 63, 65, 71, 72, 73
- PeopleSoft, 9, 11, 48
 - Workstation Client (PeopleTools), 48
- PeopleTools, 48
- Port Authority Wide Area Network (PAWANET), 9, 10, 11, 12, 14, 17, 20, 23, 30, 41
 - ATM Node Assignments, 9, 11, 12, 13, 78
 - Diagram, 10, 56
 - Functions, 11
 - Network Monitoring Software, 12
 - Protocols, 12, 15
 - Supported Protocols, 12
 - Switches and Routers, 12, 14, 25, 29, 85
- Printers, 14, 21, 25, 27
- Private Branch Exchanges, 56
- Protocols, 12, 15
- Public Folder, 38, 39, 40
- Public Folders, 38, 39, 40
- Remote Access, 47
- Routers, 12, 14, 25
- SANs, 11, 14, 15, 16, 17, 21, 28
- SAP, 9, 11, 48, 70
- Scanners, 14, 27
- Security, 15, 17, 18, 20, 33, 48, 49, 53, 55, 61, 64, 72, 76, 80
 - Applications, 55
 - Physical Security, 17, 48, 55, 61
- Servers, 14, 15, 16, 17, 21, 22, 25, 28, 30, 39, 40, 42, 52, 53, 55
 - Application, 14
 - Logical Security, 17, 53
 - Names, 15, 22
 - Physical Security, 17, 55
 - Racks, 14
 - Standard Hardware, 21
 - Web, 42
- SNA/SDLC, 12
- Software
 - Workstations, 47
- SQL Servers, 55
- Sun Solaris, 15, 53, 55
- Support Desk, 29, 32, 33, 34, 35, 36, 48, 49, 50, 58, 71, 72
 - Escalation, 50
- Switches, 12, 14, 29, 85
- System Backup and Recovery, 25, 27, 79
 - Logs, 28
 - Scheduling, 28
- System Management, 15, 18, 19, 23, 25, 27, 28, 29, 31, 33, 34, 35, 36, 46, 48, 50, 52, 55
- TCP/IP, 12, 55
- Telecommunications
 - Electrical Requirements, 30

- Standards, 29
- Telecommunications Room, 29
- Telephone Closets, 29, 85
- Telephone Company Interface, 31
- Telephone Help Desk, 58
- Telephone Network, 56, 58, 59
 - Cabling, 14, 25, 29, 82
 - Diagram, 56
- Time Restrictions, 19
- Toll Free (800) Service, 59
- Unified Wiring Plan, 82
- Uninterrupted Power Supply, 15, 30, 81
- Unix*, 53
 - Logical Security**, 53
- User Accounts, 18, 25, 46
 - Creation, 18
 - Security, 18
- Verizon, 11, 56, 57, 58, 70
- Videoconferencing, 11
- Virus, 34, 36
 - Protection, 15, 25, 35
 - Scanning, 32
- Virus Response Team, 26, 32, 33, 34, 35, 36
- Voice Mail, 58
- VShield, 47
- Wide Area Network, 9, 11, 12, 15, 20, 46, 62, 64
- Windows 2000, 15, 47, 52
- Windows NT, 15, 18, 38, 47, 52, 53
- Windows Server, 52, 53
- Wiring Closets, 14
- Workstation
 - User Accounts, 25, 46
- Workstations, 14, 16, 25, 29, 35, 46, 47, 48, 50, 85
 - Computing Resources Policy, 37, 51
 - Drive Mapping, 16, 47
 - Enterprise Software, 48
 - Enterprise Software (Peoplesoft Client), 48
 - Hardware Configuration, 47
 - Inventory, 46
 - Jacks, 29, 85
 - Naming Conventions, 46
 - Remote Access, 47
 - Security, 17, 48, 55, 61
 - Standard Software, 47
 - User Accounts, 46

[and Software Standards and Software Standards and Software Standards Standards
and Software Standards Etiquette Hardware Configurations Telephone Service Request
Line](#)

ATTACHMENT F

TECHNICAL REQUIREMENTS - COMPUTER HARDWARE, SOFTWARE AND NETWORKING EQUIPMENT

Overview:

The Port Authority, through the Technology Services Department (TSD), will provide all computing and networking equipment, which will be configured in compliance with the Standards and Guidelines for Port Authority Technology. The primary server(s), active active, and/or applications software will be installed and managed by TSD in the Port Authority Telecenter data center and the active-backup server(s) and/or applications software, if required by contract, will be installed and managed in a different Port Authority data/control center. Additional server(s) and/or applications software will be installed and managed by TSD in a Port Authority "Integration and Test" environment. All computing and networking equipment will comply with the Standards and Guidelines for Port Authority Technology, unless written approval is received from the Technology Services Department.

Design:

The Contractor shall identify its computing and communications requirements (i.e. performance needs, operating system platform, bandwidth, etcetera), which shall be in compliance with the Standards and Guidelines for Port Authority Technology, and the Technology Services Department (TSD) will design the computer equipment and network to meet the Contractors stated requirements and the requirements stated in the contract (i.e. number of workstations, availability, level of fault tolerance, bandwidth, etcetera).

Procurement:

a. Production Equipment

TSD will furnish all workstations, servers, laptop computers and networking equipment that will be installed on Port Authority property and connected to the Port Authority Wide Area Network, which will be configured for compliance with the Standards and Guidelines for Port Authority Technology. The standard for communications equipment is Cisco. The standard for File & Print is IBM servers. The standard for Application and Database servers are IBM servers and NEC FT servers for 99.999% availability. The standard for virtualization software is VMware Esxi/vSphere on both IBM and NEC servers. The standard for Workstations include the following models (check with TSD for current models):

- Lenovo ThinkCentre "M" series for a desktop personal computer
- Lenovo ThinkStation "D" model for a CAD workstation
- Lenovo ThinkPad "X" series for laptop computers
- Panasonic Tough Book "CF" series laptops

b. Contractor Equipment

The Contractor shall ensure that the equipment used to test the software in their facilities complies with the Standards and Guidelines for Port Authority Technology to avoid any problems with the installation of the applications software on the Port Authority equipment.

Installation and Location of Computing and Communications Equipment:

TSD will install the computing and communications equipment in the managed data centers and Authority facilities as required by the application.

Installation and Testing of Application Software:

Once the Contractor has completed its application development and contractually required factory inspection and testing, it will advise the Authority's project manager that it is ready for the application software to be integrated with the Port Authority Wide Area Network (PAWANET) infrastructure and services, and tested. The Contractor shall also submit procedures for the application software installation and configuration. The Contractor shall ensure that the application software, at the time of delivery, functions properly with the current versions of the operating system, database software and patches.

Under Port Authority supervision, the Contractor shall install and configure its software on the Authority servers in the Integration and Test Environment using the submitted software installation and configuration procedures. Once successfully installed and configured, the Contractor shall test its software to ensure that it works properly and is fully integrated with the Authority's infrastructure.

After the Contractor has demonstrated to its satisfaction that its software is fully functional in the Integration and Test environment and the Authority confirms that all PAWANET services are operating properly, the Contractor shall submit to the project manager a certification that its software is ready for field acceptance testing. The Contractor shall also submit updated procedures for the installation and configuration of the application software.

Upon approval from the project manager, the Contractor shall conduct the field acceptance test of the application software in accordance with the testing requirements specified in the contract documents

Subsequent to the successful testing of the application software in the Authority's Integration and Test environment and approval by the Authority's project manager, the Contractor shall install and configure its application software in the Authority's servers in the production environment under Port Authority supervision using the software installation and configuration procedures submitted by the Contractor and approved by the Port Authority. Once again the Contractor shall demonstrate the proper functioning of the applications software, in accordance with the testing requirements specified in the Contract Documents.

Access to the Production System for Maintenance of the Application Software:

The Contractor will be permitted access to the application software in the production system in order to perform its obligations in accordance with the requirements stated in the Contract Documents and the Maintenance Agreement. If it becomes necessary to physically access the production system, arrangements will be made through the Technology Services Department for the Contractor to access the production system under the Authority's supervision. The Contractor shall also be permitted limited access to the application software in the production system through the Authority's Remote Access Solution.

System Administration:

The Port Authority's Systems Administrator will maintain the operating system and all Port

Authority furnished and installed security and monitoring software on the servers, workstations and laptop computers, and perform all system administration functions.

Database Administration:

The Port Authority's Database Administrator will maintain the database and perform all database administration functions.

Maintenance of Port Authority furnished and installed servers, workstations, laptop computers and networking equipment:

The Port Authority will monitor and maintain all Port Authority furnished and installed servers, workstations, laptop computers and networking equipment.

Typical Windows 2003-32/64-bit and 2008-64bit Server Build (See Notes 1 & 2)

- Windows 2003 Server SP-2, Windows 2008 Enterprise R2
- McAfee Virus Scan 8.5.i Enterprise Edition (8.5.0.781)
- Lumension Patchlink
- IBM Director Agent
- IBM Director Agent System Availability Tool
- FDR/Upstream V3.5.0C Client
- NetVision Agent
- IBM Internet Security Systems RealSecure® Server Sensor
- MyODBC 4.0.20 Client (if required)
- Internet Information Server (if required)

Note 1: Typical build is subject to change

Note 2: Special Contractor and project requirements can be discussed with TSD during the equipment design

Typical Windows XP Desktop Build (See Notes 1 & 2)

- Windows XP SP3 _____
- Microsoft Office 2007 Pro _____ 12.0.6313.5000
- Adobe Acrobat Reader _____ 9.3.0
- IBM RECORD Now _____ 7.0
- Internet Explorer _____ 7.0.5730 SP2
- InterVideo WinDVD DVD Player _____ 5.0.11.141
- Java 2 RTE Standard _____ 1.5.0_100, 1.4.2.05, 1.4.2.06, 1.6.03
- Lan WorkPlace Pro _____ 5.2
- Adobe Flash _____ 10.0.45.2
- Microsoft .Net Framework _____ 1.0 SP3, 1.1 SP1, 3.5 SP1
- Microsoft Office Professional Edition 2003 Compatibility Pack for the 2007 Office System
- NICI _____ 2.7.0-2
- NMAS Client _____ 3.1
- Novell Client 32 _____ 4.9.1SP4 (4.91.4.20070720)
- Novell iPrint Client _____ 4.26.00

- Novell Nsure SecureLogin _____ 3.51.101
- Lumension Patchlink _____ 6.4.2.378
- QuickTime Player _____ 7.6
- Windows Installer _____ 4.5 KB942288-V3
- Windows Media Player _____ 11.0.5721.5.145
- McAfee VirusScan Enterprise _____ 8.5.0.781
- WinZip _____ 9.0 SR1 (6224)
- ZenWorks Desktop Management Agent _____ 6.5.200.50909

Note 1: Typical build is subject to change

Note 2: Special Contractor and project requirements can be discussed with TSD during the equipment design

Safeguarding Data:

All information concerning the business of the Authority which becomes accessible, or known, to the Contractor, their 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 magnetic 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 provide the same care and processes to prevent unauthorized access, modification, theft or other loss of the Authority data via the same, or enhanced, processes that it presently employs 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 will provide immediate notification to the Authority’s Contract manager. In addition, the Contractor will be held liable for damages or expense to the Authority, 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.

Secure Access to the Software Applications:

In order to maintain confidentiality of sensitive information, security provisions must be employed in the System. These include data access limitation by password and permission, maintenance of audit controls and security violation reporting. Only the assigned Port authority user may have control of the assignment, removal or reinstatement of a user. Any changes must be audited. When a database is part of the solution the Vendor may not have access to the data but can be given read access of data when approved by the Port Authority. The access is removed once the Vendor has completed their work. All passwords must be encrypted and any traffic going over the air or across a network must be encrypted. Passwords must be changed at set expiration times and account lockout of accounts for three or more tries.

ATTACHMENT G

AUDIT CONTROLS CHECKLISTS

19 ATTACHMENT I: IT CONTROL REQUIREMENTS

I. Application Controls Checklist

II. Control Security Requirements

III. Disaster Recovery Plan Checklist

IV. Security Administration Function

V, Security Requirement

VI. System Administration & Operation Manual Requirements

VII. Web-Based Application Checklist

19.1 I. APPLICATION CHECKLIST:

19.1.1 A. General

- Overview of the application, what the function is, who uses the application, and where it is physically located.
- Documented procedures, flowcharts and processes maps.
- Physical access to the application hardware should be appropriately restricted.
- If vendor(s) support the application, a vendor contract and service level agreement should be in place. The SLA should have provisions for uptime, performance monitoring, updates, etc.
- The application should have the PA's warning banner on the login screen.
- Remote access should be restricted and documented in accordance with PA policy.
- Determine what form of output is possible through the application.

19.1.2 B. Hardening of operating system/database that supports the application:

- Disable unnecessary ports/services.
- Remove all samples from the box.
- Change all default passwords; delete all default content and scripts.
- Limit user account 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.
- Follow PA password standards (90-day expiration, lockout after 3 incorrect password attempts, concurrent logins, 6 alphanumeric characters)
- Set "automatic session timeout" to 15 minutes of inactivity and require user to log back in with a valid ID and password.
- Implement access control at the database level (i.e. user roles and permissions, passwords, secure links)
- Apply all new patches and fixes to operating system and application software for security.
- 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.

19.1.3 C. 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.

19.1.4 D. Logical Access Controls

- Procedures to grant/revoke access should be documented.
- Access request forms for adding/modifying/deleting users should be used.
- 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
- Ensure that password controls for the application are consistent with PA requirements
 - Passwords must be at least 8 alphanumeric characters long
 - Passwords must be changed every 90 days
 - Passwords must not be shared
 - User ID accounts should be locked after a three logon failures.
- 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.
- Each user has a unique user ID.
- Should have a segregation of duties/roles.
 - Roles are setup with least access required to perform job responsibilities.

19.1.5 E. Application Controls

19.1.5.1 E.1 Data Validation & Input Controls

- The application should have input controls to verify the validity of the data entered.

19.1.5.2 E.2 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.
 - Sensitive data like credit card #s and social security #s should be encrypted.

19.1.5.3 E.3 Application Interfaces

- Interface file should be secured and archived.
- Reconciliation of data should be done on a batch record and totals. Detail data reconciliations should be completed on periodic basis.

19.1.5.4 E.4 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.

19.1.5.5 E.5 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.

19.1.5.6 E.6 Application Logging, Audit Trails and Record Retention

- 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.

20

20.1 System Management and Support

20.1.1 F. Management Reporting

- Management reporting should be produced through the application.
- Transaction logs should be maintained.

20.1.2 G. Contingency Planning, Disaster Recovery and Backup Management

- A Business contingency plan and a disaster recovery plan for the application should be documented.
- Plans should be tested and the outcomes of the tests (success/failure) should be documented.
- Backup copies of these plans should be stored off-site.
- Backup procedures should be documented and 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.

20.1.3 H. 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).
- There should be SLA and /or requirement with the vendor for “uptime”.

20.2 II. CONTROL SECURITY REQUIREMENTS

20.2.1 A. System Configuration

- Default accounts are secured/locked/or removed.
- Public and Guest accounts/profiles should be removed or secured with no access.
- Controlled use of administrative accounts.
- Limited assignment of administrative privileges and roles.
- Access violation reports.
- Audit trails for operating, application and database systems

- Not display last user who signed on
- No use of login scripts for accounts.
- LDAP compliant
- Encryption of data in storage and transmission of data via the network.
- Unnecessary services removed and/or disabled.
- Secured and approved remote access strategy.
- Data archiving in place.
- Data Retention Policy and Procedures in place.
- Requirement for user name and password
- System timeout for inactivity set to 15 minutes.
- All default settings or passwords changed.
- Test facility which replicates the production system.
- Patching up to date. Patch Management Procedures and documentation includes testing.
- Virus software implemented and up to date.

20.2.2 B. Physical Protection

- Appropriate fire suppression systems in place.
- Temperature and humidity monitoring.
- Environmental condition adequately controlled (no water, dirt, clutter) and monitored.
- Physical access secured by single authentication mechanism i.e. swipe card.
- Physical security adequate for equipment (locked cabinets).
- Security cameras installed in sensitive areas.
- Power surge protection and emergency power backup are in place.

20.2.3 C. Backup (

- Backup data maintained off-site
- System backup is encrypted.
- Full system backups exist.
- Backup tapes are tested periodically.

20.2.4 D. Access Controls

- Background checks are performed on all personnel as appropriate.
- Account expiration for contractors and consultants
- Account password is not the same as account name
- No concurrent login capabilities
- No accounts assigned to individuals who no longer require the account
- Default accounts are locked or secured.
- Accounts never logged into are removed.
- Accounts adequately identify the user – no generic accounts.
- Accounts not used by multiple individuals
- Administrator account passwords adequately secured.
- Disabled accounts are deleted.
- No test accounts on production.
- No generic accounts

- No excessive privileges on accounts – least privilege granted.
- Guest accounts are removed
- Inactive accounts are removed
- Review of profiles, access levels, privileges
- Access reports by user and privilege
- All user account profile should include Employee ID number and full user name.
- Assigned Security Administrator
- Baseline tools or security products are implemented on a quarterly basis.
- Adequate network zoning
- Adequate performance monitoring
- Intrusion Detection System in place
- Secured and authorized remote access
- Firewalls in place
- Warning message/banner
- No modems (dial up or wireless)

20.2.5 E. Password Controls

- Password encryption enabled.
- Password uniqueness functions enabled.
- Passwords expire every ninety days.
- Forced password change at initial log on.
- Passwords set for a minimum of six characters, combination of letters, numbers, and special characters.
- Retention of unsuccessful login attempts and length of account lockout time set to PA standards.
- Password dictionaries
- Account lockout function enabled and set according to standards.
- Password age in compliance with PA standards

20.2.6 F. Documentation / Procedures

- Security Administration Procedures documented
- Procedure for granting, modifying or deleting access to the system are documented
- Access request forms authorized
- Access request forms retained
- Access request forms are used to assign access
- Change Management procedures documented
- Test results documented
- Backup, restart and recovery procedures documented
- Disaster Recovery Plans and Business Resumption Plans documented and comprehensive.
- Documentation is current for System Manuals, Operating Instructions
- Documentation is up to date for Firewall rule sets.
- Inventory listings of equipment and software.
- Adequate training
- Password reset procedures controlled (Help desk function)

- System Administration procedures documented
- Data retention and archiving procedures documented
- Roles and Responsibilities defined and documented
- Virus Patch Management procedures documented
- Batch and Interface Management procedures documented
- Patch Management procedure documented
- Escalation procedures documented
- Incident Response procedures documented
- Incident and Error logging/tracking.
- Topologies exist and are up to date (system/network diagrams)
- System monitoring/performance
- Log reviews
- Management reporting – like Access Reports, Exception transaction reporting

20.3 III. DISASTER RECOVERY 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 (Not Applicable)
- 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 affect 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 (Not Applicable)

- 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 (Not Applicable)

- Supplemental Hardware/Software Inventory

5. Escalation Plans and Decision Points (Not Applicable)

6. Disaster Recovery Emergency Procedures (Not Applicable)

- 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 semiannually 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. (Not Applicable)

- Recovery Management
- Damage Assessment and Salvage
- Hardware Installation

8. Contacts information - This area should be reviewed semi-annually for updates and changes. (Not Applicable)

- 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. (Not Applicable)

20.4 IV. SECURITY ADMINISTRATION FUNCTION

Responsible for:

- ◆ Establishment of access rights, groups, profiles etc. for a system or application for which they are responsible and documenting their use and definitions. **(Applicable)**
- ◆ The development of security procedures which define the granting of access and the administration of security functions of their system or application. The ongoing review and update of these security procedures. **(Applicable)**
- ◆ Responsible for the development of add/change/delete access requests forms.
- ◆ The development of procedures for changing or deleting accounts or privileges when staff leave or change assignments. Execution of these procedures in a timely manner.
- ◆ Regular review of who has access to their data and determining if it is appropriate and still required.
- ◆ Ensuring that users are required to acknowledge, in writing, that they have been informed of the organization’s position on security and confidentiality of information prior to access being given.

- ◆ Assigning appropriate expiration dates for accounts used by temporary/consulting staff.
- ◆ The development of procedures for responding to, documenting and escalating security incidents.
- ◆ The investigation and appropriate escalation of a security incident matter.
- ◆ Setting any global system or application controls (i.e. password controls, time out, concurrent logins) consistent with the Port Authority Technology Standard and Guidelines.
- ◆ Restricting remote access and monitoring and reviewing the activity log. (Limit or no use of modems. Modems should be configured according to the Port Authority Technology Standard and Guidelines a certified by the Information Systems Security Officer.)
- ◆ Development and review of reports such as Kane Security Analyst, ISS or ESM to monitor areas of security exposure.
- ◆ Daily event log reviews for irregular activities and security violations.
- ◆ Keeps management and the business unit informed on security issues.
- ◆ Development of regular processing schedules for the production of security reports i.e. unsuccessful logon attempts, audit trail reports.
- ◆ Development of procedures for reviewing the reports and logs on a regular basis and taking appropriate corrective action.
- ◆ Responsible for ensuring that the system complies with the Port Authority Technology Standard and Guidelines.
- ◆ Determining high-risk activities, establishing logs of those activities and tables and determining appropriate review cycles.
- ◆ Ensuring that operating system, database system and application security issues are coordinated.
- ◆ Keeping abreast of vulnerabilities of systems, databases, or application as they are discovered and patching them or implementing compensation controls.
- ◆ Development of procedures for the disposal of unneeded confidential data produced from the application.
- ◆ Ensure all system hardware (i.e. servers, comm. rooms, backup tapes, etc.) and software are secured from tampering or damaging.
- ◆ Ensure that operating systems at a minimum complies with the Distributed Systems Environment in the Port Authority Technology Standard and Guidelines and industry standards.
- ◆ Document a virus protection and recovery plan.
- ◆ Firewall Administration, Firewall configuration, rules, logs, and patches
- ◆ Intrusion Detection System Administration, monitoring network traffic across the firewall and in the DMZ.
- ◆ Router and Switches Administration, configuration file, backups, patches, and change controls.

20.5 V. SECURITY REQUIREMENT

Network architecture

Diagram

Router and Switch Configurations

Firewall Configuration

IDS Nodes and System Signatures

Alerts and Logs
Failover & Redundancy
UNIX
Administration
Port and Services (unnecessary)
Utilities (unnecessary)
Access Rights/ Segregation of Duties
Redundancy / Data Replication
System Log & Violation Logs
Root
Vulnerability Scanner
Windows
Administration
Services and Ports (unnecessary)
Utilities (unnecessary)
Access Rights/ Segregation of Duties
Patches
System Log, Audit Trails & Violation Logs
IIS
Administrator & Guest
Vulnerability Scanner
Oracle
Administration
Services (unnecessary)
Utilities (unnecessary)
Access Rights/ Segregation of Duties
Redundancy / Data Replication
Audit Trail and Triggers
Sys, System, Internal
Vulnerability Scanner
System Administration
Batch Management & Processing
System Monitoring (HP Open View & SNMP)
Vulnerability Software & Baseline Tools (i.e. ISS & Tripewire)
Patch Management (Proactive)
Virus Management
Instance Management
Performance Monitoring
Change Control - System, Application
Web Logic & XML
SSL certificates (HTTPS)
Key Generation & Management – Smart Card
Access Rights/ Segregation of Duties
Audit Trails & Violation Logs
Java, SSL, Web Logic Patch Management
Remote Access

Security

Authentication and Integrity

Blue Ridge – VPN

IBM Mail Box

PA Approval via TSD (MF)

Security Administration

Review of Audit Trails and Violation Logs

Documentation

System Administration Manuals

Security Administration Manuals

User Manuals

General

Login Banner

Physical Security

System Defaults

Authentication & Password Controls (90 day exp., 15 min. timeout, 3 attempts, concurrent logins, 6 alpha numeric)

Escalation Procedures

Incident Response Procedures

Archiving

Backup and Recovery

Disaster Recovery (Plan & Testing)

Business Resumption (Plan & Testing)

Software Inventory

Hardware Inventory

Account Expiration for Consultants and Contractors

Vulnerability Scanner

20.6 VI. SYSTEM ADMINISTRATION & OPERATION MANUAL REQUIREMENTS

20.6.1 A. General Information

1) Server name

a) IP address

b) Location

c) Operating system – version, patch level

d) Database – version, patch level

e) Application

2) LDAP and Domain Controller Configuration

3) Diagrams

a) Network topology

b) Application flowcharts

20.6.2 B. System

4) System Configuration

5) System Applications and Services

6) Network Time Synchronization

7) Patch Management

a) Normal and Emergency Procedures

8) System Schedule

a) System downtime

- b) System backups
- c) System batch processing

20.6.3 C. Access Controls

- 9) Roles / Profiles (Access Control List)
 - a) List of ACLs
 - b) Creation and updates to ACL
 - c) Testing and Approval of ACL
- 10) Granting and Revoking User Access
 - a) Access Request Forms
- 11) User Accounts and Access Reports
 - a) Generating Reports
 - b) Report Distribution and Report Approvals/Reviews

20.6.4 D. Password Controls

- 12) Password Configuration
 - a) Length
 - b) Alpha/numeric
 - c) Password dictionary
 - d) Password age
 - e) Password expiration
- 13) Account Policies
 - a) Concurrent log in
 - b) Vendor/Consultant Account Expiration (usually the length of the contract)

20.6.5 E. Remote Access

- 14) Strategy/Approach
- 15) Approvals

20.6.6 F. Operation

- 16) Administrator(s) roles and responsibilities
 - a) Chart or description
- 17) Startup and Shutdown Server procedures
- 18) Batch processing
 - a) Production runs – list of batch programs with schedules
- 19) Backups
 - a) Schedule – frequency
 - b) Testing of tapes
 - c) Offsite locations
 - i) When picked up
 - ii) Where stored
 - d) Tape encryption
 - i) Each tape and/or disk files should have an external label
 - e) Tape destruction – scratching and disposal of tapes
- 20) Recovery
 - a) Procedures

20.6.7 G. Physical

- 21) Server Location
 - a) Site Security
 - b) Server Mounting

- i) What is the rack configuration and who has access to the keys
- c) Environmental Controls
- i) Humidity and Temperature Monitoring

20.6.8 H. Anti-Virus Management

- 22) Engine and Definition Management
- 23) Emergency Updates
- 24) Remote Distribution Server

20.6.9 I. Change Management

- 25) Testing Environment
- 26) Normal Procedures
- 27) Emergency Procedures
- 28) Requests are documented
- 29) Specific timetables/scheduling are documented
- 30) Documented reason for request and approvals
 - a) name of requester
 - b) phone number and department
 - c) requester's signature
 - d) reason for change
 - e) List of modules that need to be changed
 - f) Supervisor's name
 - g) Supervisor's approval (changes must be approved by someone other than the requester).
- 31) Determine if priorities are assigned to the change requests.
- 32) Budget/costs are communicated to system owner.
- 33) Process used to control and monitor change requests (central repository/ tracking system).

20.6.10 J. Patch Management

- 34) Procedures
 - a) Operating System
 - b) Database
 - c) Application
- 35) Testing
- 36) Approvals
- 37) Remote Distribution

20.6.11 K. Reporting and Monitoring

- 38) System Monitoring
 - a) System Utilization and Performance
 - i) CPU
 - ii) Disk space
 - b) System Response time
- 39) System Reporting –
 - i) Report generation schedule and distribution
 - ii) Review and approval
 - a) System Performance
 - b) Audit Trails
 - c) Violation Reports

20.6.12 L. Problem & Incident Management

- 40) Problem reporting/resolution tracking system

- a) Problems are appropriately logged and prioritized.
- b) Corrective measures are documented.

20.6.13 M. Segregation of Duties

- 41) Developers and or Programmer have no access to the production server.
- 42) OS administrators have no access to the Production database and application.

20.7 VII. WEB-BASED APPLICATION CHECKLIST

20.7.1 A. Web Environment Controls

- Network Architecture:
 - Ensure firewall hides the structure of the internal network.
 - Ensure outside traffic is filtered by the external firewall, and should be allowed to access the DMZ with only those services that are required (i.e. HTTP, HTTPS, FTP)
 - Ensure that all traffic passing between the internal and external networks pass through the DMZ.
 - Intrusion Response Controls Intrusion Detection/Prevention:
 - Use intelligent IDS (intrusion detection system) or IPS (intrusion prevention system) to detect or block DoS (denial of service) attacks.
 - Prepare an intrusion response strategy and document and test policies and procedures to respond to intrusions in a timely manner and eliminate potential errors, and omissions.
- Hardening of Host/Operating System:
 - Disable unnecessary ports/services
 - Remove all sample sites from the box
 - Change all default passwords; delete all default content and scripts.
 - Limit user account access.
 - Follow PA password standards (i.e. 90-day expiration, minimum of 6 alphanumeric characters, lock account after 3 incorrect passwords)
 - Set “automatic session logout” to 15 minutes of inactivity and require user to log back in with a valid ID and password.
 - Implement access control at the database level (i.e. user roles and permissions, passwords, secure links)
 - Apply all new patches and fixes to operating system and application software for security.
 - Use secure and encrypted remote access methods.
 - Log (and monitor) web traffic and trend the activity looking for abnormal activity.
- Directory Structure for Web Server:
 - Use separate directories, partitions or disk locations for web server logs, contents, scripts and other information vs. system directories and user information. In addition, use a single directory exclusively for all programs executed as part of web server content
- Web Server Security Related Configuration Settings
 - Block an IP if there are numerous requests for the URL to prevent a possible attack. (IP scan)

20.8

20.8.1 B. Web Site Management Issue

- Use certificates on the site. So users can confirm they are on the right site.

- A formal “content management” process (and supporting tools) should be in place to provide change controls, approvals, version controls, and security over changes to web site content to prevent unauthorized changes.
- Validate links periodically to identify dead or misdirected links for correction
- Ensure compliance with Payment Card Industry (PCI) Data Security Standard (DSS) Requirements (e.g. Visa, Master Card, etc).
- Systems monitoring should be in place for the server and other relevant devices including the use of automated systems management tools.
- Backups of the website including web server configuration files, static content files, script directories and etc. regularly.
- Secure application, logs, encryption keys, certificates and passwords on the production box. If possible move them to another secured or restrict access to administrators only.
- In the System Development Life Cycle (SDLC), ensure that there are application development and coding standards.
- 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.
- Access Controls:
 - Ensure that separation of duties occur at the two levels of access control for web applications: Functional access controls (URL –based) and Data-level access control (handled within application)
- Password Reset:
 - For internal applications, reset passwords via the helpdesk or security administrator of the site
 - Send forgotten password to known e-mail address or via customer service screens after the user has been validated for customer service application.
- Conduct regular audits, vulnerability testing, security scanners and MD5 hash comparisons of the production site. (MD5 – An algorithm that produces a checksum that is revalidated to detect any modification to sensitive hidden form fields, files, directories, etc.)
- All sensitive or confidential data (including passwords, session IDs for sensitive applications, confidential or sensitive business transactions, etc.) should be transmitted between browser and server within an SSL-encrypted session.

20.8.2 C. Web Application Vulnerabilities and Controls

- Best Practice and Standards:
 - 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
- Sessions IDs:

- Ensure sessions IDs are difficult to spoof/guess.
- Session IDs should be long (at least 30-40 digits for secured applications) and contain alphanumeric characters
- Session IDs should be unique, random and non-predictable.
- Session IDs should expire after a reasonable time limit (1-3 hours) or for inactivity (10-15 minutes)
- Ensure session IDs are negotiated whenever a user crosses a secured boundary (from an unsecured to a secured portion of the site)
- Ensure session IDs are transferred only within an SSL session.
- Cookies:
 - Session cookies should be assigned randomly (non-sequential).
 - Ensure that session cookies/tokens are non-persistent and are not written to a user's browser history or cache. Use a server-based session cookie/token.
 - Ensure session cookies expire and are removed from the server for elapsed time (30 minutes-2 hours) or inactivity (10-15 minutes)
 - Invalidate the session cookie/token on the server when the user logs out or leaves the site.
- Use the Post HTTP Methods to transfer information from the browser to the server.
- Preventing Hacking Reconnaissance:
 - HTTP Status Error Codes should be monitored.
 - Never use default names for directories, (e.g document root, CGI directories, etc.)
 - DNS (Domain Name Services) zone transfer – Ensure default names are changed because these are keywords hackers are searching, (e.g. “gateway”, “firewall”, and “proxy”).
- Store User dependent Data in a Session table:
 - Whenever possible, only the session ID should be stored on the browser and sent with each request
 - All other user-specific and session-specific variables should be stored on the server in a session table.
- Perform data validation & integrity checks for field values and ensure the HTML special characters are stripped for all HTML request.
- At a minimum, applications should strip all (HTML) meta-characters (e.g. <, >, &, etc.), including OS and related SQL meta characters, from user input.
- Restrict the use of the hidden fields.
- Ensure that ID, passwords and system comments are not be included in scripts and pages.
- Ensure the application will not process SQL commands from the user browser
- Do not allow site pages to be cached by user browsers.
- Error Messages:
 - Applications should trap all specific system error messages, especially those from other infrastructure components that reveal information about the application internals.
 - Ensure that only generic messages with little to no information content should be sent to the user's browser.

P.A. Standard Agreement #PAVI-13-***

**SUBJECT: PERFORMANCE OF EXPERT PROFESSIONAL SERVICES -
DEVELOPMENT AND MAINTENANCE OF AN AVIATION FACILITIES
MAPPING SYSTEM**

1. The Port Authority of New York and New Jersey (hereinafter referred to as the "Authority") hereby offers to retain <FIRM NAME> (hereinafter referred to as "the Consultant" or "you") to provide expert professional services for the development and maintenance of an Aviation Facilities Mapping System (FMS) as more fully set forth in Attachment A (including Appendices), which is attached hereto and made a part hereof. The term of the Agreement will be for two (2) years commencing on the date of receipt by you of an executed agreement. The Authority has the sole right to exercise two (2) one (1) year options.

The Authority does not guarantee the ordering of any services under this Agreement and specifically reserves the right, in its sole discretion, to use any person or firm to perform the type of services required hereunder.

The entire Agreement between the parties shall consist of, but may not be limited to, this Standard Agreement and the following attachments, as required:

Contract Specific Terms and Conditions

Appendix 1 – Port Authority Facilities

Attachment A – Scope of Work

Appendix A1 – FMS System Abstract

Appendix A2 - Current System Metrics

Attachment B – Agreement on Terms of Discussion

Attachment C – Company Profile

Attachment D – Cost Proposal

Attachment E – Technology Standards and Guidelines

Attachment F - Technical requirements for computer hardware software and networking equipment

Attachment G – Audit Controls Checklists

In the event of any inconsistency between any of the documents set forth above, the order of precedence shall be as set forth above.

No change in or modification, termination or discharge of this Agreement 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/her duly authorized representative, provided, however, that termination in the manner as described herein expressly provided shall be effective as so provided.

2. This Agreement shall be signed by you and the Authority's Director of Procurement. As used herein and hereafter, the "Director" means the Authority's Director, Aviation Department, acting either personally or through her duly authorized representatives acting within the scope of the particular authority vested in them unless specifically stated to mean acting personally.

For the purposes of this Agreement the Project Manager (or “Manager”) shall be the individual with day-to-day responsibility for managing the project on behalf of the Port Authority. The Project Manager will be assigned.

For the purpose of administering this Agreement, the Director has designated <NAME>, <TITLE>, to act as her duly authorized representative. The Project Manager for this project is <NAME>, at (***) ***-***, or e-mail address *****@panynj.gov.

The Authority reserves the right to extend this Agreement for two (2) additional one (1) year options from the expiration of the original term of this Agreement. Said extension shall be in writing by the Director to the addressee noted above (or addressees as otherwise requested in writing by the Consultant to the Director). A letter extending the Agreement term shall be sent to the Consultant at least thirty (30) days prior to the end of the term.

3. Your services shall be performed as expeditiously as possible and at the time or times required by the Director. Time is of the essence in the performance of all your services under this Agreement.

4. In response to a request for specific services hereunder and prior to the performance of any such services, you shall submit in writing to the Director for approval an estimated cost and staffing analysis of such services to the Authority. Approval of such cost and direction from the Director in writing to proceed shall effectuate the performance of services under this Agreement. After the point at which your expenditures for such services reach such approved estimated cost, you shall not continue to render any such services unless you are specifically authorized in writing to so continue by the Director and you shall submit to her for approval a revised written estimated cost of such services. If no such authorization is issued, the performance of the specifically requested services under this Agreement shall be terminated without further obligation by either of the parties as to services not yet performed, but you shall be compensated as hereinafter provided for services already completed. It is understood, however, that this limitation shall not be construed to entitle you to an amount equal to the approved estimated cost. Preparation of the cost estimate and staffing analysis mentioned in the first sentence of this paragraph shall not be a compensable service hereunder.

5. In order to effectuate the policy of the Authority, the services provided by the Consultant shall comply with all provisions of federal, state, municipal, local and departmental laws, ordinances, rules, regulations, and orders which would affect or control said services if the services were being performed for a private corporation, unless the Authority standard is more stringent, in which case the Authority standard shall be followed, or unless the Consultant shall receive a written notification to the contrary signed by the Director personally, in which case the requirements of said notification shall apply.

6. The Consultant shall meet and consult with Authority staff as requested by the Director in connection with the services to be performed herein. All items to be submitted or prepared by the Consultant hereunder shall be subject to the review of the Director. The Director may disapprove, if in her sole opinion said items are not in accordance with the requirements of this

Agreement, sound engineering principles, or professional standards, or are impractical, uneconomical, or unsuited in any way for the purpose for which the contemplated services are intended. If any of the said items or any portion thereof are so disapproved, the Consultant shall forthwith revise them until they meet the approval of the Director, but the Consultant shall not be compensated under any provision of this Agreement for performance of such revisions. No approval or disapproval or omission to approve or disapprove, however, shall relieve the Consultant of its responsibility under this Agreement to furnish the requested services in accordance with an agreed upon schedule and in accordance with professional standards.

7. You shall not continue to render services under this Agreement after the point at which the total amount to be paid to you hereunder including reimbursable expenses reaches the combined total of each of the approved estimated costs, unless you are specifically authorized in writing to so continue by the Director. If no such authorization is issued, this Agreement shall be terminated without further obligation by either of the parties as to services not yet performed, but you shall be compensated as hereinafter provided for services already completed.

8. The mutually agreed to Cost Proposal (Attachment D) forms a part of this Agreement, and contains the prices/rates to be utilized for the performance of the Services hereunder.

9. As full compensation for all your services and obligations in connection with this Agreement, the Authority will pay you the total of the amounts computed under subparagraphs A, B, C, and D below, subject to the limits on compensation and provisions set forth in paragraphs 4 and 7 above. Subject to the terms and conditions below, travel time is not reimbursable under subparagraphs A, B, and C hereunder.

A. An amount equal to the actual hourly billing rate billed by you for professional and technical personnel times the total number of hours actually spent by said personnel in the performance of services hereunder. No hour of services by an employee shall be compensable hereunder unless the employee is actually paid by you for such services at his/her usual salary rate. The hourly billing rate for each employee is the amount to be paid to you and is full compensation for all benefits, taxes, etc., to be provided and paid by you. There shall be no change in the billing rates during the term of this Agreement and no additional compensation for overtime, weekend, or holiday work. Attached hereto is a schedule of names, titles and corresponding hourly billing rates. Clearly indicate if any of the employees, proposed by you to perform the requested services, are former Authority employees. Said schedule shall be the basis for determining compensation, subject to audit and shall be updated by you in writing as required until your services under this Agreement are completed. The Authority reserves the right of approval of all personnel, amounts, billing rates for said personnel performing services under this Agreement. For compensation purposes under this Agreement, no such salary or amount shall exceed the salary or amount received by said personnel or rate customarily billed for a partner or principal as of the effective date of this Agreement unless the Director has been notified in advance, in writing, of the increased salary, rate or amount and approves the increase.

The Consultant shall verify that its employees working under this Agreement are legally present and authorized to work in the United States, as per the federally required I-9 Program.

Furthermore, upon request of the Authority, the Consultant shall furnish, or provide access to the Authority, federal Form I-9 (Employment Eligibility Verification) for each individual hired by the Consultant, performing services hereunder. This includes citizens and noncitizens.

The Authority reserves the right of approval of all personnel, amounts, billing rates and salaries of personnel performing services under this Agreement. When requesting salary or billing rate adjustments for one (1) or more of its personnel, the Consultant shall submit his/her name, title, current direct hourly rate or billing rate, proposed new direct hourly salary or billing rate, resulting percentage increase, effective date and reason for the requested adjustment setting forth in detail any increased costs to the Consultant of providing the services under this Agreement which has given rise to the request for increased salary. For adjustments submitted after the effective date of this Agreement, the Authority may grant an increase if the Consultant demonstrates compliance with all of the following conditions: that increases in salary, or partner's or principal's billing rate or amount are a) in accordance with the program of periodic merit and cost of living increases normally administered by it, b) warranted by increased costs of providing services under this Agreement, c) are based upon increases in salaries and billing rates which are generally applicable to all of Consultant's clients and d) are in accordance with the Authority's salary rate increase policy for the current year for Authority employees possessing comparable skills and experience. If during any calendar year, Authority limits are not available to the Consultant in a timely fashion, increases falling within such limits may be approved retroactively, as appropriate. The amount of increase in salary or billing rate, if any, to be applicable under this Agreement shall in all cases be finally determined by the Director or his/her designee, in their sole and absolute discretion.

B. An amount equal to the premium payments for overtime work or night work or for performing hazardous duty, actually paid to partners or principals, project/program management or other professional and technical employees for time actually spent by them in the performance of services hereunder when such overtime or other premium payments have been demonstrated to be in accordance with the Consultant's normal business practice and have been authorized in advance by the Director in writing. The Project Manager for the Authority shall have the right to authorize and approve premium payments up to a total amount of one thousand dollars (\$1,000) per occasion. Payments above said total amount shall be subject to the prior written authorization of the Director. Such premium payments to supervisory employees, who do not receive such payments in the Consultant's normal business practice shall not be given under this Agreement.

C. An amount equal to the amounts actually paid to subconsultants hereunder who have been retained after the written approval by the Director of the subconsultant and the compensation to be paid the subconsultant. The Consultant shall submit a copy of the terms and conditions of the subconsultant's compensation (including multiplier, if applicable), as well as an estimate of the number of hours required by the subconsultant to perform its services, as part of any request for approval of the subconsultant.

D. The Consultant shall also be compensated at an amount equal to the out-of-pocket expense, approved in advance by the Director, necessarily and reasonably incurred and actually paid by you in the performance of your services hereunder. Out-of-pocket expenses are

expenses that are unique to the performance of your services under this Agreement and generally contemplate the purchase of outside ancillary services, except that for the purpose of this Agreement, out-of-pocket expenses do include amounts for long distance telephone calls; rentals of equipment; travel and local transportation; and meals and lodging on overnight trips.

Notwithstanding the above, the Authority will pay an amount approved in advance by the Director and computed as follows for the reproduction of submittal drawings, specifications and reports:

1) If the Consultant uses its own facilities to reproduce such documents, an amount computed in accordance with the billing rates the Consultant customarily charges for reproduction of such documents on agreements such as this, or

2) If the Consultant uses an outside vendor for the reproduction of such documents, the actual, necessary and reasonable amounts for the reproduction of such documents.

The expenses do not include expenses that are usually and customarily included as part of the Consultant's overhead. For the purposes of this Agreement out-of-pocket expenses do not include amounts for mailing and delivery charges; typing, utilization of computer systems, computer aided design and drafting ("CADD"), cameras, recording or measuring devices, flashlights and other small, portable equipment, safety supplies, phones, telephone calls, electronic messaging including FAX, Telex and telegrams, or expendable office supplies. Unless otherwise indicated, required insurance is not a reimbursable expense.

When the Consultant uses his/her personal vehicle to provide services within the Port District, the Consultant shall be reimbursed for travel expenses beyond normal commuting costs at a rate not higher than the Annual Federal Mileage Reimbursement Rate (as determined by the General Services Administration (GSA) - <http://www.gsa.gov/portal/content/100715>) per mile traveled by auto.

When the Consultant is asked to provide services outside the Port District, the actual cost of transportation as well as the cost for hotel accommodations and meals shall be reimbursable hereunder when approved in advance in writing by the Director. The cost for all meals and lodging on approved overnight trips are limited to the amounts established by the United States General Services Administration for that locality.

General Services Administration (GSA) Rates:

Domestic Rates: <http://www.gsa.gov/portal/category/21287>.

You shall obtain the Director's written approval prior to making expenditures for out-of-pocket expenses in excess of one thousand dollars (\$1,000) per specific expenditure and for all overnight trips, which are reimbursable expenditures as set forth above. You shall substantiate all billings for out-of-pocket expenses in excess of twenty five dollars (\$25) with receipted bills and provide said receipts with the appropriate billing.

E. As used herein:

"Port District" is an area comprised of about 1,500 square miles in the States of New York and New Jersey, 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 seventeen counties, in the two States.

"Salaries paid to employees" or words of similar import shall mean salaries and amounts actually paid (excluding payments or factors for holidays, vacations, sick time, bonuses, profit participations and other similar payments) to professional and technical employees of the Consultant, for time actually spent directly in the performance of technical services hereunder and recorded on daily time records that have been approved by the employee's immediate supervisor, excluding the time of any employee of the Consultant to the extent that the time of such employee of the Consultant is devoted to typing/word processing, stenographic, clerical or administrative functions. Such functions shall be deemed to be included in the multiplier and billing rates referred to in subparagraph A above.

10. On or about the fifteenth day of each month, you shall render a bill for services performed and reimbursable out-of-pocket expenses incurred in the prior month, accompanied by such records and receipts as required, to the Project Manager. Each invoice shall bear your taxpayer number and the purchase order number provided by the Director. Upon receipt of the foregoing, the Director will estimate and certify to the Authority the approximate amount of compensation earned by you up to that time. As an aid to you the Authority shall, within thirty (30) days after receipt of such certification by the Director, advance to you by check the sum certified minus all prior payments to you for your account.

11. The Authority may at any time for cause terminate this Agreement as to any services not yet rendered, and may terminate this Agreement in whole or in part without cause upon three (3) days notice to you. You shall have no right of termination as to any services under this Agreement without just cause. Termination by either party shall be by certified letter addressed to the other at its address hereinbefore set forth. Should this Agreement be terminated in whole or in part by either party as above provided, you shall receive no compensation for any services not yet performed, but if termination is without fault on your part, the Authority shall pay you as the full compensation to which you shall be entitled in connection with this Agreement the amounts computed as above set forth for services completed to the satisfaction of the Director through the date of termination, minus all prior payments to you.

12. You shall not issue or permit to be issued any press release, advertisement, or literature of any kind, which refers to the Authority or the services performed in connection with this Agreement, unless you first obtain the written approval of the Director. Such approval may be withheld if for any reason the Director believes that the publication of such information would be harmful to the public interest or is in any way undesirable.

13. Under no circumstances shall you or your subconsultants communicate in any way with any contractor, 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 material shall be obtained by you when you find such data necessary unless otherwise instructed by the Director.

14. Any services performed for the benefit of the Authority at any time by you or on your behalf, even though in addition to those described herein, 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 express 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.

15. No certificate, payment (final or otherwise), acceptance of any work nor any other act or omission of the Authority or the Director shall operate to release you from any obligations under or upon this Agreement, or to estop 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 money paid in excess of that lawfully due, whether under mistake of law or fact or to prevent the recovery of any damages sustained by the Authority.

16. The Authority has a long-standing practice of encouraging Minority Business Enterprises (MBEs) and Women Business Enterprises (WBEs) to seek business opportunities with it, either directly or as subconsultants or subcontractors. "Minority-owned business" or "MBE" means a business entity which is at least 51 percent owned by one or more members of one or more minority groups, or, in the case of a publicly held corporation, at least 51 percent of the stock of which is owned by one or more members of 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. "Women-owned business" or "WBE" means a business which is at least 51 percent owned by one or more women; or, in the case of a publicly held corporation, 51 percent 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 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 Puerto Rican, Mexican, 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. American Indian 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.

The Authority has set a goal of 12 percent participation by qualified and certified MBEs and 5 percent to qualified and certified WBEs on technical service projects.

To be "certified" a firm must be certified by the Authority's Office of Business Diversity and Civil Rights.

In order to facilitate the meeting of this goal, the Consultant's shall use every good faith effort to utilize subconsultants who are certified MBEs or WBEs to the maximum extent feasible.

The Authority has a list of certified MBE/WBE service firms which is available to you at <http://www.panynj.gov/business-opportunities/supplier-diversity.html>. The Consultant shall be required to submit to the Authority's Office of Business Diversity and Civil Rights for certification the names of MBE/WBE firms he proposes to use who are not on the list of certified MBE/WBE firms.

17. 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 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 Consultant, its staff and subconsultants 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:

- Consultant/Subconsultant identity checks and background screening

The Consultant may be required to have its staff, and any subconsultant's staff, visitors or others over whom the Consultant/subconsultant 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 Consultant and subconsultant may also be required to use an organization designated by the Authority to perform the background checks.

The Port Authority's designated background screening provider may require inspection of not less than two (2) forms of valid/current government issued identification (at least one (1) 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.

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 is located at <http://www.secureworker.com>, or S.W.A.C. can be contacted directly at (877) 522-7922 for more information and the latest pricing. If approved by the Project Manager, the cost for said background checks for staff that pass and are granted a credential shall be reimbursable to the Consultant (and its subconsultants) 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 shall 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 Consultant and the subconsultant's staff, the Authority will supply such identification at no cost to the Consultant or its subconsultants. 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 Consultant or subconsultant to immediately report to the Authority the loss of any staff member's individual facility-specific identification credential. The Consultant or subconsultant shall be billed for the cost of the replacement identification credential. Staff shall display Identification badges in a conspicuous and clearly visible manner, when entering, working or leaving an Authority construction site or facility.

Staff may be required to produce not less than two (2) forms of valid/current government issued identification having an official photograph and an original, non-laminated social security card for identify and SSN verification.

- Designated Secure Areas

Services under the Agreement may be required in designated secure areas, as the same may be designated by the Port Authority ("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. All personnel that require access to designated secure areas who are not under 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 Consultant shall notify the Project Manager. The Consultant shall conform to the procedures as may be established by the Project 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 Consultant shall request a description from the Project 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 Project Manager during the term of the Agreement.

- 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 consultant security guards. However, this provision shall not relieve the Consultant of its responsibility to secure its equipment and work and that of its subconsultants and service suppliers at the Authority construction site or facility (including rental spaces). In addition, the Consultant, subconsultant 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 Agreement, 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 Agreement may require access to Port Authority information considered Confidential Information (“CI”) as defined in the Port Authority Information Security Handbook (“Handbook”), dated October, 2008, corrected as of February, 2009, 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 CI. 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 Handbook can be obtained upon request or at: <http://www.panynj.gov/business-opportunities/pdf/Corporate-Information-Security-Handbook.pdf>

- Audits for Compliance with Security Requirements

The Port Authority may conduct random or scheduled examinations of business practices under this section 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.

18. The Consultant assumes the following distinct and several risks to the extent arising from the negligent or willful intentional acts or omissions of the Consultant or its subconsultants in the performance of services hereunder:

A. The risk of loss or damage to Authority property arising out of or in connection with the performance of services hereunder;

B. The risk or loss or damage to any property of the Consultant or its subconsultants arising out of or in connection with the performance of services hereunder;

C. The risk of claims, arising out of or in connection with the performance of services hereunder, whether made against the Consultant or its subconsultants or the Authority, for loss or damage to any property of the Consultant's agents, employees, subcontractors, subconsultants, materialmen or others performing services hereunder;

D. The risk of claims, just or unjust, by third persons made against the Consultant or its subconsultants or the Authority on account of injuries (including wrongful death), loss or damage of any kind whatsoever arising in connection with the performance of services hereunder including claims against the Consultant or its subconsultants or the Authority for the payment of workers' compensation, whether such claims are made and whether such injuries, damage and loss are sustained at any time both before and after the completion of services hereunder.

The Consultant shall indemnify the Authority against all claims described in subparagraphs A through D above and for all expense incurred by it in the defense, settlement or satisfaction thereof, including expenses of attorneys. If so directed, the Consultant shall defend against any claim described in subparagraphs B, C and D above, in which event he shall not without obtaining express advance permission from the General Counsel of the Authority raise any defense involving in any way jurisdiction of the tribunal, immunity of the Authority, governmental nature of the Authority or the provisions of any statutes respecting suits against the Authority, such defense to be at the Consultant's cost.

The provisions of this clause shall also be for the benefit of the Commissioners, officers, agents and employees of the Authority, so that they shall have all the rights which they would have under this clause if they were named at each place above at which the Authority is named, including a direct right of action against the Consultant to enforce the foregoing indemnity, except, however, that the Authority may at any time in its sole discretion and without liability on its part cancel the benefit conferred on any of them by this clause, whether or not the occasion for invoking such benefit has already arisen at the time of such cancellation.

Neither the completion of services hereunder nor the making of payment (final or otherwise) shall release the Consultant from his obligations under this clause. Moreover, neither the enumeration in this clause or the enumeration elsewhere in this Agreement of particular risks assumed by the Consultant or of particular claims for which he is responsible shall be deemed (a) to limit the effect of the provisions of this clause or of any other clause of this Agreement relating to such risks or claims, (b) to imply that he assumes or is responsible for risks or claims only of the type enumerated in this clause or in any other clause of this Agreement, or (c) to limit the risks which he would assume or the claims for which he would be responsible in the absence of such enumerations.

No third party rights are created by the Agreement, except to the extent that the Agreement specifically provides otherwise by use of the words "benefit" or "direct right of action."

Inasmuch as the Authority has agreed to indemnify the Cities of New York and Newark against claims of the types described in subparagraph D above made against said cities, the Consultant's obligation under subparagraph D above shall include claims by said cities against the Authority for such indemnification.

19. LIABILITY INSURANCE AND WORKERS' COMPENSATION INSURANCE

A. Commercial Liability Insurance:

- 1) The Consultant shall take out and maintain at his own expense Commercial General Liability Insurance including but not limited to Premises-Operations, Completed Operations and Independent Contractors' coverages in limits of not less than \$5,000,000 combined single limit per occurrence for Bodily Injury Liability and Property Damage Liability. If vehicles are to be used to carry out the performance of this Agreement, then the Consultant shall also take out, maintain and pay the premiums on Automobile Liability Insurance covering all owned, non-owned and hired autos in not less than \$5,000,000 combined single limit per accident for bodily injury and property damage. Any/all activities performed airside must, at all times, be performed while under escort as approved in advance, and in writing by the Project Manager. If at any time, the Consultant is directed to perform services airside in the absence of an approved escort, the Commercial General Liability Insurance and Automobile Liability Insurance provided by the Consultant must contain limits of not less than \$25,000,000 combined single limit per occurrence as provided in item 2) (a) below. In addition, the liability policies (other than Professional Liability) shall include the Authority and its related entities as additional insureds and shall be specifically endorsed with a provision that the policies may not be canceled, terminated or modified without thirty (30) days written advance notice to the Project Manager as noted below. Moreover, the Commercial General Liability policy shall not contain any provisions (other than a Professional Liability exclusion, if any) for exclusions from liability other than provisions or exclusions 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. Furthermore, the Consultant's insurance shall be primary insurance as respects to the above additional insured(s). Any insurance or self-insurance maintained by the above additional insured(s) shall not contribute to any loss or claim.
- 2) Further, the certificate of insurance and the liability policy(ies) shall be specifically endorsed that "*The insurance carrier(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.*"
- 3) Additional Coverages: The Consultant shall have the policy endorsed when required by the Director for specific services hereunder and include the additional premium cost thereof as an out-of-pocket expense:

- a. If the services of the Consultant, as directed by the Authority, require the performance of services airside, the Commercial General Liability and Automobile Liability coverage limits stipulated in subparagraph 1, above, shall be increased to an amount not less than \$25,000,000 per occurrence as provided herein.
 - b. Endorsement to eliminate any exclusions applying to the underground property, explosion and collapse hazards.
 - c. Endorsement to eliminate any exclusions on account of ownership, maintenance, operation, use, loading or unloading of watercraft.
 - d. Coverage for work within 50 feet of railroad.
- B. Workers' Compensation Insurance:
- 1) The Consultant shall take out and maintain Workers' Compensation Insurance in accordance with the requirements of law and Employer's Liability Insurance with limits of not less than \$1,000,000 each accident. A waiver of subrogation in favor of the Authority and its wholly owned entities, as allowed by law, shall be included.
 - 2) Additional Coverages: The Consultant shall have the policy endorsed when required by the Engineer for specific services hereunder and include the additional premium cost thereof as an out-of-pocket expense:
 - a) United States Longshoremen's and Harbor Workers' Compensation Act Endorsement.
 - b) Coverage B Endorsement - Maritime (Masters or Members of the Crew of Vessels), in limits of not less than \$1,000,000 per occurrence.
- C. Amendments to Coverage B, Federal Employers' Liability Act in limits of not less than \$1,000,000 per occurrence. Professional Liability Insurance:
- The Consultant shall take out and maintain Professional Liability Insurance in limits of not less than \$5 million each occurrence, covering acts, errors, mistakes, and omissions arising out of the work or services performed by Consultant, or any person employed by Consultant. All endorsements and exclusions shall be evidenced on the certificate of insurance. The coverage shall be written on an occurrence form or may be written on a claims-made basis with a minimum of a three-year reporting/discovery period.
- D. Compliance:
- Prior to commencement of work at the site, the Consultant shall deliver a certificate from its insurer evidencing policies of the above insurance stating the title of this Agreement, the P. A. Agreement number and containing a separate express statement of compliance with each of the requirements above set forth, via e-mail to the Project Manager.
- 1) Renewal certificates of insurance or policies shall be delivered to the Facility Contractor Administrator, Port Authority at least fifteen (15) days prior to the expiration date of each expiring policy. The General Manager, Risk Management

- 2) 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 Consultant shall suspend performance of the Agreement at the premises. If the Agreement is so suspended, no extension of time shall be due on account thereof. If the Agreement 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 Consultant to the Authority.
- 3) Upon request of the Manager, Risk Management/Treasury, the Consultant shall furnish to the Authority a certified copy of each policy itself, including the provisions establishing premiums.
- 4) The requirements for insurance procured by the Consultant shall not in any way be construed as a limitation on the nature or extent of the contractual obligations assumed by the Consultant under this Agreement. The insurance requirements are not a representation by the Authority as to the adequacy of the insurance to protect the Consultant against the obligations imposed on them by law or by this or any other Agreement.
- 5) 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 Management for the Port Authority may consider such cost as an out-of-pocket expense.

20. CERTIFICATION OF NO INVESTIGATION (CRIMINAL OR CIVIL ANTI-TRUST), INDICTMENT, CONVICTION, DEBARMENT, SUSPENSION, DISQUALIFICATION AND DISCLOSURE OF OTHER INFORMATION

By proposing on this Agreement, each Consultant and each person signing on behalf of any Consultant certifies, and in the case of a joint proposal each party thereto certifies as to its own organization, that the Consultant and each parent and/or affiliate of the Consultant has not:

- A. been indicted or convicted in any jurisdiction;
- B. been suspended, debarred, found not responsible or otherwise disqualified from entering into any agreement with any governmental agency or been denied a government agreement for failure to meet standards related to the integrity of the Consultant;
- C. had an agreement terminated by any governmental agency for breach of agreement 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 Proposal;

E. had any business or professional license suspended or revoked or, within the five years prior to proposal opening, had any sanction imposed in excess of \$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, proposal 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.

21. NON-COLLUSIVE PROPOSING, AND CODE OF ETHICS CERTIFICATION, CERTIFICATION OF NO SOLICITATION BASED ON COMMISSION, PERCENTAGE, BROKERAGE, CONTINGENT OR OTHER FEES

By proposing on this Agreement, each Consultant and each person signing on behalf of any Consultant certifies, and in the case of a joint proposal, each party thereto certifies as to its own organization, that:

A. the prices in its proposal 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 Consultant or with any competitor;

B. the prices quoted in its proposal have not been and will not be knowingly disclosed directly or indirectly by the Consultant prior to the official opening of such proposal to any other Consultant or to any competitor;

C. no attempt has been made and none will be made by the Consultant to induce any other person, partnership or corporation to submit or not to submit a proposal 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 April 11, 1996 (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 Consultant for the purpose of securing business, has been employed or retained by the Consultant to solicit or secure this Agreement on the

understanding that a commission, percentage, brokerage, contingent, or other fee would be paid to such person or selling agency;

F. the Consultant 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 Agreement; and

G. no person or organization has been retained, employed or designated on behalf of the Consultant to impact any Authority determination with respect to (i) the solicitation, evaluation or award of this Agreement; or (ii) the preparation of specifications or request for submissions in connection with this Agreement.

The foregoing certifications, shall be deemed to be made by the Consultant as follows:

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

* if the Consultant is a partnership, such certification shall be deemed to have been made not only with respect to the Consultant itself, but also with respect to each partner.

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

In any case where the Consultant cannot make the foregoing certifications, the Consultant shall so state and shall furnish with the signed proposal a signed statement, which sets forth in detail the reasons therefor. If the Consultant is uncertain as to whether it can make the foregoing certifications, it shall so indicate in a signed statement furnished with its proposal, setting forth in such statement the reasons for its uncertainty. With respect to the foregoing certification in paragraph "21G," if the Consultant cannot make the certification, it shall provide, in writing, with the signed proposal: (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 Agreement, as described in the Procurement Disclosure policy of the Authority (a copy of which is available upon request to the Director of the Procurement Department of the Authority). Such disclosure is to be updated, as necessary, up to the time of award of this Agreement. As a result of such disclosure, the 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-responsibility.

Notwithstanding that the Consultant may be able to make the foregoing certifications at the time the proposal is submitted, the Consultant shall immediately notify the Authority in writing during

the period of irrevocability of proposals on this Agreement or any extension of such period of any change of circumstances which might under this clause make it unable to make the foregoing certifications or require disclosure. The foregoing certifications or signed statement shall be deemed to have been made by the Consultant 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 this Agreement. In the event that the Authority should determine at any time prior or subsequent to the award of this Agreement that the Consultant has falsely certified as to any material item in the foregoing certifications 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 Consultant is not a responsible Consultant with respect to its proposal on the Agreement or with respect to future proposals on Authority agreements and may exercise such other remedies as are provided to it by the Agreement with respect to these matters. In addition, Consultants 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.). Consultants are also advised that the inability to make such certification will not in and of itself disqualify a Consultant, and that in each instance the Authority will evaluate the reasons therefore provided by the Consultant. Furthermore, the Consultant selected for performance of the subject services shall immediately notify the Authority in writing, at any time during the term of the Agreement, of any change of circumstances which might under this clause make it unable to make the foregoing certifications, or might require disclosure.

Under certain circumstances the Consultant may be required as a condition of this Agreement 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 Authority. Said Monitor shall be charged with, among other things, auditing the actions of the Consultant to determine whether its business practices and relationships indicate a level of integrity sufficient to permit it to continue business with the Authority.

22. CONSULTANT ELIGIBILITY FOR AWARD OF AGREEMENTS - DETERMINATION BY AN AGENCY OF THE STATE OF NEW YORK OR NEW JERSEY CONCERNING ELIGIBILITY TO RECEIVE PUBLIC AGREEMENTS

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

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

which the Consultant was entitled by the requirements of due process of law, or (iii) the state agency determination was clearly erroneous or (iv) the state agency 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.

23. NO GIFTS OR GRATUITIES

During the term of this Agreement, the Consultant shall not offer, give or agree to give anything of value either to an Authority employee, agent, job shopper, consultant, construction manager or other person or firm representing the 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 Authority of duties involving transactions with the Consultant on behalf of the Authority, whether or not such duties are related to this Agreement or any other Authority agreement or matter. Any such conduct shall be deemed a material breach of this Agreement.

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 Agreement or any other Authority agreement), etc. which might tend to obligate the Authority employee to the Consultant, 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 Agreement or any other Authority agreement. Where used herein, the term "Port Authority" or "Authority" shall be deemed to include all subsidiaries of the Authority.

The Consultant 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.

24. NON-DISCLOSURE/CONFIDENTIALITY, OFFERS OF EMPLOYMENT

During the term of this Agreement, the Consultant shall not make an offer of employment or use confidential information in a manner proscribed by the Code of Ethics and Financial Disclosure dated April 11, 1996 (a copy of which is available upon request to the Office of the Secretary of the Authority). Without the express written approval of the Director, you shall keep confidential, and shall require your employees, your subconsultants, and your subconsultants' employees to keep confidential a) all information disclosed by the Authority or its consultants to you or b) developed by you or your subconsultants in the performance of services hereunder. Disclosure of any such information shall constitute a material breach of the Agreement.

The Consultant shall include the provisions of this clause in each subagreement entered into under this Agreement.

25. CONFLICT OF INTEREST

During the term of this Agreement, the Consultant shall not participate in any way in the preparation, negotiation or award of any agreement (other than an agreement for its own services to the Authority) to which it is contemplated the Authority may become a party, or participate in any way in the review or resolution of a claim in connection with such an agreement if the Consultant has a substantial financial interest in the Consultant or potential Consultant of the Authority or if the Consultant has an arrangement for future employment or for any other business relationship with said Consultant or potential Consultant, nor shall the Consultant 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 Consultant has reason to believe such an arrangement may be the subject of future discussion, or if the Consultant has any financial interest, substantial or not, in a Consultant or potential Consultant of the Authority, and the Consultant's participation in the preparation, negotiation or award of any agreement with such a Consultant or the review or resolution of a claim in connection with such an agreement is contemplated or if the Consultant has reason to believe that any other situation exists which might be viewed as or give the appearance of a conflict of interest, the Consultant shall immediately inform the Director in writing of such situation giving the full details thereof. Unless the Consultant receives the specific written approval of the Director, the Consultant shall not take the contemplated action which might be viewed as or give the appearance of a conflict of interest. In the event the Director shall determine that the performance by the Consultant of a portion of its services under this Agreement is precluded by the provisions of this numbered paragraph, or a portion of the Consultant's said services is determined by the Director to be no longer appropriate because of such preclusion, then the Director shall have full authority on behalf of both parties to order that such portion of the Consultant's services not be performed by the Consultant, 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 Consultant's execution of this document shall constitute a representation by the Consultant that at the time of such execution the Consultant 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 Consultant's part. The Consultant 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 agreements that result, directly or indirectly, from the services provided by the Consultant hereunder.

26. DEFINITIONS

As used in sections 20 to 25 above, the following terms shall mean:

Affiliate – Two (2) or more firms are affiliates if a parent owns more than fifty (50%) 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 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 Consultant by whatever titles known.

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

27. No commissioner, officer, agent or employee of the Authority shall be charged personally by you with any liability or held liable to you under any term or provision of this Agreement, or because of its execution or attempted execution or because of any breach hereof.

28. If the foregoing meets with your approval, please indicate your acceptance by signing the original and the additional enclosed copy in the lower right-hand corner and returning them to the Authority.

Very truly yours,

ACCEPTED:

THE PORT AUTHORITY OF
NEW YORK AND NEW JERSEY

FIRM:

Lillian D. Valenti
Director
Procurement Department

By: _____

Title: _____

Date _____

Date: _____

CONTRACT SPECIFIC TERMS AND CONDITIONS

TABLE OF CONTENTS

1.	GENERAL AGREEMENT	4
2.	DEFINITIONS	4
3.	GENERAL PROVISIONS.....	4
4.	INTELLECTUAL PROPERTY.....	5
5.	PROPRIETARY RIGHTS IN SUBJECT MATTER NOT WITHIN THE INTELLECTUAL PROPERTY CLAUSE.....	6
6.	INDEMNITY IN REGARD TO INFRINGEMENT MATTER.....	6
7.	COMPLIANCE WITH WEB SITE TERMS OF USE AND PRIVACY POLICIES	7
8.	CONSULTANT PERSONNEL STANDARDS OF PERFORMANCE.....	7
9.	ASSIGNMENTS AND SUBCONTRACTS.....	7
10.	CERTAIN CONSULTANT’S WARRANTIES	8
11.	RIGHTS AND REMEDIES OF THE AUTHORITY.....	10
12.	RIGHTS AND REMEDIES OF THE CONSULTANT	11
13.	TAX EXEMPTIONS	11
14.	NOTICE REQUIREMENTS	11
15.	SERVICE OF NOTICES ON THE CONSULTANT	12
16.	SUBMISSION TO JURISDICTION	12
17.	APPLICABLE LAW	13
18.	AUTHORITY OF THE DIRECTOR.....	13
19.	APPROVALS BY THE DIRECTOR	14
20.	CONTRACT REVIEW AND COMPLIANCE AUDITS	14
21.	AUTHORITY ACCESS TO RECORDS.....	15
22.	HARMONY	15
23.	CLAIMS OF THIRD PERSONS.....	16

24. NO DISCRIMINATION IN EMPLOYMENT, EQUAL EMPLOYMENT OPPORTUNITY 16

25. CONFIDENTIAL INFORMATION/NON-PUBLICATION..... 16

26. PROVISIONS OF LAW DEEMED INSERTED 17

27. INVALID CLAUSES 17

28. MODIFICATION OF CONTRACT 18

GENERAL CONTRACT PROVISIONS

1. GENERAL AGREEMENT

The undersigned Consultant (hereinafter referred to as the “Consultant,” “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 the services 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 Consultant shall perform the same as though they were specifically mentioned, described and delineated.

2. DEFINITIONS

As used herein, the term “days” or “calendar days” in reference to a period of time shall mean consecutive calendar days, Saturdays, Sundays, and holidays included.

“Facility” Port Authority Facilities within the Port District, as set forth in Appendix H1.

“Services” or “Work” shall 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.

As used herein, the term “Work Day” shall mean a day between Monday and Friday with Monday and Friday included.

As used herein the term “Specifications” shall 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.

As used herein, the terms “Port Authority” or “Authority” shall mean the Port Authority of New York and New Jersey.

3. GENERAL PROVISIONS

- A. The Consultant 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 Consultant of every rule and regulation hereafter adopted by it.

- B. This Contract does not constitute the Consultant as an agent or representative of the Port Authority for any purpose whatsoever. The Consultant shall perform all services hereunder as an independent Contractor and the Consultant, its officers, and employees shall not be deemed to be agents, servants, or employees of the Port Authority.

4. INTELLECTUAL PROPERTY

- A. Originals of estimates, reports, records, data, charts, documents, renderings, computations, computer tapes or disks, and other papers of any type whatsoever, whether in the form of writing, figures or delineations, which are prepared or compiled in connection with this Agreement, shall become the property of the Authority, and the 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. Except as provided below: as between the Port Authority and the Consultant 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 Consultant 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 Consultant without separate or additional compensation. Where the services under this Agreement require the Consultant 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 Consultant, utilized by the Consultant 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 Consultant.

- C. When in the performance of the contract services the Consultant 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 Consultant 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 Consultant hereunder in the performance of his services hereunder shall be licensed to the Consultant 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 Consultant without additional compensation.

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

If in accordance with this Contract the Consultant 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 Consultant, its officers, agents, employees, subcontractors, or suppliers, not custom software, and not covered under the clause herein 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 Consultant 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 Consultant 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 Consultant 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 Consultant 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 Consultant 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 Consultant 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 Consultant 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 Consultant to supply, temporarily or permanently, facilities not subject to such injunction and not infringing any proprietary rights and if the Consultant shall fail to do so, the Consultant 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 Consultant 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 idea, design, method, material, equipment, or Intellectual Property used, developed or licensed in connection with the performance of the Work or otherwise in connection with this Contract.

7. 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 Consultant under the Standard Agreement, the Consultant 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 Consultant shall immediately implement all procedures in connection with such policies and in furtherance thereof as directed by the Authority.

8. CONSULTANT PERSONNEL STANDARDS OF PERFORMANCE

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

At the time the Consultant is carrying out its operations there may be other persons working physically in the vicinity or in the same logical or technical infrastructure. . The Consultant 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.

9. ASSIGNMENTS AND SUBCONTRACTS

Any assignment or other transfer by the Consultant 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 Consultant 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 Consultant as a subcontractor, the Consultant 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 Consultant pursuant to the clauses of the "Integrity" Section of the Standard Agreement 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 Consultant 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 Consultant, all assignees, subcontractors, and other transferees shall for all purposes be deemed to be agents of the Consultant. 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 Consultant personally or through other approved subcontractors. All subcontractors shall make the certifications required by the "Certification of No Investigation Indictment, Conviction, Debarment Suspension, Disqualification and Disclosure of Other Information" clause of the Standard Agreement.

10. CERTAIN CONSULTANT'S WARRANTIES

The Consultant 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 Consultant 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;
- A. 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;
- B. 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 Consultant to enter into this Contract or has been relied upon by the Consultant, 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 Consultant's services by the Authority, or the existence of any patent or trade name, the Consultant 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 Consultant 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 Consultant 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 Consultant'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 Consultant 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 Consultant 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 Consultant 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 Consultant 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.

11. RIGHTS AND REMEDIES OF THE AUTHORITY

The Authority shall have the following rights in the event the Director shall deem the Consultant 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 Consultant, either directly or through other Consultants/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 Consultant 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 Consultant 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 Consultant 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 Consultant 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 Consultant'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 Consultant's duties or obligations, nor any aid provided to the Consultant 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.

12. RIGHTS AND REMEDIES OF THE CONSULTANT

Inasmuch as the Consultant can be adequately compensated by money damages for any breach of this Contract which may be committed by the Authority, the Consultant 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.

13. 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 Consultant's services under this Contract is exempt from Sales Taxes. Accordingly, the Consultant must not include Sales Taxes in the price charged to the Port Authority for the Consultant's services under this Contract.

14. NOTICE REQUIREMENTS

No claim against the Authority shall be made or asserted in any action or proceeding at law or in equity, and the Consultant shall not be entitled to allowance of such claim, unless the Consultant 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 Consultant to give such written notice and information as to any claim shall be conclusively deemed to be a waiver by the Consultant 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 Consultant, including daily records showing all costs which the Consultant 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 Consultant's obligation under this Agreement.

15. SERVICE OF NOTICES ON THE CONSULTANT

Whenever provision is made in this Contract for the giving of any notice to the Consultant, its deposit in any post office box, enclosed in a postpaid wrapper addressed to the Consultant 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 Consultant's office will be that stated in his/her Proposal. Notices may also be served personally upon the Consultant; or if a corporation, upon any officer, director or managing or general agent; or if a partnership upon any partner.

16. SUBMISSION TO JURISDICTION

The Consultant 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 Consultant agrees that the service of process on the Consultant 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 Consultant indicated on the signature sheet, or by actual personal delivery to the Consultant, if the Consultant is an individual, to any partner if the Consultant be a partnership or to any officer, director or managing or general agent if the Consultant 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.

17. APPLICABLE LAW

This Contract shall be construed in accordance with the laws of the State of New York. The Consultant 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 Consultant agrees that mailing of process by registered mail addressed to it at the address of the Consultant 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.

18. 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 Attachment A 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 Consultant'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 Consultant 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 Consultant 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 Consultant 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 Consultant 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.

19. 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 Consultant from its full responsibility for the satisfactory performance of the services to be supplied. "Approved equal" shall mean approved by the Director.

20. CONTRACT REVIEW AND COMPLIANCE AUDITS

The Consultant, 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 Consultant, and any subcontractors, shall support requests related to audits of the agreement and administration tasks and functions covered by this Contract.

The Consultant, and any subcontractors, shall keep daily records of the time spent in the performance of services hereunder by all persons whose salaries or amounts paid thereto will be the basis for compensation under this Agreement as well as records of the amounts of such salaries and amounts actually paid for the performance of such services and records and receipts of reimbursable expenditures hereunder, and, notwithstanding any other provisions of this Agreement, failure to do so shall be a conclusive waiver of any right to compensation for such services or expenses as are otherwise compensable hereunder. The Authority shall have the right to audit all such records.

The Authority shall have the right to inspect your records, and those of your subconsultants, pertaining to any compensation to be paid hereunder, such records to be maintained by you and your subconsultants for a period of three (3) years after completion of all services to be performed under this Agreement.

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.

21. AUTHORITY ACCESS TO RECORDS

The Authority shall have access during normal business hours to all records and documents of the Consultant 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 Consultant records shall be kept in the Port District. The Consultant 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 Consultant, provided, however, that if within the aforesaid one year period The Authority has notified the Consultant 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 Consultant 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 Consultant 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 Consultant 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 Consultant charges to the Authority. The Authority shall have access to the detail records that support Consultant 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.

22. HARMONY

- A. The Consultant 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 Consultant under this Contract.

The Consultant 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 Consultant 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 Consultant at the Facility or against any operations of the Consultant under this Contract, whether or not caused by the employees of the Consultant, 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 Consultant 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 Consultant under this Contract, and during the period of the suspension the Consultant 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 Consultant using the equipment which is used by the Consultant in its operations hereunder as the Port Authority deems necessary and without cost to the Port Authority. During such time of suspension, the Consultant 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 Consultant 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 Consultant 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 Consultants performing at the worksite, all of which shall remain uninterrupted.

The Consultant 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.

23. CLAIMS OF THIRD PERSONS

The Consultant 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.

24. NO DISCRIMINATION IN EMPLOYMENT, EQUAL EMPLOYMENT OPPORTUNITY

During the performance of this Contract, the Consultant agrees as follows:

- A. The Consultant is advised to ascertain and comply with all applicable Federal, State and Local statutes, ordinances, rules and regulations and Federal Executive Orders pertaining to equal employment opportunity, affirmative action and non-discrimination in employment.
- B. Without limiting the generality of any other term or provision of this Contract, in the event of the Consultant's non-compliance with any such statutes, ordinances, rules, regulations or orders, this Contract may be canceled, terminated, or suspended in whole or in part.

25. CONFIDENTIAL INFORMATION/NON-PUBLICATION

- A. As used herein, confidential information shall mean all information disclosed to the Consultant or the personnel provided by the Consultant 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 Consultant'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 February, 9 2009)*, and as may be amended, from time to time, 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 Consultant shall hold all such confidential information in trust and confidence for the Authority, and agrees that the Consultant and the personnel provided by the Consultant 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 Consultant and the personnel provided by the Consultant 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 Consultant and the personnel provided by the Consultant 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 Consultant 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 Consultant has knowledge, relating to any idea, design, method, material, equipment or other matter related to this Contract or coming to the Consultant's attention in connection with this Contract.

26. 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.

27. 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.

28. 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.

Port Authority New Jersey Facilities

During the duration of the Contract, the Port Authority may, at its discretion, add, delete, or modify locations and/or facilities. The “Port District” comprises about 1,500 square miles in the States of New York and New Jersey, 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 seventeen counties, in the two States.

The Consultant will be advised by the Port Authority, and is subject to changes by the Port Authority.

Port Authority Technical Center
241 Erie Street
Jersey City, NJ 07310

Newark International Airport
Newark, NJ 07114

Holland Tunnel
13th & Provost Streets
Jersey City, NJ 07310

Newark Legal Center
One Riverfront Plaza
Newark, NJ 07102

JAMS Building
777 Jersey Avenue
Jersey City, NJ 07310

Gateway Plaza
Newark, NJ 07102

Journal Square Transportation Center
One Path Plaza
Jersey City, NJ 07306

Port Newark/Port Elizabeth
260 Kellogg Street
Port Newark, NJ 07114

5 Marine View Plaza
Hoboken, NJ 07310

George Washington Bridge
220 Bridge Plaza South
Fort Lee, NJ 07024

Lincoln Tunnel
500 Boulevard East
Weehawken, NJ 07087

Teterboro Airport
Teterboro, NJ 07608

2 Montgomery St.
Jersey City, NJ 07302

Port Jersey-Port Authority Marine Terminal
51 Port Terminal Blvd
Bayonne, NJ 07002
Operations – Rm. 115

The Port Authority, at its discretion may add, delete or modify locations and/or Facilities in New York and New Jersey within the Port District, which encompasses an approximate 25-mile radius from the Statue of Liberty. The Contractor will be advised by the Port Authority, and is subject to changes by the Port Authority.

Port Authority New York Facilities & Offices

225 Park Avenue South
New York, NY 10003

233 Park Avenue South
New York, NY 10003

620-630 West 30th Street
New York, NY

LaGuardia Airport
Various Buildings
Flushing, NY 11371

NY Marine Terminals
90 Columbia Street
Brooklyn, NY 11201

Goethal's Bridge
Building 2777 Goethal's Rd. N.
Staten Island, NY 10303

Bayonne Bridge
70 Trantor Place
Staten Island, NY 10303

Outerbridge Crossing
101 Boscombe Avenue
Staten Island, NY 10303

116 Nassau Street
2nd Floor
New York, NY 10006

100 Broadway
New York, NY

111 Broadway
New York, NY

Port Authority Bus Terminal
625 8th Avenue
New York, NY 10018

JFK International Airport
Various Buildings
Jamaica, NY 11430

Bathgate Industrial Park
1701 Bathgate Avenue
Bronx, NY 10457

The Teleport
One Teleport Drive
Staten Island, NY 10311

Port Ivory/Howland Hook
40 Western Avenue
Staten Island, NY 10303

115 Broadway
Various Floors
New York, NY 10006

WTC Police Command
4 Vesey Street
New York, NY 10048

*Stewart International Airport
1180 First Street
New Windsor, NY 12553

22 Cortlandt Street
New York, NY

WTC
New York, NY

The Port Authority, at its discretion may add, delete or modify locations and/or Facilities in New York and New Jersey within the Port District, which encompasses an approximate 25-mile radius from the Statue of Liberty. The Contractor will be advised by the Port Authority, and is subject to changes by the Port Authority.

*Stewart International Airport is included as a New York facility although it is out of the approximately 25-mile radius from the Statue of Liberty as stated in the above paragraph.