

THE PORT AUTHORITY OF NY & NJ
PROCUREMENT DEPARTMENT
ATTN: BID/PROPOSAL CUSTODIAN
4 WORLD TRADE CENTER
150 GREENWICH STREET, 21ST Floor
NEW YORK, NY 10007

REQUEST FOR PROPOSALS

ISSUE DATE: AUGUST 26, 2016

**TITLE: THE PORT AUTHORITY OF NEW YORK AND NEW JERSEY,
PORT AUTHORITY TRANS-HUDSON CORPORATION (PATH)
REQUEST FOR PROPOSALS (RFP) FOR LEASING, MANAGEMENT,
MAINTENANCE, AND OPERATION OF PARKING GARAGE AT JOURNAL
SQUARE TRANSPORTATION CENTER (JSTC)**

RFP NO.: 47054

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

**PRE-PROPOSAL MEETING/SITE INSPECTION:
SEPTEMBER 13, 2016 TIME: 10:00AM**

QUESTIONS DUE BY: SEPTEMBER 20, 2016 TIME: 3:00P.M.

PROPOSAL DUE DATE: OCTOBER 5, 2016 TIME: 2:00 P.M.

**CONTACT: LESLEY BROWN
PHONE: (212) 435-4648
EMAIL: lbrown@panynj.gov**

TABLE OF CONTENTS

1. INFORMATION FOR PROPOSERS ON THIS REQUEST FOR PROPOSALS 5

A. General Information: The Port Authority of New York and New Jersey 5

B. Definitions 5

C. Brief Summary of Scope of Work 6

D. Deadline for Receipt of Proposals 7

E. Vendor Profile 8

F. Submission of Proposals 8

G. Communications Regarding this RFP 8

H. Proposal Acceptance or Rejection 9

I. Union Jurisdiction 9

J. Governmental Requirements 9

K. Pre-Proposal Meeting and Site Inspection: 10

L. Available Documents 10

M. Aid to Proposers 11

N. Additional Proposer Information 12

O. Contractor Staff Background Screening 12

P. Automated Clearing House Enrollment 12

Q. Exhibits attached to this RFP and Lease 12

2. PROPOSER PREREQUISITES 13

3. FINANCIAL INFORMATION 14

4. EVALUATION CRITERIA AND RANKING 14

5. MBE/WBE SUBCONTRACTING PROVISIONS 15

6 . CERTIFICATION OF RECYCLED MATERIALS PROVISION 16

8. PROPOSAL SUBMISSION REQUIREMENTS 16

A. Letter of Transmittal 16

B. Executive Summary 17

C. Agreement on Terms of Discussion 17

D. Certifications With Respect to the Contractor’s Integrity Provisions 17

E. Documentation of Proposer Prerequisites 18

F. Proposal 18

G. Acknowledgment of Addenda 20

H. Acceptance of Lease Terms and Conditions 21

I.	MBE/WBE Requirements	21
8.	CONDITIONS FOR THE SUBMISSION OF A PROPOSAL	21
A.	Changes to this RFP.....	21
B.	Proposal Preparation Costs	21
C.	Disclosure of Proposal Contents / Use of Ideas and Materials	21
D.	Ownership of Submitted Materials	21
E.	Subcontractors	21
F.	Conflict of Interest	22
G.	Authorized Signature.....	22
H.	References	22
I.	Evaluation Procedures and Negotiation	22
J.	Taxes and Costs.....	22
K.	Most Advantageous Proposal/No Obligation to Award	22
L.	Multiple Contract Awards	22
M.	Right to Extend Lease.....	23
N.	Rights of the Port Authority	23
O.	Personal Non-Liability.....	24
P.	Contractor’s Integrity Provisions.....	
	ATTACHMENT A.....	25
	AGREEMENT ON TERMS OF DISCUSSION.....	29
	ATTACHMENT B.....	31
	PART I – LEASE.....	32
	PART II – SCOPE OF WORK: LEASING, MANAGEMENT, MAINTENANCE, AND	
	OPERATION OF PARKING GARAGE AT JOURNAL SQUARE	
	TRANSPORTATION CENTER (JSTC).....	33
	PART III - LEASE PROPOSAL FORM	37
	ATTACHMENT C- PROPOSER REFERENCE FORM.....	39
	ATTACHMENT D - Certified Environmentally Preferable Products/Practices	40
	ATTACHMENT E.....	41
	RULES AND REGULATIONS OF THE PORT AUTHORITY TRANS-HUDSON	
	SYSTEM (PATH)	41
	ATTACHMENT F.....	42
	TENANT ALTERATION CONSTRUCTION APPLICATION	42
	ATTACHMENT G: SITE PLAN AND AERIAL PHOTO	43
	ATTACHMENT H.....	45
	PART I TECHNOLOGY STANDARDS	46

PART II CYBER SECURITY GUIDELINES.....	47
PART III COMPUTING RESOURCES POLICY.....	48
PART IV CLOUD COMPUTING FRAMEWORK.....	49
PART V AUDIT DEPARTMENT CONTROLS REQUIREMENT CONTRACT CHECKLIST.....	65
EXHIBIT 3 JSTC PARKING GARAGE DRAWING.....	66

1. INFORMATION FOR PROPOSERS ON THIS REQUEST FOR PROPOSALS

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

The Port Authority of New York and New Jersey (the "Port Authority" or the "Authority") is an agency of the States of New York and New Jersey, created and existing by virtue of the Compact of April 30, 1921, made by and between the two States, and thereafter consented to by the Congress of the United States. It is charged with providing transportation, terminal and other facilities of trade and commerce within the Port District. The Port District comprises an area of about 1,500 square miles in both States, centering about New York Harbor. The Port District includes the Cities of New York and Yonkers in New York State, and the cities of Newark, Jersey City, Bayonne, Hoboken and Elizabeth in the State of New Jersey, and over 200 other municipalities, including all or part of seventeen counties, in the two States. The Port Authority manages and/or operates all of the region's major commercial airports (Newark Liberty International, John F. Kennedy International, Teterboro, LaGuardia and Stewart International Airports), marine terminals in both New Jersey and New York (Port Newark 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."

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

The Port Authority Trans-Hudson Corporation (PATH), is hereby seeking proposals from qualified firms to provide Leasing, Management, Operations and Maintenance of Journal Square Transportation Center (JSTC) parking garage located in Jersey City, New Jersey as more fully described herein. For purposes of this RFP and Lease Agreement, the Port Authority may act on behalf of PATH.

B. Definitions

Basic Rental: Means the fixed rental amount that Lessee shall pay to PATH, escalating annually (amount and escalation to be proposed by the Proposer).

Contractor (also referred to herein as "Lessee"): Means the Proposer selected to enter into a lease agreement with the Port Authority to manage, maintain and operate the Facility.

Facility: Means the public parking garage on the first parking level and on the roof level of the Journal Square Transportation Center in the City of Jersey City, County of Hudson and State of New Jersey, shown on the sketch attached hereto as Attachment I.

Initial Work: Means the improvements that the Lessee will perform to bring the Facility to a condition consistent with comparable commuter parking garages in the region and install a Revenue Collection and Management System (RCS), as further described in Attachment B, Part II. It is anticipated that the cost of the Initial Work will be offset by a credit against the rent paid by the Lessee over the term of the Lease.

Journal Square Transportation Center or JSTC: Means the Port Authority Journal Square Transportation Center in Jersey City, NJ.

Lease: Means the lease agreement substantially in the form attached as Attachment B, Part I.

Percentage Rental: Means rental payments that Lessee shall pay to PATH in addition to the Basic Rental, which are anticipated to be a percentage (to be proposed by the Proposer and accepted by PATH) of Lessee's gross receipts above the Percentage Rent Threshold.

Percentage Rent Threshold: Means the amount of Lessee's Gross Receipts above which Lessee shall pay a certain percentage to PATH as Percentage Rent.

RCS, or Revenue Collection and Management System: Means a system that allows the Lessee to control access, collect parking revenues, provide revenue accounting, and accept multiple payment methods including, but not limited to, cash, credit/debit card (including chip technology) and is potentially adaptable for *EZ-Pass*® electronic payment collection system and mobile payment technology.

C. Brief Summary of Scope of Work

The Port Authority is seeking a qualified firm to lease, manage, maintain and operate the five-hundred thirty-nine (539) space, bi-level public parking garage located at the Port Authority's JSTC in Jersey City, New Jersey (the "Facility") in order to maximize parking revenues for the Port Authority and provide high-quality service to customers. The location of the Facility is 16 PATH Plaza in the Journal Square section of Jersey City. The Facility has a prime location in a fast growing neighborhood, and has convenient access to the Journal Square PATH station and bus lanes. The parking lot currently fills to capacity Monday through Friday and demand is expected to increase due to new development in the surrounding area. For informational purposes, current parking rates and sales are detailed in this RFP.

The Lessee will enter into a Lease Agreement with PATH in substantially the form attached hereto as Attachment B, Part I (the "Lease").

The term of the Lease shall be five (5) years, with the Port Authority having the option to extend the term for two (2) two, (2)-year option periods followed by one (1), one (1)-year option period. The Lessee shall assume all responsibilities specified in the Lease, including operating the Facility twenty-four hours (24) a day, seven (7) days a week, and maintaining the Facility in a manner that complies with the Rules and Regulations of PATH (See Attachment G). The Lessee will be

expected to maximize revenue by setting rates consistent with the local market and effectively managing capacity (which may include a valet component to supplement current self-park operations). The Lessee will also be required to report metrics on market demand and supply, pricing, revenues/expenses, and construction costs.

Additionally, the Lessee shall implement initial repair work (as further described in Attachment B, Part II) in order to bring the Facility to a condition consistent with industry standards, and replace the existing "cash only" revenue collection system with a revenue collection and management system (RCS) that improves customer experience, revenue accounting, accepts multiple payment methods including but not limited to cash, credit/debit card (including chip technology) and is adaptable for EZ-Pass and mobile payment technology. Proposers' Lease Proposal shall include a design and budget for the repairs described in Attachment B, Part II and the RCS that meets the minimum requirements listed in Attachment B. It is anticipated that the cost of the initial repair work and installing the new RCS will be offset by a credit against the Lessee's rent.

The Port Authority will retain the right to use spaces at the Facility. The Lessee shall be compensated for the Port Authority's use of such parking spaces in the form of a credit against the Lessee's rental payments. The current number of spaces utilized by the Port Authority is detailed in Section 1(M) of this RFP, "Aid to Proposers."

D. Deadline for Receipt of Proposals

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

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

Proposal submissions will be received at:

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

Clearly mark the solicitation number on the outermost package.

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

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

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

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

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

E. Vendor Profile

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

F. Submission of Proposals

One reproducible original (containing original signatures and clearly designated as such) and **twelve (12) double-sided copies of the proposal and eleven (11) CDs or Flash Drives** copies of the proposal shall be submitted on or before the due date and time in accordance with the information on the cover page of this RFP and sent or delivered to the RFP Custodian at the address specified on the cover page. Each copy of the proposal as well as the parcel(s) used for shipping must be conspicuously marked with the Proposer's name and address as well as the Proposer's Vendor Number, if available. In addition, the outside of the package must clearly state the title of this RFP, the number of this RFP and the Proposal Due Date. Failure to properly label proposal submissions may cause a delay in identification, misdirection or disqualification of proposal submissions.

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

G. Communications Regarding this RFP

All communications concerning this RFP should be directed to the Principal Buyer listed on the cover page. All questions regarding this RFP should be submitted in writing to the Principal Buyer at the email address listed on the cover page no later than 3:00 p.m. (EST) on September 20, 2016.

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

Neither the Principal Buyer nor any other employee of the Port Authority is authorized to interpret the provisions of this RFP or give additional information as to

its requirements. If interpretation or other information is required, it will be communicated to Proposers by written addenda and such writing shall form a part of this RFP.

H. Proposal Acceptance or Rejection

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

I. Union Jurisdiction

Proposers are advised to ascertain whether any union now represented or not represented at the facility will claim jurisdiction over any aspect of the operations to be performed hereunder and their attention is directed to the Section of this RFP entitled "Harmony" included in the "Standard Contract Terms and Conditions" hereunder.

J. Governmental Requirements

- a. The Lessee shall procure from all governmental authorities having jurisdiction over the operations of the Lessee at the premises of the Facility all licenses, certificates, permits or other authorization, which may be necessary for the conduct of its operations.
- b. The Lessee shall pay all taxes, license, certification, permit and examination fees and excises which may be assessed, levied, exacted or imposed on its property or operation hereunder or on the gross receipts or income there from, and shall make all applications, reports and returns required in connection therewith.
- c. The Lessee shall promptly observe, comply with and execute the provisions of any and all present and future governmental laws, rules, regulations, requirements, orders and directions which may pertain or apply to the operations of the Lessee on the premises or its occupancy thereof.
- d. The obligation of the Lessee to comply with governmental requirements is provided herein for the purpose of assuring proper safeguards for the protection of persons and property on the premises and a proper operation by the Lessee. Such provision is not to be construed as a submission by PATII to the application to itself of such requirements or any of them.

K. Pre-Proposal Meeting and Site Inspection:

Any questions concerning this RFP should be submitted in writing, however, responses may be deferred and provided at a later date by written addenda.

The Pre-Proposal Meeting and Site Inspection is scheduled for September 13, 2016 at 10:00AM at the following location:

**1 PATH Plaza
7TH Floor Conference Room
Jersey City, New Jersey**

Site Inspection:

A site inspection allows Proposers to tour and physically inspect the actual site(s) of work prior to the submission of proposals. No questions will be taken during site inspections.

Attendance is strongly recommended. Information conveyed may be useful to Proposers in preparing their proposals and Proposers not attending assume all risks which may ensue from non-attendance.

Attendees interested in attending should RSVP to **Mr. Andrew Izzo at aizzo@panynj.gov or (201) 216-6367** no later than 12 noon (EDT) of the business day preceding the scheduled date(s) to confirm their attendance and/or receive traveling directions.

A maximum of two (2) individuals per company are allowed to attend. Two (2) valid forms of photo ID are required with one form being a driver license/state identification card or passport to attend the pre-submittal meeting and facility inspections.

Individuals planning to attend should RSVP as set forth above, and include **all** of the following information:

- a. Legal First and Last name
- b. Company Name
- c. Phone Numbers (office and/or cell)
- d. Email address
- e. Which site inspection(s) he/she will attend

Failure to provide complete and correct information may result in individuals being denied attendance.

It is highly recommended attendees arrive thirty-(30) minutes prior to the start of the Pre-Proposal Meetings and Site Inspections.

L. Available Documents

Certain documents, specified below, will be made available for examination by at the Pre-Proposal/Site Inspection or by contacting **Andrew Izzo at 201-216-6367 or Paul Berg at 212-435-5520** Monday through Friday between the hours of 9AM and 5PM.

These documents were not prepared for the purpose of providing information for Proposers on this RFP but they were prepared for other purposes, such as for other Contracts or for design purposes for this or other Contracts, and they do not form a part of this RFP. The Port Authority makes no representation or guarantee as to, and shall not be responsible for, their accuracy, completeness or pertinence, and, in addition, shall not be responsible for inferences or conclusions drawn there from. They are made available to Proposers merely for the purpose of providing them with such information, whether or not such information may be accurate, complete, and pertinent or of any value to Proposers.

Said documents are as follows:

- Current lease agreement for the Facility
- Site plans of the garage, “helix”-shaped ramp structure, and entry driveway and pavilion

M. Aid to Proposers

As an aid to Proposers in determining the appropriate amount of materials required in the performance of this Contract, the Port Authority provides the following historical data. The Port Authority makes no representation, guarantees or warranties that the estimated amounts of materials or numbers provided herein are accurate or complete, or that they will constitute the amounts of materials required to be furnished under this Contract and, in addition, shall not be responsible for the conclusions to be drawn therefrom.

1. Current Public Parking Rates (as of June 2016)

Up to One Hour: \$6
Up to Four Hours: \$8
Up to Seven Hours: \$9
Up to Twelve Hours: \$11
Maximum to Twenty-Four Hours: \$14
Early bird – enter by 6AM: \$9
Weekend Rate Special for up to Twelve Hours: \$7
Monthly: \$195
Jersey City Parking Taxes included in the rates

2. Sales History

Average parking sales in April 2016 were as follows.

- Weekday Hourly Customers: 547
- Saturday Hourly Customers: 299
- Sunday Hourly Customers: 245
- Monthly Customers: 78

3. Parking Spaces Utilized by the Port Authority

On average, the following number of parking spaces were utilized by the Port Authority in April 2016:

- Weekday average: 80 spaces occupied by Port Authority personnel
- Saturday average: 64 spaces occupied by Port Authority personnel

- Sunday average: 56 spaces occupied by Port Authority personnel

N. Additional Proposer Information

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

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

O. Contractor Staff Background Screening

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

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

P. Automated Clearing House Enrollment

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

Q. The Contractor shall comply with all exhibits attached to this RFP and Lease which include the following:

- 1) Port Authority Cloud Computing Framework
- 2) Port Authority Computing Resources
- 3) Port Authority Audit Controls Requirement Contract Checklist
- 4) Technology Standards for the Port Authority

- 5) Cyber Security Guidelines for the Port Authority of NY & NY
- 6) Tenant Construction or Alteration Application
- 6) Site Plan and Aerial Photo
- 7) JSTC Parking Garage Drawing
- 8) Rules And Regulations Of The Port Authority Trans-Hudson System

2. PROPOSER PREREQUISITES

Only Proposers who can demonstrate that they comply with the following should submit proposals as only proposals from such Proposers will be considered:

A. The Proposer shall have had at least five (5) years of continuous experience immediately prior to the date of the submission of its proposal in the management, operation, and provision of maintenance services of a public parking lot business and have actually engaged in providing these services to commercial and industrial accounts under contract. The Proposer may fulfill this prerequisite if it can demonstrate that the persons or entities owning and controlling the Proposer have had a cumulative total of at least the same number of years and type of direct continuous experience immediately prior to the submission of this proposal as is required of the Proposer, or has owned and controlled other entities which meet the requirement.

B. During the time period stated in (A) above, the Proposer shall demonstrate satisfactory performance of at least one (1) contract for similar services of similar scope.

C. The Proposer shall demonstrate that it has earned gross revenues of at least three million dollars and no cents (\$3,000,000.00) a year for the last two (2) fiscal or calendar years.

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

With respect to subparagraphs (A) and (B) above, the prerequisite will be considered satisfied if the joint venture itself, or any of its participants individually, can meet the requirements. With respect to subparagraph (C) the gross income of the joint venture itself may meet the prerequisites or the gross income of the participants in the joint venture may be considered cumulatively to meet the prerequisite.

If the proposal is submitted by a common law joint venture, a joint venture that has not been established as a distinct legal entity, each participant of the joint venture shall be held jointly and severally liable and must individually execute and perform all acts required by this proposal. Documents signed by a common law joint venture, in connection with this proposal, shall include the names of all participants of the joint venture followed by the words "acting jointly and severally". All joint venture proposers must provide documentation of their legal status.

All Proposers must include documentation that they meet the above prerequisites.

By furnishing this solicitation document to Proposers, the Port Authority has not made a determination that the Proposers have met the prerequisites or have otherwise been deemed qualified to perform the services. In addition, a determination that a Proposer has met the prerequisites is no assurance that they will be deemed qualified in connection with other proposal requirements included herein.

3. FINANCIAL INFORMATION

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

- A. (1) Certified financial statements, including applicable notes, reflecting the Proposer's assets, liabilities, net worth, revenues, expenses, profit or loss and cash flow for the most recent year or the Proposer's most recent fiscal year.
- (2) Where the certified financial statements in (1) above are not available, then either reviewed or compiled statements from an independent accountant setting forth the aforementioned information shall be provided.
- (3) Where neither certified financial statements nor financial statements from an independent accountant are available, as set forth in (1) and (2) above, then financial statements containing such information prepared directly by the Proposer may be submitted; such financial statements, however, must be accompanied by a signed copy of the Proposer's most recent Federal income tax return and a statement in writing from the Proposer, signed by an executive officer or his/her designee, that such statements accurately reflect the present financial condition of the Proposer.

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

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

4. EVALUATION CRITERIA AND RANKING

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

A. Value of the Lease

The financial value of the lease to the Port Authority, based on the Proposer’s Lease Proposal Form.

B. Install and Maintain Revenue Collection and Management System (RCS)

- (i) Quality of the design concept, including its innovation and compatibility with the requirements of the parking garage;
- (ii) Technical approach to aspects of the project that are consistent with and conform to the requirements of the parking garage;
- (iii) Qualifications and experience of the proposed mechanical, structural and geotechnical (as applicable) engineering firms; and
- (iv) Approach to phasing the work and the schedule/timing for completing the improvements.

C. Management/Staff Approach

The clarity and feasibility of the Proposal, which shall include the Proposer’s management philosophy, principles and programs to be utilized by the Lessee in performing the service, and which shall include, but is not limited to, consideration of the following:

- (i) Proposed quality assurance/quality control program(s) addressing how the Proposer will ensure compliance with the Lease Agreement requirements.
- (ii) On-site management plans and work plans for this Lease Agreement including improvement, maintenance, snow and ice removal, customer service, and marketing plans.
- (iii) The extent to which proposed labor and supervisory staff (i.e. parking attendant, parking manager, assistant manager and weekend supervisor) have relevant qualifications and experience in operating a public parking lot facility.
- (iv) The extent to which the Proposer, and the managerial and supervisory personnel proposed to be dedicated to this program have experience in implementing and managing similar services in a similar environment using staff comparable in size to that necessary for the services to be provided hereunder.
- (v) The extent to which the Proposer has experience operating, maintaining, and providing improvements to parking facilities, including installing and or operating “state of the art” revenue control systems (RCS) and executing snow and ice removal plans, and the ability to operate under Port Authority Trans-Hudson (PATH) guidelines.

D. Staff Qualifications and Experience

The extent to which proposed labor and supervisory staff have relevant qualifications and experience in operating a public parking lot facility.

5. MBE/WBE SUBCONTRACTING PROVISIONS

See Schedule F of the Lease Agreement.

6 . CERTIFICATION OF RECYCLED MATERIALS PROVISION

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

Recycling Definitions:

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

- a. "Recovered Material" shall be defined as any waste material or by-product that has been recovered or diverted from solid waste, excluding those materials and by-products generated from, and commonly reused within, an original manufacturing process.
- b. "Post-consumer Material" shall be defined as any material or finished product that has served its intended use and has been discarded for disposal or recovery having completed its life as a consumer item. "Post-consumer material" is included in the broader category of "Recovered Material".
- c. "Pre-consumer Material" shall be defined as any material or by-product generated after the manufacture of a product but before the product reaches the consumer, such as damaged or obsolete products. Pre-consumer Material does not include mill and manufacturing trim, scrap, or broken material that is generated at a manufacturing site and commonly reused on-site in the same or another manufacturing process.
- d. "Recycled Product" shall be defined as a product that contains the highest amount of post-consumer material practicable, or when post-consumer material is impracticable for a specific type of product, contains substantial amounts of Pre-consumer Material.
- e. "Recyclable Product" shall be defined as the ability of a product and its packaging to be reused, reconditioned for use, or recycled through existing recycling collection programs.
- f. "Waste Reducing Product" shall be defined as any product that will result in less waste generated due to its use rather than another product designed to serve the same function with a greater waste generation rate. This shall include, but not be limited to, those products that can be reused, refilled or have a longer life expectancy and contain a lesser amount of toxic constituents.

7. PROPOSAL SUBMISSION REQUIREMENTS

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

A. Letter of Transmittal

The Proposer shall submit a letter on its letterhead, signed by an authorized representative, stating its experience and qualifications in meeting the requirements of this RFP. This letter shall include a statement on whether the Proposer is

submitting a proposal as a single entity, a joint venture, or is partnering with another firm in a prime/subcontracting relationship. In all cases, information required for a single entity is required for each participant in a joint venture

The Letter of Transmittal shall contain:

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

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

If an individual: a statement of residence;

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

B. Executive Summary

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

C. Agreement on Terms of Discussion

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

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

The Proposer makes the certifications in the "Contractor's Integrity Provisions," included as Attachment E, Part I, JSTC Public Parking Lot Lease No. LRR-378 of

this RFP. If the Proposer cannot make any such certifications, it shall enclose an explanation of that inability.

E. Documentation of Proposer Prerequisites

The Proposer shall submit documentation to demonstrate that it meets all prerequisites, if any, included herein.

F. Proposal

The Proposer must submit a proposal that details and clearly describes its experience and capability to perform the parking garage management and operation service, provide the revenue collection and management system, and execute the onsite management and work plans described in this RFP, as well as its approach to such work and the cost of such work to the Port Authority. At a minimum, the proposal shall include the following components:

1. Value of the Lease

The Proposer shall submit a Lease Proposal in the form provided as Attachment B – Part III. The Lease Proposal must contain the following components:

- a. Proposed Basic Rental and Percentage Rental payments, which will be evaluated based on the total value to PATII.
- b. A five-year cash flow pro forma in Microsoft Excel format that includes parking rates, revenues, operating expenses, rent payments, administrative/management expenses and profits.
- c. The Proposer shall submit a cost proposal for the Initial Work indicating the compensation it expects to receive. The Cost Proposal shall be complete, include all Cost Proposal Forms supplied in this solicitation, and be inclusive of all work required in this RFP and shall include, but not be limited to, material and labor costs, any wages, salaries, health benefits and other supplemental benefits, overheads, profits.

Cost proposal forms shall be submitted in both hard copy and in electronic spreadsheet format in Excel 2007 or later. Electronic version shall include calculations and summation for ease of reviewing the cost proposal forms.

2. Install and Maintain Revenue Collection and Management System

Proposer shall submit a design (including a narrative, schematic, and hardware specifications), construction schedule and budget to purchase and install a new RCS as described in Attachment B-Part II, “Scope of Work”.

The Proposer shall submit information to allow the Port Authority to evaluate it with respect to the technical expertise and experience as more fully set forth in Section 4 above, “Evaluation Criteria and Ranking”. The Proposal should include, but not be limited to, the Proposer’s technical expertise and experience in delivering, installing, and managing:

- a. Revenue Collection Systems for parking facilities;
- b. Utilization of technological advances in parking garages and resulting benefits;
- c. Quality of the design concept, including its innovation and compatibility with the requirements of the parking garage;

- d. Technical approach to aspects of the project that are consistent with and conform to the requirements of the parking garage;
- e. Qualifications and experience of the proposed mechanical, structural and geotechnical (as applicable) engineering firms on projects of similar size, scope and complexity.

3. Management/Staff Approach

The Proposers' management philosophy, principles and programs to be utilized by the Lessee in performing the service, and which shall include, but is not limited to, consideration of the following:

- a. A description of how Proposer will deliver and implement training to staff in operating the Facility described in the RFP
- b. Service standards, concepts and procedures that Proposer intends to implement in order to obtain a high level of service and quality of in operating a facility
- c. A description of how the Lessee will manage its staff through:
 - 1. Quality assurance and control programs
 - 2. Recruiting and retention procedures
 - 3. Self-assessment plan
 - 4. Workplace safety programs
- d. An organization chart which shows how the services in the RFP will be implemented and provided. The Proposer shall show the number of full time and part time employees to be utilized in providing these services, including supervisory staff. The Proposer shall submit a plan to minimize employee turnover. It is the Port Authority's preference to have the Proposers submit a staffing plan that maximizes the use of full time employees.
- e. Describe the Proposer's employee retention plan for this Lease Agreement.
- f. Describe the Proposer's training and workplace safety programs for this Lease Agreement.
- g. A description of how the Proposer will meet:
 - 1. Insurance requirements set forth in the Lease
 - 3. The proposed Certified Environmentally Preferable Products/ Practices Form

4. Staffing Qualifications and Experience

The Proposer shall submit information with respect to the extent to which proposed labor and supervisory staff have relevant qualifications and experience in operating a public parking lot facility.

- a. Describe the Proposer's plan to ensure that an employee who performed a similar role at the Facility under a previous Port Authority Contract suffers no diminution in wage rate under the new Lease Agreement.
- b. The Proposer should

provide a statement indicating the qualifications and experience of managerial and supervisory personnel employed by the firm who are to be exclusively dedicated to the Lease Agreement, including:

- Their length of service with the firm
- The anticipated function of each person on the Lease Agreement
- A summary of the relevant experience of each person listed
- The resumes of the individuals who are being recommended for these positions should be included in the Proposal.

c. The Proposer should provide a complete description of all employee management programs (covering both supervisory and non-supervisory personnel), currently utilized by your firm, including, but not limited to:

- Parking garage related training
- Security training
- OSHA safety training
- Employee motivation and incentive programs
- Quality Assurance/Quality Control programs
- Payroll processing
- Recruitment procedures
- Staffing retention plan
- Disciplinary procedures, etc. (include, if available, copies of manuals or other associated documents).

5. Contractor Identity Check/Background Screening Plan

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

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

G. Acknowledgment of Addenda

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

If the Proposer downloaded this RFP document, it is the responsibility of the Proposer to periodically check the Port Authority website at <http://www.panynj.gov/business-opportunities/bid-proposal-advertisements.html> and download any addenda that might have been issued in connection with this solicitation.

H. Acceptance of Lease Terms and Conditions

The Port Authority has attached to this RFP as Attachment B, Part I, JSTC Public Parking Lot Lease No. LRR-378. The Proposer is expected to agree with the Lease Agreement Terms and Conditions. However, if the Proposer has any specific exceptions, such exceptions should be set forth in a separate letter included with its response to this RFP. After the proposal due date, the Proposer will be precluded from raising any exceptions unless such exceptions are justified by and directly related to substantive changes in the business or technical requirements and are agreed to by the Proposer and the Port Authority.

I. MBE/WBE Requirements

The Proposer shall refer and adhere to Section 55 of the Lease Agreement, the Tenant Construction or Alteration Application Requirements, and Schedule E of the Lease Agreement.

8. CONDITIONS FOR THE SUBMISSION OF A PROPOSAL

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

A. Changes to this RFP

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

B. Proposal Preparation Costs

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

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

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

D. Ownership of Submitted Materials

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

E. Subcontractors

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

F. Conflict of Interest

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

G. Authorized Signature

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

H. References

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

I. Evaluation Procedures and Negotiation

Only Proposers which meet the prerequisites, if any, may have their proposals evaluated based on the evaluation criteria set forth in this RFP. The Port Authority may use such procedures that it deems appropriate to evaluate such proposals. The Port Authority may elect to initiate contract negotiations with one or more Proposers including negotiation of costs/price(s) and any other term or condition, including modifying any requirement of this RFP. The option of whether or not to initiate contract negotiations rests solely with the Port Authority.

J. Taxes and Costs

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

K. Most Advantageous Proposal/No Obligation to Award

The Port Authority reserves the right to award the Contract to other than the Proposer proposing the lowest price. The Contract will be awarded to the Proposer whose proposal the Port Authority believes, in its sole discretion, will be the most advantageous to the Port Authority. Neither the release of this RFP nor the acceptance of any response thereto shall compel the Port Authority to accept any proposal. The Port Authority shall not be obligated in any manner whatsoever to any Proposer until a proposal is accepted by the Port Authority in the manner provided in the Section of this RFP entitled "Proposal Acceptance or Rejection."

L. Multiple Contract Awards

The Port Authority reserves the right to award multiple Contracts for the products, work and/or services that are the subject matter of this RFP and Proposers are hereby

given notice that they may not be the Port Authority's only contractor for such products, work and/or services.

M. Right to Extend Lease

If this is a proposal for a contract for a term of years, including specified options for renewal, the Port Authority reserves the additional right to extend the contract term for an additional 365 days, upon the same terms and conditions of the original Contract negotiated between the Port Authority and the successful Proposer.

N. Rights of the Port Authority

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

acceptance of a proposal. Information shall be submitted within three (3) calendar days after the Port Authority's request unless a shorter or longer time is specified therein.

O. Personal Non-Liability

Neither the Directors of PATH, the Commissioners of the Port Authority nor any of them, nor any officer, agent or employee of PATH or the Port Authority, shall be charged personally by the Contractor with any liability, or held personally liable to the Contractor under any term or provision of this Agreement, or because of its execution or attempted execution, or because of any breach, or attempted or alleged breach, thereof.

P. Contractor's Integrity Provisions

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

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

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

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

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

- a. the prices in its bid have been arrived at independently without collusion, consultation,

communication or agreement for the purpose of restricting competition, as to any matter relating to such prices with any other bidder or with any competitor;

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

c. no attempt has been made and none will be made by the Bidder to induce any other person, partnership or corporation to submit or not to submit a bid for the purpose of restricting competition;

d. this organization has not made any offers or agreements or taken any other action with respect to any Authority employee or former employee or immediate family member of either which would constitute a breach of ethical standards under the Code of Ethics dated March 11, 2014, or as may be revised (a copy of which is available upon request) nor does this organization have any knowledge of any act on the part of an Authority employee or former Authority employee relating either directly or indirectly to this organization which constitutes a breach of the ethical standards set forth in said Code;

e. no person or selling agency other than a bona fide employee or bona fide established commercial or selling agency maintained by the Bidder for the purpose of securing business, has been employed or retained by the Bidder to solicit or secure this Contract on the understanding that a commission, percentage, brokerage, contingent, or other fee would be paid to such person or selling agency; and

f. the Bidder has not offered, promised or given, demanded or accepted, any undue advantage, directly or indirectly, to or from a public official or employee, political candidate, party or party official, or any private sector employee (including a person who directs or works for a private sector enterprise in any capacity), in order to obtain, retain, or direct business or to secure any other improper advantage in connection with this Contract.

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

The foregoing certifications in this Part III, Sections 1 and 2, shall be deemed to have been made by the Bidder as follows:

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

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

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

In any case where the Bidder cannot make the foregoing certifications, the Bidder shall so state and shall furnish with the signed bid a signed statement which sets forth in detail the reasons therefor. If the Bidder is uncertain as to whether it can make the foregoing

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

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

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

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

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

The policy permits a Bidder whose ineligibility has been so determined by an agency of the

State of New York or New Jersey to submit a bid on a Port Authority contract and then to establish that it is eligible to be awarded a contract on which it has bid because (i) the state agency determination relied upon does not apply to the Bidder, or (ii) the state agency determination relied upon was made without affording the Bidder the notice and hearing to which the Bidder was entitled by the requirements of due process of law, or (iii) the state agency determination was clearly erroneous or (iv) the state determination relied upon was not based on a finding of conduct demonstrating a lack of integrity or violation of a prevailing rate of wage law.

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

4. Contractor Responsibility, Suspension of Work and Termination

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

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

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

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

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

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

subsidiaries of the Port Authority.

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

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

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

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

6. Conflict of Interest

During the term of this Contract, the Contractor shall not participate in any way in the preparation, negotiation or award of any contract (other than a contract for its own services to the Authority) to which it is contemplated the Port Authority may become a party, or participate in any way in the review or resolution of a claim in connection with such a contract if the Contractor has a substantial financial interest in the contractor or potential contractor of the Port Authority or if the Contractor has an arrangement for future employment or for any other business relationship with said contractor or potential contractor, nor shall the Contractor at any time take any other action which might be viewed as or give the appearance of conflict of interest on its part. If the possibility of such an arrangement for future employment or for another business arrangement has been or is the subject of a previous or current discussion, or if the Contractor has reason to believe such an arrangement may be the subject of future discussion, or if the Contractor has any financial interest, substantial or not, in a contractor or potential contractor of the Authority, and the Contractor's participation in the preparation, negotiation or award of any contract with such a contractor or the review or resolution of a claim in connection with such a contract is contemplated or if the Contractor has reason to believe that any other situation exists which might be viewed as or give the appearance of a conflict of interest, the Contractor shall immediately inform the Chief Procurement Officer in writing of such situation giving the full details thereof. Unless the Contractor receives the specific written approval of the Chief Procurement Officer, the Contractor shall not take the contemplated action which might be viewed as or give the appearance of a conflict of interest. The Chief Procurement Officer may require the Contractor to submit a mitigation plan addressing and mitigating any disclosed or undisclosed conflict, which is subject to the approval of the Chief Procurement Officer and shall become a requirement, as though fully set forth in this Contract. In the event the Chief Procurement Officer shall determine that the performance by the Contractor of a portion of its Services under this Agreement is precluded by the provisions of this numbered paragraph, or a portion of the Contractor's said Services is determined by the Chief Procurement Officer to be no longer appropriate because of such preclusion, then the Chief Procurement Officer shall have full authority on behalf of both parties to order that such portion of the Contractor's Services not be performed by the Contractor, reserving the right, however, to have the Services performed by others and any lump sum compensation payable hereunder which is applicable to the deleted work shall be equitably adjusted by the parties. The Contractor's execution of this document shall constitute a representation by the

Contractor that at the time of such execution the Contractor knows of no circumstances, present or anticipated, which come within the provisions of this paragraph or which might otherwise be viewed as or give the appearance of a conflict of interest on the Contractor's part. The Contractor acknowledges that the Authority may preclude it from involvement in certain disposition/privatization initiatives or transactions that result from the findings of its evaluations hereunder or from participation in any contract, which results, directly or indirectly, from the Services provided by the Contractor hereunder. The Port Authority's determination regarding any questions of conflict of interest shall be final.

ATTACHMENT A
AGREEMENT ON TERMS OF DISCUSSION

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

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

(Company)

(Signature)

(Title)

(Date)

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

Rev. 8/5/16

**ATTACHMENT B
TABLE OF CONTENTS**

PART I LEASE

PART II SCOPE OF WORK

PART III LEASE PROPOSAL FORM

ATTACHMENT B

PART I – LEASE (See attached)

ATTACHMENT B

PART II – SCOPE OF WORK: LEASING, MANAGEMENT, MAINTENANCE, AND OPERATION OF PARKING GARAGE AT JOURNAL SQUARE TRANSPORTATION CENTER (JSTC)

1. GENERAL INFORMATION

The Lessee will enter into a Lease Agreement to provide management, operations, and maintenance services at the Facility. With the exception of the Initial Work as described in Item 2 below, the cost of all management, operations and maintenance shall be the responsibility of the Lessee. The Lessee will be expected to set parking rates consistent with the local market and manage capacity pursuant to industry standards (which may include a valet component to supplement current self-park operations). Proposals should include a rent offer in the Lease Proposal Form attached as Attachment B, Part III that maximizes revenues to the Port Authority. Rent proposals should include both a guaranteed Basic Rental and a substantial Percentage Rental, and will be evaluated based on the total revenue generated for the Port Authority.

The Lessee will operate the facility in a manner that complies with the Rules and Regulations of PATH (See Attachment G), including but not limited to times of operation, security requirements, services, and pricing agreements. The term of the Lease shall be five (5) years, with the Port Authority having the option to extend the term for two (2), two (2)-year option periods followed by one (1), one (1)-year option period.

The Facility has five hundred and thirty-nine (539) parking spaces, including fifteen (15) handicap accessible spaces. Of the five hundred and thirty-nine (539) spaces, two hundred and fifty-five (255) spaces and eight (8) handicap spaces are located on the first level, and two hundred and sixty-nine (269) spaces and seven (7) handicap spaces are located on the open-roof second level. This total excludes approximately ninety (90) spaces that will remain unavailable during the term of the lease due to security infrastructure that blocks the spaces. The Port Authority will maintain the right to use a certain number of parking spaces. The number of spaces currently utilized by the Port Authority is detailed in Section I(M) of this RFP (“Aid to Proposers”). It is anticipated that the value of these spaces will be provided as a credit against the Lessee’s rental payments, pursuant to the terms of the Lease. The remaining parking spaces shall be available to the public at a price set by the Lessee and subject to review and approval by the Port Authority.

The location of the Facility is 16 PATH Plaza in the Journal Square section of Jersey City. The Facility has a prime location in a fast growing neighborhood, and has convenient access to the Journal Square PATH station and bus lanes. The Facility currently fills to capacity Monday through Friday and demand is expected to increase due to new development in the surrounding area. For informational purposes, current parking rates and sales are detailed in this RFP, Section M: “Aid to Proposers. The Facility is accessed via a helix-shaped ramp (the “Helix”) located at Summit Avenue and Magnolia Avenue.

Each month the Lessee will report to the PATH Facility Manager the exact number of spaces used by the Port Authority for that month.

The Lessee’s responsibilities shall include staffing the operation of the Facility, maintaining continuous service, installing improvements, removing snow and ice, and replacing the existing revenue control system, as further described below.

The Port Authority anticipates that the successful Proposer will have thirty (30) calendar days from the date of the lease award to the commencement of operations. During this timeframe, the selected Proposer must, at a minimum, procure all necessary labor and supervision, provide all essential training, and obtain required uniforms and equipment, such as snow removal vehicles and equipment, and complete necessary background investigations.

2. CAPITAL IMPROVEMENTS TO BE PERFORMED BY THE LESSEE

The Lease will require that the Lessee implement an initial scope of repair work in order to bring the Facility to a condition consistent with industry standards and perform capital improvements associated with a new RCS (collectively, the “Initial Work”). Proposers must include plans, a schedule and budget as part of their response. It is anticipated that the cost of the Initial Work will be offset by a credit against the rent paid by the Lessee over the term of the Lease.

Currently, the Facility utilizes a cash-only collection system, in which parking customers pay personnel stationed at the booth at the exit. Proposers are asked to propose a new RCS as part of their submissions for this RFP. The new RCS shall accept multiple payment methods including, but not limited to, cash and credit/debit card (including chip technology), and may also accept EZ-Pass and mobile payment technology. Proposals may include upgrades to the existing payment infrastructure at the entry/exit lanes, as well as pay-on-foot (POF) automated payment machine(s) that accept payments and dispense change. Proposers may propose that POF machines be installed in locations through the JSTC facility, although installation locations are subject to approval by the Port Authority and the Facility Manager.

The electronic payment systems newly installed at this facility shall meet the Payment Card Industry Data Security Standards (PCI), and the U.S. Fair and Accurate Credit Transactions Act (FACTA), and/or any industry accepted applicable laws or national standards. More information is available at <https://www.pcisecuritystandards.org>. Proposers are advised that power supply and basic telephone connections are available in the existing cashier booths at the entry/exit lanes. In addition, power supply may available in certain interior locations subject to approval by the PATH Facility Manager.

The Initial Work to be performed by the Lessee will satisfy minimum standards as detailed below. In the event that the new RCS requires a reconfiguration of the existing entry/exit location, any such reconfiguration must be consistent with these standards:

- a. Number of lanes – Total of four (4) lanes. One (1) By-Pass Lane; Two (2) Lanes to service the rush hour traffic pattern; One (1) Lane to service opposite rush-hour traffic pattern;
- b. Width of lanes – The current width of the one (1) By-Pass Lane is 8’-4””; the width of the other three (3) lanes are 8’-1””. These dimensions are to be upheld at a minimum. Proposers may propose wider lane designs for consideration;
- c. Curbs – Rusted curbs must be replaced;
- d. Potholes shall be repaired;
- e. Paint – The Lessee shall repaint the Facility as needed;
- f. Roof of entry/exit pavilion – The pavilion roof structure currently supports security camera & lighting infrastructure, and protect equipment from poor weather conditions. Any reconfiguration must take these functions into consideration;
- g. Lighting – Existing lighting at the entry/exit lanes shall be maintained. Any deficient lighting at the Facility shall be repaired/improved consistent with industry standards;
- h. Security camera system – Existing security camera system shall be maintained;
- i. Sewer drain – Existing sewer drain shall be maintained;

- j. Traffic spikes – The traffic spikes located at the entry/exit point currently do not function and may be removed; and
- k. Below-grade infrastructure – Proposers should be aware that there is an electrical and communication supply located below grade on the west end of the booth.

Subsequent to completion of the Initial Work, the selected Proposer shall be responsible for performing and funding ongoing maintenance, aesthetic improvements and operational investments to the Facility. Such improvements and investments occurring at a minimum every two (2) years shall be the refurbishment of the parking lot to provide new coating, striping, and any needed masonry repair, but exclude all structural improvements and paving. PATH is responsible for these improvements. The selected Proposer must comply with the rules and regulations outlined in the Lease, including upholding the set hours of operation, security requirements, required services, and pricing agreements. Additionally, within the first period of the Lease, the Lessee shall provide new street and parking levels signage, to be approved by PATH facility management.

Pursuant to Port Authority construction requirements, the Lessee shall reference the “Tenant Construction and Alteration Process” (TCAP) in Attachment H. to identify the processes to follow for any alteration done on PATH property. For the electronic version of the TCAP manual click on <http://www.panynj.gov/business-opportunities/tcap/pdf/tcap-manual.pdf>).

3. SNOW AND ICE REMOVAL PLAN:

Removing snow and ice efficiently and effectively from the Facility is a key responsibility of the Lessee. The cost of snow and ice removal is the responsibility of the Lessee. Specific responsibilities and regulations are detailed below and are set forth in Exhibit SR to the Lease Agreement.

- (a) The Lessee is solely responsible for removing snow and ice from the entirety of the Facility, including but not limited to its crosswalks, parking decks, entrance and exit ramps, interior roadways, emergency exits, and toll plazas. Roadways, including ramps and crosswalks, must be kept clear of snow and ice and maintained by Lessee using chemicals approved in advance by PATH.

During a winter storm event, it is expected that the rooftop parking deck will remain open to the public, even during snow removal operations. Exceptions are permissible, upon receiving approval from PATH, if safety concerns arise.

- (b) The Lessee shall have a dedicated snow and ice removal vehicle to be solely used at the Facility. The vehicle shall be a full sized four-wheel drive pickup truck (Chevy 2500 series, GMC 2500, Ford 250 or PATH approved equal) with an eight-foot (8) wide power angle western snow plow and a one-ton Salty Dog gas-fired salt spreader, or PATH-approved equal. The vehicle shall be equipped with back-up alarms, and rotating amber beacon to facilitate personnel backup protection in active roadway areas. The vehicles shall not be more than two (2) model years old, as of the date of the Lease’s execution.
- (c) When the forecasted snow accumulation is four (4) inches or more, the Lessee will be required to hire a professional Snow/Ice removal Contractor to be on-call and respond to the Facility at the start of a storm. The Contractor must be certified, bonded, fully insured, and

capable of managing the winter weather problems. All costs associated with this on-call Contractor shall be borne by the Lessee.

Services of the Contractor will include, but are not be limited to: snow plowing, snow removal and hauling, salt and sanding for both pre- and post-treatment, and dump truck services.

- (d) Snow may be piled to a height not to exceed four (4) feet. Piling of snow along the north and south walls is permitted on the rooftop parking level. Piling of snow outside of the entrance to the tollbooths is permitted but may not exceed a height of three (3) feet. If snow piles exceed a height of four (4) feet, the Lessee will be responsible for hauling the snow to a designated nearby site approved by PATH.
- (e) Entrance and exit ramps, in addition to the five (5) parking spaces near the exit, the six (6) emergency exits, and all drains, on the rooftop parking deck are to be free of snow and ice. Snow may be piled in the area near these ramps if it can be accomplished without restricting access to the five (5) designated snow-free parking spaces.
- (f) The Lessee shall use only such chemicals to melt snow and ice as shall be consented to in advance by PATH.
- (g) Approved snow and ice removing chemicals must be applied to all parking ramps at least two (2) hours prior to a predicted snowfall.
- (h) The Lessee is responsible for any damage caused by snow and ice removal operations.
- (i) The Lessee will be required to provide a skid steer loader equal to or better than that of a John Deere model 318D to remain at the Facility from November 1 through March 31 for the duration of the Lease. All costs related to the vehicle, including, but not limited to, fuel, oil, maintenance, and any liability insurance shall be borne by the Lessee.

In accordance with these responsibilities, the Lessee must submit a snow and ice removal plan to PATH for approval. The plan should include a description of the dedicated snow and ice removal vehicles and machines that will remain on site during the snow season, in addition to subcontractor services that can be made available during major weather events. Furthermore, the plan should detail snow and ice removal procedures that clearly explain how snow and ice will be cleared from the parking decks and where it will be piled. The plan should consider how to remove and pile snow so as to not damage the parking lot and its structural integrity, and also how to maintain sight lines and reduce blind spots from piled snow. A diagram should be included that explicitly shows which parking spaces will be dedicated to snow piles and the anticipated loss of revenue associated with the lost space.

4. REPORTING

In addition to the reporting requirements under the Lease, the Lessee shall report metrics on market demand and supply, pricing, revenues/expenses and construction costs. PATH may call upon the Lessee to cooperate with a cost-benefit study to determine the viability of constructing a third deck at the Facility in addition to any and all other requested reports.

ATTACHMENT B

PART III - LEASE PROPOSAL FORM

1. Proposers are asked to complete the blanks below.

Rental Payments

A. Basic Rental: \$ _____

B. Percentage Rental:

i. Estimated Annual Gross Receipts*: \$ _____

ii. Percentage Rent Threshold: \$ _____

iii. Percentage: The Lessee shall pay to PATH _____ % of Gross Receipts above the Percentage Rent Threshold

iv. Estimated Annual Percentage Rental Payment: \$ _____

C. Total Estimated Payment (Basic + Percentage Rental): \$ _____

Note: Proposers may provide an attachment to this section to describe their rental payment proposals

2. Proposals must include a five-year cash flow pro forma in Microsoft Excel format showing expected parking rates and revenues, operating expenses, rent and profit. A template is provided on the following page as an example.
3. Proposals must include a design (including a narrative, schematic and hardware specifications), construction schedule and budget (including any administrative fee, to be broken out separately from direct costs) to perform the Initial Work.

*Gross receipts shall include any rent credits received by Lessee for use of spaces by PATH or the Port Authority, as described in Section 70a of the Lease Agreement.

ATTACHMENT B

PART III LEASE PROPOSAL FORM, CONTINUED

Following is a template for the pro forma, which Proposers must submit in Microsoft Excel format. This template is provided as an example only; Proposers may provide additional information as applicable.

Parking Rates	
1 Hour	
4 Hours	
7 Hours	
12 Hours	
Daily	
Monthly	

	Year 1	Year 2	Year 3	Year 4	Year 5
Revenues					
Number of Parkers <i>(break out by hourly-daily-monthly)</i>					
Parking Revenue <i>(break out by hourly-daily-monthly)</i>					
Other Income					
GROSS RECEIPTS					
Parking Tax					
NET REVENUES					
Operating Expenses					
Rent – Basic Rental					
Rent – Percentage Rental					
Wages/Payroll Taxes/Benefits					
Utilities					
Telephone					
Repairs/Maintenance					
Printing/Tickets					
Uniforms					
Supplies					
Insurance					
Auto Damage					
Bank Charges/Credit Card Fees					
Administrative/Management					
TOTAL OPERATING EXPENSES					
NET OPERATING INCOME					
Capital Expenses					
Capital Repairs <i>(break out by line item)</i>					
Revenue Collection System					
Administrative/Management					
Offset – Rent Credit from Landlord					
NET CASH FLOW					

ATTACHMENT C- PROPOSER REFERENCE FORM

Name of Proposer: _____

Please provide a list of references on the firm's performance of similar work within the last five (5) years, including all current contracts. Use additional sheets as necessary.

Include the following information for each reference:

Customer Name: _____

Address: _____

Contact Name and Title: _____

Phone and Fax Numbers of Contact: _____

Contract date(s): _____

Contract cost: _____

Description of work: _____

Customer Name: _____

Address: _____

Contact Name and Title: _____

Phone and Fax Numbers of Contact: _____

Contract date(s): _____

Contract cost: _____

Description of Work: _____

Customer Name: _____

Address: _____

Contact Name and Title: _____

Phone and Fax Numbers of Contact: _____

Contract date (s): _____

Contract cost: _____

Description of work: _____

ATTACHMENT D - Certified Environmentally Preferable Products/Practices

Proposer Name: _____ Date: _____

In line with the Port Authority's efforts to promote products and practices which reduce our impact on the environment and human health, Proposers are encouraged to provide information regarding their environmentally preferable/sustainable business practices as they relate to this contract wherever possible. Proposers **must** complete this form and submit it with their response, if appropriate. Proposers **must** submit appropriate documentation to support the items for which the Proposer indicates a "Yes" and present this documentation in the proper sequence of this Attachment.

1. Packaging

Has the Proposer implemented any of the following environmental initiatives? (A checkmark indicates "Yes")

- _____ Use of corrugated materials that exceed the EPA recommended post-consumer recycled content
- _____ Use of other packaging materials that contain recycled content and are recyclable in most local programs
- _____ Promotes waste prevention and source reduction by reducing the extent of the packaging and/or offering packaging take-back services, or shipping carton return
- _____ Reduces or eliminates materials which have been bleached with chlorine or chlorine derivatives
- _____ Eliminates any packaging that may contain polyvinyl chloride (PVC), or polystyrene or heavy metals

If yes, a description of the practices being followed must be included with the submission.

2. Business Practices / Operations / Manufacturing

Does the Proposer engage in practices that serve to reduce or minimize an impact to the environment, including, but not necessarily limited to, the following items? (A checkmark indicates "Yes")

- _____ Recycles materials in the warehouse or other operations
- _____ Use of alternative fuel vehicles or vehicles equipped with diesel emission control devices for delivery or transportation purposes
- _____ Use of energy efficient office equipment or signage or the incorporation of green building design elements
- _____ Use of recycled paper (that meets federal specifications) in their marketing and/or resource materials
- _____ Other sustainable initiative

If yes, a description of the practices being followed must be included with the submission.

3. Training and Education

Does the Proposer conduct/offer a program to train or inform customers and employees of the environmental benefits of the products to be offered under this contract, and/or does the Proposer conduct environmental training of its own staff?

Yes No If yes, Proposer must attach a description of the training offered and the specific criteria targeted by the training.

4. Certifications

Has the Proposer or any of its manufacturers and/or subcontractors obtained any of the following product / industry certifications? (A checkmark indicates "Yes")

- _____ ISO 14000 or adopted some other equivalent environmental management system
- _____ Other industry environmental standards (where applicable), such as the CERES principles, LEED Certification, C2C Protocol, Responsible Care Codes of Practice or other similar standards
- _____ Third Party product certifications such as Green Seal, Scientific Certification Systems, Smartwood, etc.

If yes, Proposers must attach copies of the certificates obtained.

5. Other Environmental Criteria

Proposers are encouraged to respond to criteria specifically indicated in this RFP as "Management Approach" (and attach the appropriate documentation) to receive consideration in the evaluation.

I hereby certify, under penalty of the law that the above statements are true and correct.

_____ Name _____ Date

ATTACHMENT E
RULES AND REGULATIONS OF THE PORT AUTHORITY TRANS-HUDSON SYSTEM
(PATH) (See attached)

RULES AND REGULATIONS OF THE PORT
AUTHORITY TRANS-HUDSON (PATH) RAIL
SYSTEM

Effective December 20, 2015

I. Definitions

“Bus” shall mean a self-propelled highway vehicle designed and constructed for the carriage of passengers for hire, employing as a source of motive power (either directly or by electrical transmission) a reciprocating or rotary internal-combustion or turbine engine (not including a jet propulsion engine) utilizing as fuel, gasoline, diesel oil or any other substance utilized by highway vehicles for fuel and permitted by the laws of New Jersey then in effect, and having overall dimensions not in excess of the following: length, forty-five (45) feet; width, one hundred and two (102) inches; height, twelve (12) feet eight (8) inches, and having a maximum gross loaded weight not in excess of thirty-five thousand (35,000) pounds avoirdupois, distributed to provide no more than twenty thousand (20,000) pounds per axle; provided however, that larger or heavier passenger-carrying vehicles may be operated at the Center by prior mutual consent of PATH and the operator and each such shall be deemed, for the period of such operation by consent, a “bus.”

“Carrier” shall mean an operator of one or more vehicles for the transportation of passengers for hire.

“Center” shall mean the Journal Square Transportation Center and its entire area including roadways and structures, which comprises the Center.

“Electronic cigarette” shall mean an electronic device that delivers vapor which is inhaled by an individual user.

“Fare zone” shall mean the areas of the PATH system for which payment of a fare or use of a PATH authorized non-revenue credential is required for entry by a passenger.

“Manager of the Center” or “Manager” shall mean the person or persons from time to time designated by PATH to exercise the powers and functions vested in the said Manager with respect to the Center by these Rules and Regulations, including the Manager of the Journal Square Transportation Center, the Acting Manager of the Journal Square Transportation Center for the time being or the duly designated representatives of such persons.

“PATH” refers to The Port Authority Trans-Hudson System, including the Center.

“PATH system” shall refer to the PATH rail system, its rolling stock and its stations.

“Parking” shall mean the halting of a vehicle on a roadway or other area while not actually engaged in receiving or discharging passengers, except when halted in obedience to traffic regulations, signs or signals, and without regard to the presence or absence of the driver.

“Passenger” shall mean any natural person who rides on a rail car operated by the PATH system, other than a PATH employee or a PATH contractor engaged in the performance of his or her duties, including a Port Authority Police Officer.

“Person” shall mean any individual or natural person, and any firm, partnership, corporation or incorporated or unincorporated association, and shall include any assignee, receiver, trustee, executor, administrator or similar representative appointed by a court, and shall mean the United States of America or any department of the government thereof, any state or political subdivision thereof, any foreign government or political subdivision thereof, or the United Nations.

“Port Authority” shall mean The Port Authority of New York and New Jersey.

“Stand” shall mean to halt a bus for the purpose of loading or unloading or for waiting in position for loading or unloading.

“Rules” shall refer to the Rules and Regulations of the Port Authority Trans-Hudson System (PATH)

“U.S. Department of Transportation regulations” shall mean regulations of the U.S. Department of Transportation as from time to time in effect.

“Vehicle” shall mean and include automobiles, trucks, buses, trailers, semi-trailers, and any other devices in or upon or by means of which any person or property is or may be transported, carried or drawn upon land only, except railroad rolling equipment or other devices designed to operate only on stationary rails or tracks.

II. Application

These Rules regulate conduct on and within on any portion of the PATH, including the Center, unless reference is made to any specific portion of PATH, in addition to any applicable laws, ordinances or regulations of other government bodies.

III. General Conditions

- A. No passenger shall enter the PATH system fare zone unless he or she has paid the required fare or has used a PATH authorized non-revenue credential.
- B. No person shall pass through any portion of the PATH system except a person intending to board a PATH train or who has recently disembarked from a PATH train, except as otherwise provided herein. All passengers must vacate any rail

car operated by PATH and exit from the PATH system fare zone when the rail car reaches a terminal station.

- C. The Port Authority may prohibit any conduct that violates any requirement for, or condition of, the receipt of federal grant in aid funds, or any other governmental program in which the Port Authority participates to obtain funds for use at PATH.
- D. Permission to use PATH or be on PATH property may be denied to or withdrawn from persons who violate these Rules, applicable laws, ordinances or regulations of other government bodies or for such other reason as may be permitted by law.
- E. Nothing herein contained shall be construed to limit the use of any area or portion of PATH by officers or employees of the Port Authority or PATH, or by Port Authority or PATH contractors, or to prevent any Police Officer, Fire Officer or other public officer or employee from entering upon any part of PATH when properly required so to do in the performance of his official duties.
- F. Access to Closed and Restricted Areas
 - 1. No person except a person assigned to duty therein shall enter without permission of PATH any area posted as a closed area or otherwise identified as closed.
 - 2. No person shall enter without authorization any area posted as a restricted area or otherwise identified as a restricted area unless such person complies with such restriction.

IV. Safety

- A. No person shall touch any other person without his or her consent.
- B. No person shall litter, leave refuse, or create any unsafe or unsanitary condition.
- C. Except with the permission of PATH, no person shall bring into or carry in PATH any radioactive materials, explosives, acids, flammables, compressed gases or articles or materials having or capable of producing strong or offensive odors, or articles or materials likely to endanger persons or property, in any container whatsoever, including the fuel chambers of portable vehicles and tools.
- D. 1. No person shall bring into, cause to be brought into, or keep in PATH any signal-flare or any container filled with or which has been emptied or partially emptied of petroleum products, paint or varnish, except with the permission of PATH.

2. Any such articles or materials brought into, caused to be brought into, or kept in PATH pursuant to such permission shall be stored in appropriate receptacles in rooms or areas approved therefor by PATH.
3. The presence of the following at the Center shall not be a violation of this regulation:
 - (a) Gasoline or other motor fuel contained in a non-pressurized tank permanently attached to a vehicle.
 - (b) Kerosene signal-flares in good condition required or permitted by U.S. Department of Transportation regulations stored in buses in accordance with such U.S. Department of Transportation.
- E. No person shall use flammable liquids for cleaning without permission of PATH.
- F. No tag showing the date of last inspection attached to a unit of fire extinguishing and/or fire fighting equipment shall be removed therefrom, except by permission of PATH.
- G.
 1. No person shall create, or permit any machine or vehicle of which such person is in charge to create, obnoxious odors, noxious gases, smoke or fumes.
 2. The creation of internal-combustion engine exhaust fumes by vehicles in the Center, which are maintained and are being operated in a manner in compliance with these Rules shall not be a violation of this regulation.
- H. No person shall spit, urinate or defecate on any part of the PATH except in a urinal or toilet intended for that purpose.
- I. No person shall store bundles, paper, cloth, cardboard or any other material in solid, liquid or gas form that could in any way pose a fire or safety hazard or obstruct or hinder passage without the express, written approval of PATH.
- J. No person shall use a skateboard or rollerskates or use shoes equipped with skate wheels as skates, or ride a bicycle, scooter or any other self propelled vehicle or device, except a wheelchair or other ambulatory device assisting a disabled person, on or through any building, area, car or other rolling stock of PATH.
- K. No person shall cook, light a fire or otherwise create a fire or life safety hazard.
- L. No person shall do or permit to be done anything which may interfere with the effectiveness or accessibility of any of the following within PATH: fire protection, heating, lighting, electrical, signal, sprinkler, drainage, alarm, telephone, public announcement, closed circuit television inter-communication,

plumbing, air conditioning or ventilation system; fire hydrant, standpipe, hose or fire extinguisher; PATH emergency response vehicle or associated equipment and materials; or other equipment installed at a PATH station, building, area or location. No person shall operate, adjust or otherwise handle or manipulate, without permission of PATH, any of the aforesaid systems, machinery, equipment or devices, or portions thereof, or any other systems, machinery, equipment or devices installed or located in PATH.

- M. No person shall make any sound in excess of 86 dBA on the A weighted scale measured at 5 feet from the source of the sound in any interior space.
- N. No person shall make any sound that interferes with the ability of persons to hear any announcement made over the public address system of PATH, or by a police officer, or by an employee of the PATH, The Port Authority of New York and New Jersey or any subsidiary thereof;
- O. No person shall unreasonably interfere with rail, pedestrian or vehicular traffic flow, the formation or progress of any line of persons waiting for service, such as a line at a telephone, vending or information kiosk, bus or bus stop or gate, taxi loading area, or automatic teller machine, or any construction or maintenance activity.
- P. No person shall erect any permanent or temporary structure on any property of PATH without the express written permission of PATH's Director/General Manager.
- Q. No person within the PATH system shall do or omit to do any act if the doing or omission thereof unreasonably endangers persons or property in addition to the absence or presence of any specific prohibition or permission in these Rules.
- R. No person shall hang from or lean upon any railing or handhold in any PATH rail car.
- S. No person shall engage in any dance, or acrobat exhibition, in any PATH rail car.

V. Personal Conduct

- A. No person shall play or operate any musical instrument or device, tape or disc player, radio or television anywhere on PATH property except with the use of personal headphones or earphones producing sounds audible only to the user thereof.

- B. No person shall plug a television, radio or other electrical device into any electrical outlet or connect any device to any utility at, in or supplying power to, the PATH system or the Center.
- C. No person shall eat any food or drink any beverage on the station platforms of PATH or while aboard any rail car operated by PATH.
- D. No person shall sell or distribute any food or drink, with the exception of employees of lessees or permittees of PATH who are authorized to engage in such activity pursuant to an agreement with PATH and/or the Port Authority.
- E. No person other than authorized employees of the Port Authority, PATH or a Port Authority or PATH contractor in areas designated for that purpose, shall bathe, shower or shave, or launder or change clothes, or remain undressed, anywhere on property or rolling stock owned or controlled by PATH.
- F.
 - 1. All persons finding lost articles on the PATH system shall deliver them to the PATH Police Desk located at the Journal Square Station, Jersey City, New Jersey.
 - 2. Articles unclaimed by the owner(s) will be turned over to the finder, other than a PATH or Port Authority employee, as provided in applicable PATH or Port Authority regulations, policies and procedures.
- G. No person shall engage in commercial conduct except pursuant to an agreement for the use of space therefore with PATH and/or the Port Authority.
- H. No person shall gamble or conduct or engage in any game of chance. The foregoing does not apply to sales of government lottery tickets within space occupied pursuant to an agreement with PATH and/or the Port Authority permitting such activity.
- I. No person shall deface, mark, break, or affix any sign or any other item to, or otherwise damage or alter, any part of PATH or any property thereof, except an employee of the Port Authority or PATH or a contractor of the Port Authority or PATH, engaged in the performance of his or her duties.
- J. Nor shall any person remove, alter or deface any barricade, fence or sign, except an employee of the Port Authority or PATH or a contractor of the Port Authority or PATH, engaged in the performance of his or her duties.
- K.
 - 1. No person shall enter in or upon PATH with any animal that is not properly confined for shipment.

2. Paragraph 1 does not apply to:

- (a) A Port Authority Police Officer or other person employed by PATH or the Port Authority authorized to be accompanied by an unconfined animal as part of the person's duties.
- (b) A disabled person accompanied by the person's assistance animal such as a "seeing eye dog."

- L. No person shall panhandle, beg or solicit the immediate contribution of money.
- M. No person shall drink, or carry an open container of, any alcoholic beverage.
- N. No person shall smoke or carry a lighted cigar, cigarette, or pipe containing tobacco or any other substance anywhere else within the PATH system or interior portions of the Center.
- O. No person shall smoke or carry a lighted electronic cigarette within the PATH system or interior portions of the Center.
- P. No person shall transport, in bulk, any materials or goods, including recyclable items, on the PATH system.
- Q. No Passenger on any rail car operated by PATH may sleep or occupy more than one seat.
- R. No person shall sleep, or lie down or sit on any floor, ledge, platform, step or escalator, within or at any PATH property.
- S. No one shall chain or otherwise affix a bicycle to any railing, pole or any physical object other than a designated bicycle rack.

VI. Elevators & Escalators

- A. Passenger elevators and escalators shall not be used to carry freight.
- B. An elevator for the handling or freight service will be operated in accordance with an established schedule, if any, for such elevator, unless the arrangements are made for operation at other times.

- C. The use of any escalator, elevator, private right-of-way or truck loading dock at the Center is subject to the direct control of the Manager.
- D. No person shall transport any goods or materials whose total weight exceeds one thousand (1000) pounds on any elevator in the Center without having obtained the prior permission of the Manager and without following the directions of the Manager issued when such permission is granted.
- E.
 - 1. No unauthorized person shall cause an elevator or escalator to stop by means of an emergency stopping device unless continued operation would appear to result in probable injury to a person or persons.
 - 2. Any such stopping should be reported immediately to the nearest available PATH Control Center by use of a Patron Assistance Telephone, or to the Manager if the elevator or escalator is located within the Center.
- F. No wheeled conveyance of persons or merchandise, including dollies, handtrucks, suitcases, backpacks, or strollers, shall be used on an escalator by resting the wheels of such conveyance on the steps of the escalator. Enclosed conveyances carrying merchandise, such as suitcases and backpacks, may be hand-carried on an escalator, provided that the contents are fully enclosed by the conveyance. Conveyances carrying persons, such as strollers, and unenclosed conveyances, such as handtrucks, may be carried on an escalator only if they are emptied of their contents, folded into the smallest size possible, and both the conveyance and its contents may be safely and securely hand-carried on the escalator.

VII. Journal Square Transportation Center

- A. The regulations contained in this part shall apply to the Journal Square Transportation Center or "Center."
- B. No person shall travel or remain in, or permit any vehicle of which such person has charge to travel or remain in, any portion of the Center except upon the roadways, walks or other places or areas provided for the particular class of traffic. No person shall occupy, or permit any vehicle of which such person has charge, to occupy the walks, roadways, entrances, exits, waiting rooms or other areas of the Center in such a manner as to hinder or obstruct their use by others.
- C. No person shall pass through the Bus Station portion of the Center except:
 - 1. A person employed by or doing business with a carrier whose duties require such passage.
 - 2. An authorized representative of PATH or the Port Authority.

3. A person granted permission by PATH or the Port Authority.
 4. A person intending to board a bus scheduled to depart within 30 minutes or less, or has disembarked from a bus which arrived no more than 30 minutes earlier.
- D. Persons using public parking levels shall pay all parking charges as established and approved by PATH.
- E. PATH may require that any payments made pursuant to these Rules or to any tariff or schedule of charges duly adopted and applicable to the Center be supported by records and books of account which the user shall maintain in accordance with accepted accounting practices, to be subject to audit by PATH, its agents or employees, permitted at any time during ordinary business hours.
- F. All persons doing business in the Center shall provide fire protection appliances and systems as required by PATH, by any code(s) which PATH has stated in writing are applicable to or shall be adhered to by PATH, and by National Fire Protection Association standards.
- G. Vehicles
1. The Manager of the Center shall have the authority to deny access to the Center to any bus or other vehicle not maintained, operated, and registered in accordance with these regulations, or which is otherwise in violation of these Rules or the laws, ordinances or regulations of the United States, the State of New Jersey, or the City of Jersey City, and shall have the authority to require removal of any such vehicle from the Center on five (5) minutes' notice. In the event the vehicle is not so removed, PATH may remove it under the provisions of Paragraph 16 below.
 2. No vehicle which, in the opinion of the Manager, is loaded in such a manner, or with such materials, or which is so constructed, operated, equipped or maintained, as to endanger or to be likely to endanger persons or property, or to obstruct traffic, shall be permitted in or upon the Center.
 3. No vehicle will be permitted in or upon the Center which has a weight or dimensions larger than the maximum herein established for buses or which utilizes any fuel not permitted as a source of motor power for buses, as defined in these regulations.
 4. No motor vehicle shall be permitted in the Center, which is not registered in accordance with the provisions of the laws of the State of New Jersey.

5. No person shall operate a motor vehicle in or upon any part of the Center except persons duly authorized to operate such a motor vehicle in the State of New Jersey.
6. Except when standing in a bus space, a bus driver shall stand his or her vehicle in the Center only at a space designated for such vehicle by the Manager or other authorized PATII representative. Where space is used in common by the buses of more than one carrier, a bus driver shall cause his or her bus to stand in the most forward portion of such space available upon arrival, and shall, except when passengers are actually boarding or leaving the bus, continually move his or her bus forward, toward, and to the most forward vacant portion of the space, and shall, except when passengers are actually boarding or leaving the bus, move or remove his or her bus to avoid blocking egress of a bus ready for departure.
7. The driver of any vehicle involved in an accident within the Center resulting in injury or death to any person or damage to any property shall immediately stop such vehicle at the scene of the accident, render such assistance as may be needed, and give his name, address, the number of his driver's license, and the registration number of the vehicle to the person injured or to any Police Officer. The driver, operator, or owner of such vehicle shall make a report of such accident in accordance with the law of the State of New Jersey, and shall deliver a copy of said report to the Manager within seven (7) days of the occurrence.
8. No unauthorized person shall tamper with any vehicle, start the motor thereof, move the vehicle, or otherwise interfere with the operation thereof at the Center.
9. Except to the extent specifically permitted in any written agreement between PATII and the carrier, no person shall fuel, defuel, lubricate, clean or repair a vehicle or any part thereof at the Center without permission.
10. Every driver who causes a vehicle to park or stand in the Center for three (3) or more minutes shall turn off its motor.
11. Prolonged sounding of the horns of vehicles in the Center is forbidden.
12. No person shall leave a vehicle unattended in the Center without first having made sure that its motor is turned off and its parking brakes set.
13. (a) Except for vehicles that are parked in designated public areas or

are occupying a permanently assigned space, no vehicle shall remain in the Center for longer than the time necessary for permitted operations in connection therewith, and, unless a shorter time limitation is elsewhere imposed, no vehicle shall remain in the Center for longer than thirty (30) minutes.

(b) Within five (5) minutes notice, which may be given orally to the driver, the Manager shall have authority to require the removal from the Center of any vehicle which shall have been standing or parked at the Center in excess of prescribed limits; in the event the vehicle is not so removed, PATH may remove it under the provisions of Paragraph 16 below.

14. (a) Drivers of vehicles in the Center must at all times comply with any traffic order, signal or direction given by voice or by hand, of an authorized representative of the PATH or the Port Authority.

(b) When traffic is controlled by traffic lights or signs or by mechanical or electrical signals, such lights, signs and signals shall be obeyed unless and authorized representative of PATH or the Port Authority, then directs otherwise.
15. Unless other provision for reports is expressly made, each driver of a bus of any carrier shall report to the Manager or his representative immediately upon arrival at the Center, shall pay all fees required, shall give information of the expected time of departure, and shall immediately before departure check out at the office of the Manager.
16. Unless other provision for the removal of disabled vehicles has been made by agreement, PATH may cause the removal from the Center (or to a different location in the Center) any vehicle which has become disabled, which may interfere with vehicular or pedestrian traffic or construction or maintenance activities in the Center, or whose operation or presence is in violation of these Rules, and whose operator has refused or failed to remove such vehicle.

II. Loading Docks

1. Truck loading docks in the Center shall be used for immediate transfer of merchandise between the freight elevators and trucks, and merchandise shall not be stored or held on a truck loading dock awaiting the arrival of trucks or transfer to premises or space at the Center.
2. Truck loading docks shall be used in the manner directed by the Manager.

I. Trash Removal

All persons occupying space at the Center are shall deposit, or cause to be deposited, such trash contained in, or generated at, such space in the compactor provided by the Manager for such purpose, unless the Manager has expressly consented in writing to such other method of trash disposal.

J. Eating and Drinking

No person shall eat any food or drink any beverage in any area in which such activity is prohibited by the Manager.

VIII. Continuous Expressive Activity Directed At The Public

A. For the purpose of these regulations, "expressive activity" refers to the following: Continuous display of a sign to passerby, continuous distribution of literature to passerby, continuous speech addressed to passerby.

B. Expressive activity is prohibited in PATH except that such activity is permitted in the area set forth in Section E(2), subject to the regulations set forth hereinabove and hereinafter.

C. No person, while engaged in expressive activity, shall:

1. Carry on any commercial activity;
2. Distribute food, flowers, or any other product;
3. Place any chair, table, or other structure on the floor, except as specifically provided herein;
4. Misrepresent through words, signs, leaflets, attire or otherwise such person's affiliation with or support by any organization, group, entity or cause, including any affiliation with or support by PATH, The Port Authority of New York and New Jersey or a subsidiary thereof;
5. Carry a sign or placard attached to a rod or stick in any interior space, or plaza areas.
6. Engage in the solicitation of funds for immediate receipt in any interior space.
7. Enter or remain in any space at, adjacent to, or within ten feet of, any of the following: turnstile; vending machine; doorway, entrance or exit; elevator or escalator; stairway or landing; telephone; dining area; sale

or service counter kiosk or booth; building lobby or hallway; bench or seating area; line of persons for service, such as a line at a kiosk or automatic teller machine; curbside check-in area or vehicle loading or discharge area; restroom; designated waiting area; or bus gate. The ten-foot restriction does not apply any space within an area specifically designated as a place where expressive activity may occur.

8. The General Manager of PATH, or in his or her absence, the person designated to act in his or her stead for general management purposes, may prohibit expressive activity on PATH property which would otherwise be permitted in the event of, and during the pendency of, an emergency condition such as a snowstorm, fire, accident, power failure, transportation carrier schedule interruption, or other condition of such nature and character that the conduct of permitted activities would cause a danger to persons or property during the pendency of such emergency condition.
9. (a) Persons shall conduct expressive activities in the designated areas of the PATH system only pursuant to a permit obtained pursuant to Section D, for the use of one or more of the areas designated on the attached schedule and diagrams of the PATH system, when those areas are not occupied by construction or maintenance activity affecting a permanent structure, subject to the number restrictions set forth on such schedule.
 - (b) Tables measuring no more than 60 inches by 30 inches are permitted in the designated areas.
 - (c) Expressive activity on the Concourse of the World Trade Center station is subject to the following restrictions:
 - i. Expressive activity is permitted only in the area designated as C on the attached diagram.
 - ii. A permit will be issued for use of one of the subdivisions of C, designated locations C-1 to C-8 on a first come, first serve basis.
 - iii. Coordinated expressive activity by 25 or more persons is subject to the following restrictions.
 - a. Coordinated expressive activity by 25 or more persons is permitted in areas locations C-1, C-2, C-7 and C-8 only.
 - b. An applicant may request permits for use of locations C-1 and C-2 in combination or use of locations C-7 and C-8 in combination.

- c. A permit may not be granted for use of locations C-1, C-2, C-7 or C-8, or any combination thereof, for coordinated expressive activity by 25 or more persons if a permit has been issued for use of any adjacent location for expressive activity.
- d. A permit may not be issued for use of any location adjacent to C-1, C-2, C-7 or C-8 for expressive activity if a permit has been issued for use of C-1, C-2, C-7 or C-8, or any combination thereof, by 25 or more persons.
- e. No more than 90 persons may use each of C-2, C-7 or C-8 at one time for expressive activity, and no more than 45 persons may use C-1 at one time for expressive activity. A combination of any of these spaces may not be used by more than the total of the maximum number of persons who may use each of the combined spaces.

D. Permit application shall be made, and acted upon, as set forth below:

- 1. A permit application shall be submitted in writing no later than thirty-six (36) hours preceding the commencement of the activities for which the permit is sought, and no earlier than seven (7) days preceding the commencement of the activities for which the permit is sought.
- 2. Permit application shall be submitted in person to the Permit Administrator of PATH, or the designee thereof, during the hours of 9:00 AM to 10:30 A.M. and 1:30 PM to 3:30 P.M., Monday through Friday, excluding holidays.
- 3. (a) The permit application shall set forth the type, time, location and duration of activities to be conducted, the name, address and telephone number of the person making the request (in the case of a group, it shall be sufficient to supply the name, address, and telephone number of the person who can be contacted if problems arise concerning the granting of the request).

(b) If a person making the application indicates an affiliation with an organization or group, the name and address of a local representative of the organization or group to act as a liaison will be requested; however, refusal to provide such information shall not be grounds for denial of a permit.

4. Each permit shall be valid for a period of time specified by the applicant, not exceeding fourteen (14) days pursuant to a single application.
5. (a) Renewal applications shall be made in the same form used for new applications, and shall be processed as if they were new applications.

(b) All locations will be assigned on a first-come, first-serve basis, without regard to renewal status.

(c) The use of space previously used pursuant to a permit is not guaranteed by acceptance of a renewal application.
6. (a) A permit for any location will be granted on a first-come, first-serve basis.

(b) An application will be denied only if the area requested is unavailable, the application is incomplete, or the application discloses that the activities to be performed thereunder will violate these Rules.
7. (a) A permit will be issued, or the application denied, by the PATH Permit Administrator, or a designee thereof, no later than 5:00 PM of the day following submission of the application, excluding Saturdays, Sundays and holidays observed by PATH.

(b) The reason for the denial of an application shall be set forth in writing.
8. (a) Upon the denial of any application for a permit, or the failure to issue a permit by 5:00 PM of the day following submission of the appeal, excluding Saturdays, Sundays and holidays recognized by PATH, an applicant may submit a written appeal to the PATH General Manager, or a designee thereof, setting forth the reasons why the application should be granted.

(b) An appeal shall be submitted in person to the PATH Permit Administrator, or a designee thereof, during the hours of 8:00 A.M. to 5:00 P.M., Monday through Friday, excluding holidays. The PATH Permit Administrator, or the designee thereof, shall cause the appeal to be delivered to the PATH General Manager, or a designee thereof.
9. (a) A written decision denying the appeal, or issuing a permit shall be made no later than 5:00 PM of the day following submission of the appeal, excluding Saturdays, Sundays and holidays observed by PATH.

(b) If no decision is issued by 5:00 PM of the day following submission of the appeal, excluding Saturdays, Sundays and holidays observed by PATH, the appeal shall be deemed to be denied on the basis of the original decision denying the application.

10. Any person whose application for a permit has been denied may seek review of the final decision denying such application in a proceeding commenced pursuant to Article 78 of the Civil Practice Laws and Rules of the State of New York, or action in lieu of prerogative writ in the courts of the State of New Jersey.
11. Persons who engage in expressive activity pursuant to the permit described herein must possess a copy of such permit when and shall display such document upon the request of PATH personnel or Port Authority Police Officers.
12. Each time a person or group ceases use of a designated area for expressive activity, such action shall be reported to the Permit Administrator of the PATH system or a designee thereof.
13. For the purposes of this regulation, "holidays" refers to the following:

New Year's Day	January 1*
Martin Luther King, Jr. Day	Third Monday in January
Presidents' Day	Third Monday in February
Memorial Day	Last Monday in May
Independence Day	July 4*
Labor Day	First Monday in September
Columbus Day	Second Monday in October
Veterans Day	November 11*
Thanksgiving Day	Fourth Thursday in November
Day after Thanksgiving	Fourth Friday in November
Christmas Day	December 25*

*If any of the days marked with an * shall fall on a Saturday, the

preceding Friday will be observed as a holiday; if any of the days marked by an * shall fall on a Sunday, the succeeding Monday will be observed as a holiday.

- E. 1. There shall be no expressive activity at the following PATH locations: Christopher Street; 9th Street; 14th Street; 23rd Street; Harrison; and Newark.
- 2. Expressive activity shall be permitted at the following stations, in the specific areas designated on the attached drawings: World Trade Center; 33rd Street; Grove Street; Exchange Place; Hoboken; Pavonia-Newport; and the Journal Square Transportation Center.

IX. Photography and similar activity.

- A. The taking or making of photographs of any portion of the PATH system is prohibited except as provided herein.
- B. The taking or making of films, video recordings, and drawings or other visual depictions are subject to the same prohibitions, restrictions and procedures as are applicable to photography.
- C. Photography which involves any of the following must comply with the requirements of the Extended Photography Policy and Procedures, in addition to these Rules:
 - 1. Exclusive use of any area or any railcar or part of a railcar.
 - 2. Exclusion of members of the public, PATH or Port Authority personnel, or PATH or Port Authority contractors from any area or any railcar or part of a railcar.
 - 3. Use of equipment other than handheld equipment with self-contained power sources.
- D. 1. No person may take a photograph of any portion of the PATH system unless he or she is accompanied by a representative of PATH.
- 2. No photograph shall be taken of any specific location, device or structure if such representative advises that such photography is prohibited because it will create an image which could be used to aid in the planning of an attempt to disable, destroy, avoid or circumvent any operational, safety, security, evacuation or emergency response device, structure or procedure, or which could be used in the planning of an attempt to commit an act of violence or intentionally cause disruption of rail service or public panic within the PATH system or a part thereof. If possible, a suggestion for alternative photography

in PATH which would not have such an effect shall be made by the PATH representative.

3. A photographer and all members of his or her party shall follow the directions of such representative made for the purpose of preventing unreasonable interference with PATH operations, maintenance and construction, and to preserve the health and safety of the photographer or others.
 4. A photographer may protest any direction made pursuant to paragraph (2) or (3) in the same manner as an appeal from the denial of a permit as set forth herein.
- E. No person may take any photograph within PATH unless he or she has been issued a permit therefore by PATH as set forth herein.
1. A permit application shall be submitted in writing no later than thirty-six (36) hours preceding the commencement of the activities for which the permit is sought, and no earlier than seven (7) days preceding the commencement of the activities for which the permit is sought.
 2. Permit application shall be submitted in person to the PATH Permit Administrator, or the designee thereof, during the hours of 9:00 AM to 10:30 AM and 1:30 PM to 3:30 PM, Monday through Friday, excluding holidays.
 3. The permit application shall set forth the type, time, location and duration of activities to be conducted, and the name, address and telephone number of the person making the request (in the case of a group, it shall be sufficient to supply the name, address, and telephone number of the person who can be contacted if problems arise concerning the granting of the request). If a person making the application indicates an affiliation with an organization or group, the name and address of a local representative of the organization or group to act as a liaison will be requested; however, refusal to provide such information shall not be grounds for denial of a permit.
 4. Permits will be granted on a first-come, first serve basis depending on the availability of escorts. An application will be denied in whole or in part only if: (a) the presence of visitors in a requested location would unreasonably interfere with PATH operations, maintenance and construction; (b) if the conduct cannot be performed without creating an image which could be used to aid in the planning of an attempt to disable, destroy, avoid or circumvent any operational, safety, security, evacuation or emergency response device, structure or procedure, or which could be used in the planning of an attempt to commit an act of violence or intentionally cause disruption of rail service or public panic within the PATH system or a part thereof; (c) if the location requested may not be visited safely by persons other than PATH or other operation, construction or maintenance personnel; (d) the application is

incomplete; or, (e) the application discloses that the activities to be performed thereunder will violate these Rules.

5. A permit will be issued, or the application denied, by the PATH Permit Administrator or a designee thereof, no later than 5:00 PM of the day following submission of the application, excluding Saturdays, Sundays and holidays recognized by PATH. The reason for the denial of an application or any part thereof shall be set forth in writing.
6. (a) Upon the denial of any application for a permit, or the failure to issue a permit by 5:00 PM of the day following submission of the application, excluding Saturdays, Sundays and holidays recognized by PATH, the applicant may submit a written appeal to the PATH General Manager, or a designee thereof, setting forth the reasons why the application should be granted.

(b) An appeal shall be submitted in person to the PATH Permit Administrator, or a designee thereof, during the hours of 9:00 AM to 5:00 PM, Monday through Friday, excluding holidays. The PATH Permit Administrator, or the designee thereof, shall cause the appeal to be delivered to the General Manager, or a designee thereof.
7. A written decision denying the appeal, or issuing a permit, shall be made no later than 5:00 PM of the day following submission of the appeal, excluding Saturdays, Sundays and holidays recognized by PATH. If no decision is issued by 5:00 PM of the day following submission of the appeal, excluding Saturdays, Sundays and holidays recognized by PATH, the appeal shall be deemed to be denied on the basis of the original decision denying the application.
8. A decision made in response to an application for a permit or an appeal of a denial of a permit shall not disclose information which could be used to aid in the planning of an attempt to disable, destroy, avoid or circumvent any operational, safety, security, evacuation or emergency response device, structure or procedure, or which could be used in the planning of an attempt to commit an act of violence or intentionally cause disruption of rail service or a public panic within the PATH system or a part thereof.
9. Any person whose application for a permit has been denied may seek review of the final decision denying such application in a proceeding commenced pursuant to Article 78 of the Civil Practice Laws and Rules of the State of New York, or action in lieu of prerogative writ in the courts of the State of New Jersey.
10. The General Manager of PATH, or in his or her absence, the person designated to act in his or her stead for general management purposes, may

withdraw or suspend a permit for photography in the event of, and during the pendency of, an emergency condition such as a snowstorm, fire, accident, power failure, transportation carrier schedule interruption, or other condition of such nature and character that the conduct of permitted activities would cause a danger to persons or property during the pendency of such emergency condition.

11. For the purpose of this regulation, "holidays" refers to the days set forth in VII (D) (13) above.

ATTACHMENT F
TENANT ALTERATION CONSTRUCTION APPLICATION

NOTE: This is an instruction sheet only. Please remove before completing alteration application.

PREPARATION OF TENANT CONSTRUCTION OR ALTERATION APPLICATIONS

Tenant Construction or Alteration Applications are prepared as follows:

1. Prepare 4 copies of form PA 531 for minor alterations such as electric outlets, partitions, cabinets, etc. Attach 1 copy of plans and specifications to each copy of form.
2. Prepare 7 copies of form PA 531 for all other tenant construction. Include 10 copies of plans and specifications for an application whose estimated cost is \$50,000 or more.

TENANT CONSTRUCTION PLAN AND SPECIFICATION GUIDELINES

The following comments are to assist your engineer or architect in preparing drawings of proposed work. Use of the guidelines, where pertinent, will minimize Port Authority review time and resultant comments.

1. Locate area of construction with respect to existing conditions, (i.e., column numbers, coordinates, dimensions to existing structures, etc.), and provide a "Plot Plan."
2. Indicate existing structures and facilities in area affected and adjacent areas; also indicate all demolition and removals.
3. Include on drawings the plans, sections, elevations and details of proposed work.
4. Show arrangement of equipment and furniture, which might constitute an obstruction of passage to exits.
5. Provide floor plans to include that area beyond the limits of proposed work area necessary to show the entire means of ingress and egress.
6. Indicate where prescribed occupancy count for all area.
7. Give location and specifications for all fire protection equipment, i.e. fire doors, fire dampers, smoke detectors, sprinklers, fire alarm systems, hose cabinets, extinguishers, etc.
8. Include a note on the drawings requiring all work to be done in accordance with the National Electrical Code and the applicable code of the City, or municipality in which work occurs. F.I.R.O. and Employers Group of Insurance Companies approval required for sprinkler and fire protection items.
9. Indicate power requirements and source of power. Also indicate size and type of all electrical equipment, i.e. conduit, wire, panels, control devices, etc.
10. Provide details of all built-in equipment.
11. Provide complete specifications for all materials.
12. Show all new and modified ventilating systems including that portion outside the area of proposed work necessary to indicate the complete circulation cycle.
13. Provide design computations for major structural members including all existing members receiving additional loads.
14. All drawings must bear the stamp of a Registered Architect or Professional Engineer licensed in the state in which the work is to be performed.
15. If proposals require resubmission, clearly indicate change from original on the resubmitted drawings.
16. "As Built" Drawings are to be furnished after completion of this work.
17. Asbestos Certification Letter, Form PA 3677, is to be submitted with Form PA 531.
18. If Form PA 3677, Asbestos Certification Letter, indicates that asbestos will be disturbed, Form PA 3678 is to be submitted with Form PA 531.
19. If Form PA 3677, Asbestos Certification Letter, indicates that asbestos will be disturbed and the tenant is waiving his/her right to participate in the Port Authority's litigation, Form PA 3679 is to be submitted with Form PA 531.
20. All materials used for the construction of this project, whether building materials or appurtenances, shall be non-asbestos containing materials.
21. A contractor approved by the Port Authority must perform asbestos work.
22. All environmental services required to be performed with respect to tenant construction, including and without limitation, surveys, monitoring, laboratory analysis and waste removal, must be performed by a contractor/consultant, approved in advance by the Port Authority.

FINAL RECONSTRUCTION PERMIT APPLICATION PA-0531/09-10

For Port Authority Use Only	
Facility	APP. No.
Date	Applicant's Name

225 Park Avenue South New York, New York 10003

APPLICANT MUST READ THE TERMS AND CONDITIONS INCLUDED WITH THIS FORM

The Applicant shall not commence performance of any of the said work prior to the receipt by Applicant of a copy of this application duly signed in Part Two hereof on behalf of the Port Authority of New York and New Jersey. Upon receipt thereof, the Applicant agrees to perform said work in accordance with the following "Information to be Furnished by Applicant" and to comply with and be bound by all requirements and conditions set forth below under the remarks, if any, in Part Two hereof and the terms and conditions set forth in this form.

Minimum Insurance Limits Unless Specified to be Greater -- Bodily Injury \$500,000 each person; \$500,000 each occurrence; Property Damage \$500,000 each accident; \$500,000 aggregate.

PART ONE: Information to be furnished by Applicant (Refer to your lease or permit for required information)

Permission is hereby requested to perform the following described work on the space occupied by the Applicant.

At (Facility)	Pursuant to (Lease, Space, Permit) No.	Location (Building No. or Area) of Space to be Altered
Description of Work and Reason		

Estimated Cost of Work \$	Estimated Time to Complete (Days)	Starting Date	Completion Date
---------------------------	-----------------------------------	---------------	-----------------

Plans: Prints of each drawing must be submitted with copies of application. Include floor plan and show area affected by proposed Work (size 8 1/2" x 11" or larger).

TITLE OF DRAWING	DRAWING NO.	DATED
------------------	-------------	-------

Name & Address of Contractor (If Not Known, Submit Later)	Name & Address of Engineer or Architect	Telephone No.
Email (Optional)	Email (Optional)	License No.

Send Correspondence To:
(Name & Address of Employee in Charge of Work)

Email (Optional)
Telephone No.

Applicant's Name (As it Appears on Lease or Permit)

ENGINEER OR ARCHITECT CERTIFICATION
I have supervised the preparation of plans and specification of the entire work represented herein and hereby certify that they conform to the requirements of the respective enactments, ordinances, resolutions and regulations of the City, town or municipality in regard to construction and maintenance of buildings and structures and in regard to health and fire protection which should be applicable if the Port Authority were a private corporation.

By (Signature of Authorized Rep.)	Title	Date	Signature of Licensed Prof. Engineer or Architect	Date
-----------------------------------	-------	------	---	------

PART TWO: Prepared by Port Authority and returned to applicant.

The above Application is Approved Disapproved. Subject to the following conditions:

Continued on Rider "A" attached

Please advise the undersigned in writing, when this work has been completed.

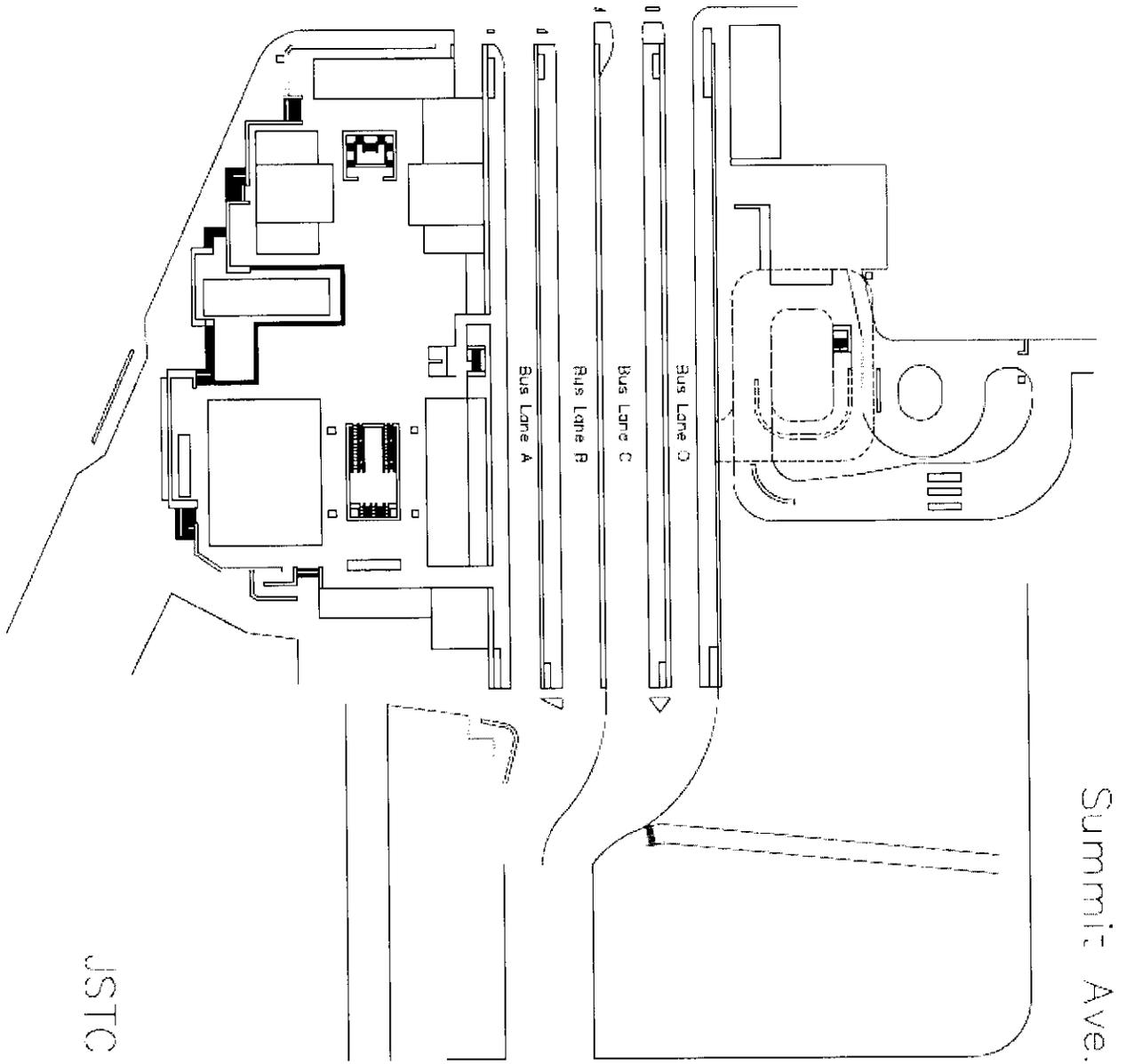
The Port Authority of New York and New Jersey		By:
Inspected By	Date	Title
		Date

TERMS AND CONDITIONS

1. In the performance of work covered hereunder the Applicant shall, unless otherwise directed in writing by the Port Authority, conform to the requirements of the respective enactments, ordinances, resolutions and regulations of the city, town or municipality in which the Facility is located in regard to the construction and maintenance of buildings and structures and in regard to health and fire protection which would be applicable if the Port Authority were a private corporation. The Applicant's obligations to comply with the above governmental requirements is for the purpose of assuring proper safeguards for the protection of persons and property at the Facility and is not to be construed as a submission by the Port Authority to the applications to itself of such requirements or any of them.
2. The Applicant shall comply also with such federal, state and municipal laws, statutes, orders and regulations, if any, as may be legally applicable to the work or the performance thereof or its employees therein. The Applicant shall consult with the Facility Manager with respect to the applicability of any and all laws, statutes, enactments, ordinances, resolutions and regulations and as to the procedures to be followed before taking any other action with respect thereto, and shall follow the instructions and procedure prescribed by said Facility Manager with respect thereto.
3. The Applicant shall also observe and obey (and compel its officers, employees, agents and contractors to observe and obey) the rules and regulations of the Port Authority now in effect which are applicable to the performance of the work and such further applicable rules and regulations which may from time to time during the said performance be promulgated by the Port Authority for reasons of safety, health, preservation of property or maintenance of a good and orderly appearance of the Facility, or for the safe and efficient operation of the Facility.
4. The Applicant shall procure and maintain bodily injury and property damage liability insurance in its own name in at least the limits specified in the preamble to this Application and Workmen's Compensation insurance; or if the work is to be done by an independent contractor, the Applicant shall require such contractor to procure and maintain such insurance in the contractor's name. A certificate evidencing such insurance shall be furnished to the Port Authority Facility prior to the commencement of the work.
5. The Applicant shall indemnify and hold harmless the Port Authority, its Commissioners, officers, agents and employees, against and from (a) the risk of injuries (including wrongful death) or damage direct or consequential, to it or them or to its or their property, arising out of or in connection with the performance of the work, and (b) the risk of claims and demands by third persons arising or alleged to arise out of the performance of the work, whether such risks arise out of acts of omissions or the Applicant its contractors, the Port Authority, or otherwise.
6. The Applicant shall pay all claims lawfully made against it by contractors, subcontractors, materialmen and workmen, and all claims lawfully made against it by other third persons arising out of or in connection with or because of the performance of the work, and shall cause all contractors and subcontractors to pay all such claims lawfully made against them.
7. Only first-class materials and workmanship shall be used in the performance of the work, which shall be done in accordance with the drawings described in Part 1 of this Application and to the satisfaction and subject to the inspection of the Facility Manager; the Applicant shall re-do or replace at its own expense any work not approved by him.
8. The Applicant shall notify the Facility Manager no less than two days prior to the commencement of the work, and shall complete the same within the number of days specified in Part 1 of this Application; and upon completion shall notify the Facility Manager.
9. In the performance of the work, (a) the Applicant shall not do or permit to be done any act affecting the operation of the existing plumbing, heating, fire-protection, fire-alarm, sewerage, drainage, water supply, electrical, sprinkler, ventilating, refrigerating, fuel or communication system at the Facility, or other such service system thereat, including all pipes, tubes, lines, mains, wires, conduits, equipment and fixtures, except with the express written approval of the Facility Manager or the Port Authority resident engineer; (b) the Applicant shall obtain a Port Authority permit from the Facility Manager prior to any cutting or welding and shall comply with the conditions which form a part of said permit, a sample of which may be examined in the office of the Facility Manager.
10. (a) Prior to the commencement of the work and throughout the performance thereof, the Applicant shall erect and maintain at its own expense in or about the space such barriers, shields and other suitable protective devices for the protection of the public and others and their property as in the opinion of the Facility Manager may be necessary or desirable for the purpose. The work shall be performed in such manner as will cause the minimum inconvenience to members of the public and others at the Facility. During the performance of the work, the Applicant shall not permit the accumulation in or about the space of any debris, rubbish or litter of any sort resulting from such performance and shall make such arrangements for the frequent removal thereof from the Facility, by means of facilities to be furnished by the Applicant, as may in the opinion of the Facility Manager be necessary to prevent such accumulations.
(b) In the performance of the work covered by this permit, the Applicant shall not employ any contractor nor shall the Applicant or any of its contractors employ any persons or use or have any equipment or materials or allow any condition to exist if any such shall, or in the opinion of the Port Authority, may cause or be conducive to any labor troubles at the Facility which interfere, or in the opinion of the Port Authority, are likely to interfere with the operations of the Facility by the Port Authority or with the operations of others at the Facility or with the progress of other construction work thereat. The determinations of the Port Authority shall be conclusive on the Applicant and, upon notice from the Port Authority, the Applicant shall immediately remove such contractor or withdraw or cause its contractors to withdraw from the Facility the persons, equipment or materials specified in the notice and replace them with unobjectionable contractors, persons, equipment and materials and the Applicant shall or shall cause its contractor to immediately rectify any conditions specified in the notice in the event of failure by the Applicant or any of its contractors to immediately comply with the requirements of this paragraph (whether or not such failure is due to the Applicant's fault) the Port Authority shall have the right to suspend this permit and the permission thereby granted, without prior notice when the labor troubles shall be so settled that such interference or the danger thereof no longer exists, the Port Authority, by notice to the Permittee, shall reinstate this permit on all the same terms and conditions as before the suspension. "Labor troubles" shall mean and include strikes, boycotts, picketing, work-stoppages, slowdowns, complaints, disputes, controversies or any other type of labor trouble, regardless of the employer of the person involved or their employment status if any.
(c) Notwithstanding the approval of this permit by the Port Authority, the Applicant shall not perform or permit to be performed any work hereunder, the performance of which or the subsequent use or occupancy of which will (1) invalidate or conflict or conflict with any insurance covering the Facility or any part thereof, or in any property located therein or thereon, or (2) increase the rate of any fire insurance, extended coverage, rental insurance or other insurance on the Facility, or any part thereof or upon any property located therein or thereon. The Applicant shall promptly observe, comply with and execute the provisions of any and all present and future rules, regulations, requirements, orders, directions and standards of the National Board of Fire Underwriters as interpreted by the New York Fire Insurance Rating Organization as to work performed in New York State, or as interpreted by the Fire Insurance Rating Organization of New Jersey as to work performed in New Jersey, or of any other board or organization exercising or which may exercise similar functions, which may pertain or apply to the performance of the work or to the completed work (including use or operation (hereof) and the Applicant shall make any and all structural and non-structural improvements, alterations or repairs of the work that may be required at any time hereafter by any such present or future rule, regulation, requirement, or order or direction. If because of the work done or by reason of any failure on the part of the Applicant to comply with the provisions of this paragraph any such insurance shall at any time be limited, cancelled or invalidated, then the Applicant shall immediately remove the work, or if the rate of premium for any such insurance shall be higher than it otherwise would be, then the Applicant shall pay to the Port Authority on demand that part of all premiums which shall have been charged because of such work or by reason of such failure by the Applicant. The Applicant shall furnish to the Port Authority evidence of approval of the work by the insurance authority having jurisdiction.
11. Title to any installation, improvement, alteration, modification, addition, repair or replacement resulting from work done pursuant hereto shall immediately upon completion vest in the Port Authority (or in the Port Authority's lessor, if any and if the agreement between such lessor and the Port Authority so provides) without execution of any further instrument. The Applicant shall not remove or change the same unless the Port Authority, on or prior to the expiration or termination of the lease or permit described in Part 1 of this Application or within sixty (60) days after such expiration or termination, shall give notice to the Applicant requiring removal or restoration, in which case the Applicant (on or prior to the expiration or termination date or, if the notice is given after such date, then immediately after receipt of the notice) shall complete the removal of all of the same (or as much thereof as may be required by the notice) and the restoration (to the extent required by the notice) of the space affected by the work to the same condition as it was in prior to the commencement of the said work. If the Applicant shall fail to comply with such notice, the Port Authority may effect the removal and restoration and the Applicant shall pay the cost thereof to the Port Authority upon demand.
12. A certificate of completion shall be issued by the Facility Manager upon request of the Applicant on completion of the work hereunder in accordance with the Terms and Conditions hereof and inspection thereof by the Facility Manager. Issuance of such certificate shall not preclude the Port Authority from showing that Applicant has failed to comply with his obligations hereunder nor shall it release Applicant from such obligations.

ATTACHMENT G: SITE PLAN AND AERIAL PHOTO

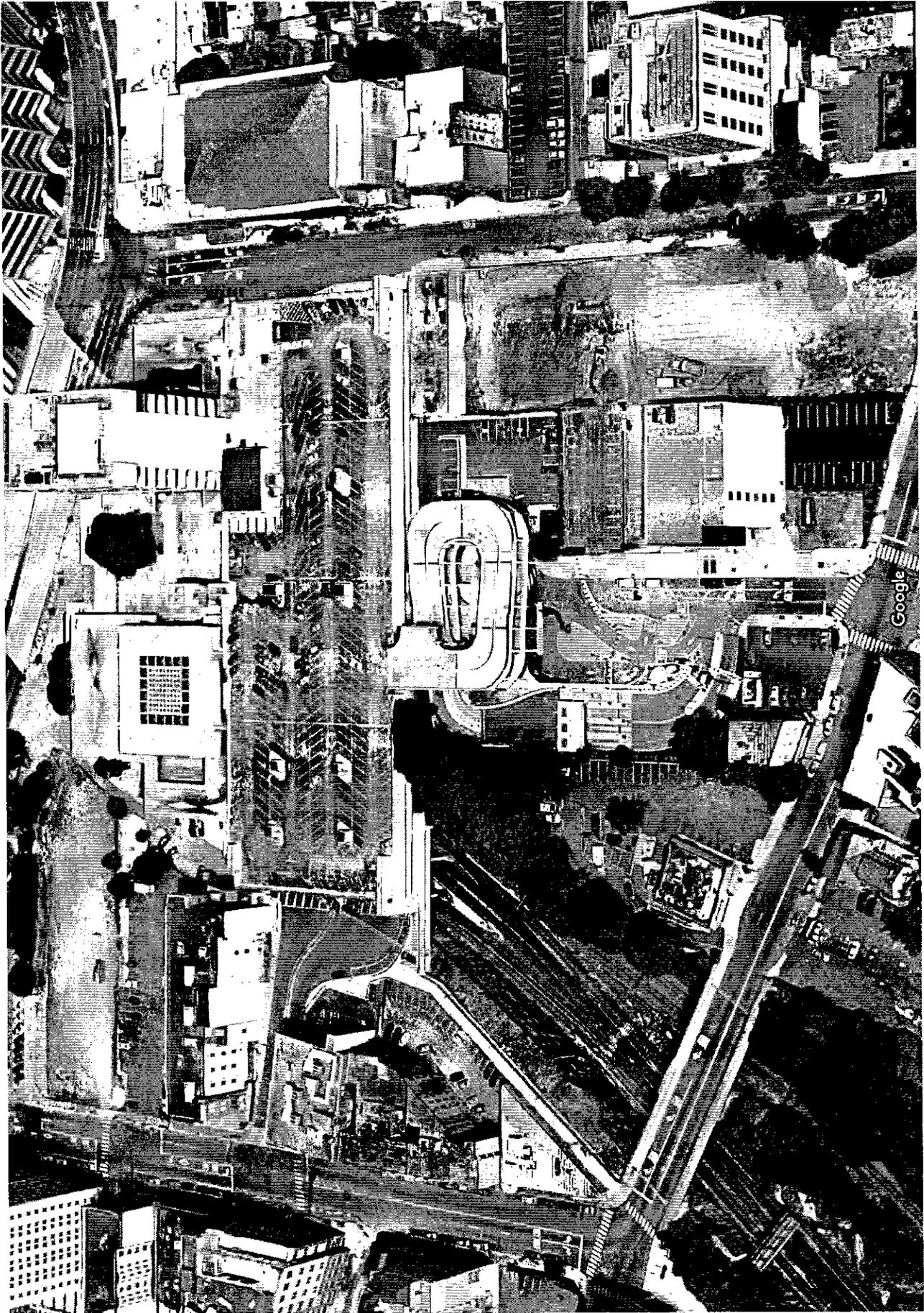
Pavonia Ave.



JSTC SITE PLAN

Sip Ave.

Summit Ave.



ATTACHMENT H

TABLE OF CONTENTS

PART I Technology Standards

PART II Cyber Security Guidelines

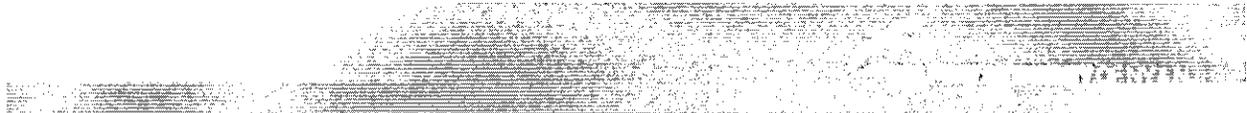
PART III Computing Resources Policy

PART IV Cloud Computing Framework

PART V Audit Department Controls Requirement Contract Checklist

ATTACHMENT H

PART I Technology Standards



Technology Department

TECHNOLOGY STANDARDS FOR THE PORT AUTHORITY

*(Non-Confidential Sections for Use
in Preparation/Distribution with RFPs)*

Revised December 2015

Table of Contents

Introduction.....	6
1.0 The Port Authority Wide Area Network (PAWANET).....	6
1.1 PAWANET Overview.....	6
1.2 PAWANET Circuit Diagram.....	6
1.3 Inter-site Services Providers.....	8
1.4 PAWANET Functions.....	8
1.5 Features of PAWANET.....	8
1.6 Supported Protocols.....	8
1.7 PAWANET Switches and Routers.....	8
1.8 Approved Servers.....	9
1.9 Enterprise Addressing Scheme (including IP addressing).....	9
1.10 Enterprise Network Monitoring Software.....	9
2.0 Network Resources.....	9
2.1 Network Overview.....	9
2.2 Enterprise Network Architecture.....	10
2.2.1 Server Operating System and Software.....	10
2.2.2 Configuration.....	10
2.2.3 Network Resources Security.....	12
2.2.4 Network Access and User Account Security.....	13
2.2.5 Remote Access System.....	14
2.2.6 Hardware Standards.....	15
2.3 Network Naming Conventions.....	16
2.3.1 Server Names.....	16
2.4 Directory Services and Structure.....	16
2.5 System Backup and Recovery.....	16
2.5.1 Backup Logs.....	16
2.5.2 Backup Scheduling.....	17
2.6 Business Resumption Plan.....	17
2.7 Telecommunications Standards for Enterprise Network Resources.....	17
2.7.1 Closet and Telecommunications Room Access.....	17
2.7.2 Telecommunications Installation Contractor's Responsibilities.....	17
2.7.3 Electrical Requirements.....	18
2.7.4 Telephone Company Interface.....	18
2.8 Documentation.....	18

3.0	Virus Scanning & Management.....	19
3.1	Overview.....	19
3.2	Standards.....	19
3.3	Acquisition and Installation.....	19
3.4	Virus Detection and Response.....	19
4.0	Electronic Mail.....	20
4.1	E-Mail Overview.....	20
4.2	E-Mail System Architecture.....	20
4.3	E-Mail Environment: Design Considerations and Infrastructure.....	20
4.4	Integrating Applications Server with Port Authority Email System.....	21
4.4.1	Requesting SMTP Services.....	21
4.4.2	Email Restrictions.....	21
5.0	Intranet.....	21
5.1	Intranet Overview.....	21
5.2	Direction of eNet Development.....	22
5.3	eNet Software Infrastructure Standards.....	22
5.3.1	Design Standards.....	23
5.3.2	Accessibility Standards.....	23
6.0	Workstation Hardware and Operating System Software.....	23
6.1	Overview.....	23
6.2	Workstation Operating System Standard.....	23
6.3	Workstation Configuration.....	24
6.3.1	Workstation Naming Conventions.....	24
6.3.2	Automated Software Distribution for Computers.....	24
6.3.3	Remote Workstation Management.....	24
6.3.4	Drive Mappings.....	24
6.3.5	Standard Workstation Hardware Configurations.....	24
6.3.6	Standard Workstation Software.....	25
6.3.7	Enterprise Software.....	25
6.3.8	Other Business Applications.....	25
6.4	Workstation Security.....	26
6.4.1	Physical Security.....	26
6.4.2	Logical Security.....	26
7.0	Distributed Systems Environment.....	27
7.1	Overview.....	27
7.2	Microsoft Windows Servers.....	27

7.2.1	Virtual Environment	27
7.2.2	Windows Data Encryption.....	27
7.3	Unix.....	27
7.3.1	Unix Security.....	27
7.3.2	Backup.....	27
7.3.3	Download Scripts in the Unix/Linux Environment	27
7.4	z/OS.....	28
7.4.1	Databases.....	28
7.4.2	Geographic Information System.....	28
7.5	Application Security	28
7.6	Server Physical Security.....	28
7.7	Load Balancing – Failover Architecture.....	28
8.0	Vendor Provided Dedicated Systems.....	28
8.1	Overview.....	28
8.2	Physical Security Technology Standards.....	29
8.2.1	Agency Standard for Digital Video Recording, Access Control and Alarm Monitoring 29	
8.2.2	Situational Awareness Platform Software	30
8.3	Communications Infrastructure Standards	30
8.4	Server Infrastructure Standard	30
9.0	Wireless Technologies	31
9.1	Wireless Standards	31
9.1.1	Purpose and Scope	31
9.1.2	General Policy	31
9.1.3	Personal Area Networks - PAN.....	31
9.1.4	Wireless Local Area Networks – WLANs.....	31
9.2	Cellular Phone & Wireless Modem.....	34
9.3	Technology Mobile Device Policy.....	34
9.3.1	Introduction.....	34
9.3.3	Software.....	35
9.3.4	Support.....	35
9.3.5	Training.....	35
9.3.6	Acquisition	35
9.3.7	Personal Acquisition.....	35
9.3.8	Data Security Considerations.....	35
9.3.9	Data Backup	35

Technology Standards for the Port Authority (Non-Confidential) – December 2015

Appendices	36
Appendix 1 -- Business Resumption Plan Document Format	36
Appendix 2 -- Communication Rooms/Closets Standards	38
Appendix 3 -- Standard Cabling Schemes	39
Appendix 4 -- Unified Wiring Plan	40
Appendix 5 -- Telephone Closet / IDF Termination Blocks	42
Appendix 6 -- Workstation Jacks	43
Appendix 7 -- Standard Switches Inside the Department.....	44
Appendix 8 -- Workstation and Lateral Cable Identification Management.....	45
Appendix 9 -- Fiber Optic Specification for Network Services - PAWANET.....	46
Appendix 10 -- Public Telephone Ordering Standards.....	47

Introduction

The purpose of this document is to communicate the standards established by the Technology Department (TEC) for Information Technology (IT) solutions deployed at Port Authority of New York & New Jersey (PANYNJ), the Agency.

To that end, these standards intend to help RFP Submitters do the following:

- Implement computing and networking solutions that ensure the utmost reliability, availability and security.
- Procure hardware and software that advances business needs in a manner that is compatible in an ever-changing IT environment that enables departments to work with each other more effectively.
- Communicate and exchange information throughout the agency easily and efficiently.
- Achieve greater systems integration so that the application will be interoperable resulting in cost effectiveness and quality control.
- Adherence to these standards ensures that IT investments achieve Enterprise connectivity, interoperability, consistency, and will enhance performance in a cost-effective way.

1.0 The Port Authority Wide Area Network (PAWANET)

1.1 PAWANET Overview

The Port Authority has a modern distributed computing network, called the Port Authority Wide Area Network (PAWANET), which is managed as an enterprise resource. It connects all the various Port Authority facilities and transportation systems using high-speed voice, data, and video lines or links.

This network is crucial to all Port Authority businesses because it provides the connections for applications such as e-Mail, Internet and Intranet access, SAP, PeopleSoft, Electronic Toll Collection, Computer Aided Design and Drafting (CADD), Lease Video Teleconferencing, and more.

PAWANET consist of a Managed Fiber Optic Dense Wave Division Multiplexed (DWDM) Network, provided by Verizon Select Services, as an Integrated Optical Service (IOS) network. This network consists of eleven separate and distinct (1) Gbps lightwave networks, each interconnecting with the data centers at Telecenter and the Port Authority Technical Center (PATC). Site-to-Site interconnectivity is achieved via the "hub and spoke" topology through the data centers. Additional high-speed Ethernet Private Lines (EPL) have been deployed to support key Port Authority off-ring facilities.

Remote locations are linked using redundant high-speed dedicated point-to-point leased communication lines. Wireless connectivity also supported when hardwired connections are not practical.

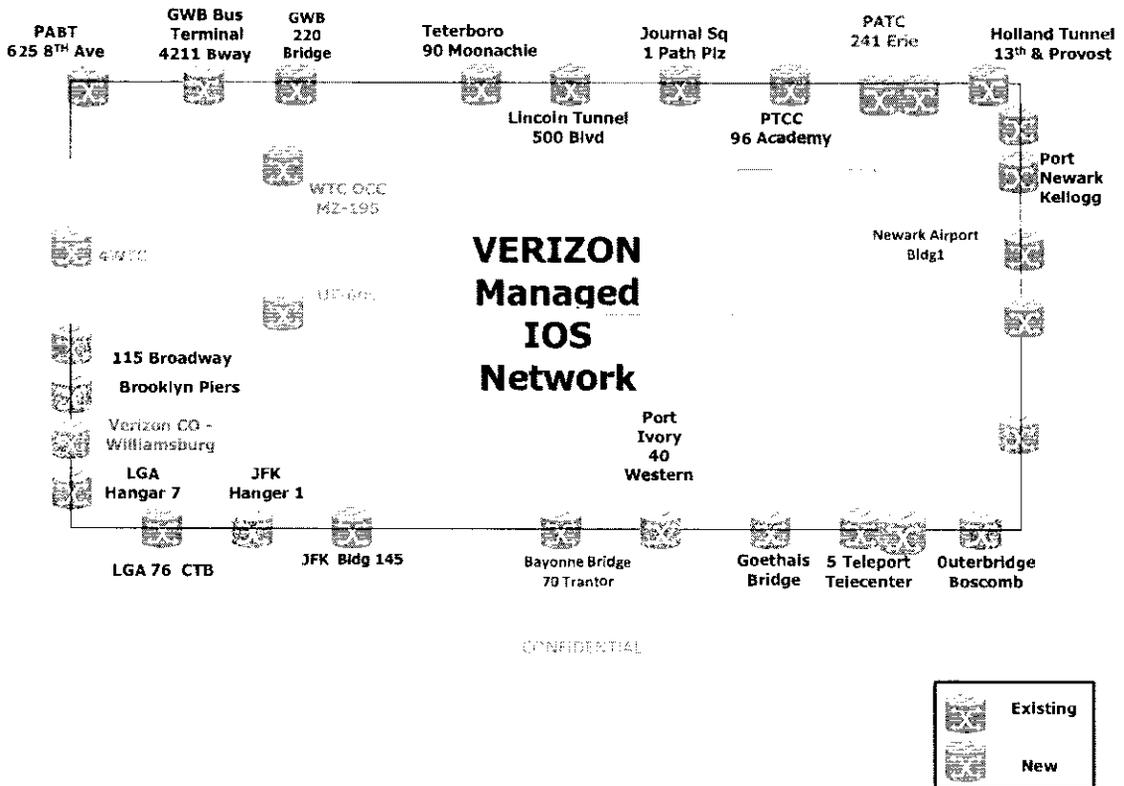
The network consists of state-of-the-art Cisco Systems equipment and services, such as, high performance Cisco Catalyst switches and routers. The Port Authority uses a managed Network Monitoring Services to monitor PAWANET, and Cisco Systems SMARTnet hardware/software maintenance services, and Cisco's Technical Assistance Center (TAC) to support and maintain the network. The Authority has also deployed the Riverbed network performance monitoring products to provide performance data on end user workstations and systems.

1.2 PAWANET Circuit Diagram

The current PAWANET network is being upgraded with Verizon's Protected Riders, which will enable a seamlessly network recovery. [*Protected Riders: The Port Authority Verizon managed IOS DWDM network*

has been upgraded far additional layer of reliability. All existing Port Authority locations now support redundant dual fiber protection to avoid service outages in the event of any fiber cuts.]

The new design will replace the current PAWANET Circuit Diagram.



CONFIDENTIAL

1.3 Inter-site Services Providers

The Technology Department (TEC) has contracted with a variety of companies to provide inter-site services. Companies providing communications services for the Wide Area Network are listed below.

- AT&T Local Services
- Verizon

1.4 PAWANET Functions

Currently PAWANET is used to transport the following:

Data	Supports the low and high volume transfer of data used for applications, such as SAP and PeopleSoft, and for network communications, such as e-mail. Provides a data path for off-site, data backup of file, print and application servers. Enables the use of Storage Area Network (SAN) for network storage of user files and routing jobs to shared network printers.
Video	The transfer of Closed Circuit TV (CCTV) data is supported across the entire network to provide visibility to the Port Authority's key facilities.
Voice/VoIP	The network provides the hardware capabilities for voice and VoIP transmission. Voice over Internet Protocol (VoIP), which currently serves the majority of Port Authority users, is in the process of being implemented for the agency to replace the legacy Nortel system.
Videoconferencing	The network switches and transmission lines are used for videoconferencing to enable diversely located staff participate in meetings across large geographic area.

1.5 Features of PAWANET

PAWANET provides a high performance, resilient, and reliable fail-safe communications network. These are its key features:

- Alternate paths of communication
- Internet access
- Support of high volume traffic
- Cisco Catalyst 3000, 4000 and 6500 switches at all the major sites
- Cisco high performance 2000, 3000, ASR900 and 7200 router family products with redundant power supplies

1.6 Supported Protocols

The network supports the following network protocols, allowing dissimilar platforms to communicate within PAWANET:

TCP/IP: TCP/IP is the universal protocol that allows communications between all systems within the Port Authority's network, as well as other networks.

1.7 PAWANET Switches and Routers

The current standard switches and routers used on PAWANET are:

- Tellabs Reconfigurable Optical Add Drop Multiplexers (ROADMS) are the Dense Wavelength

- Division Multiplexing (DWDM) nodes on the Verizon Managed IOS Network.
- Cisco High performance 3000, 4000, and 6000 series switches.
- Cisco High performance 2000, 3000 series routers for intermediate connectivity.
- Cisco 7200 and ASR900 high performance routers
Provide high-speed connectivity and routing capabilities across the network in support of TCP/IP, and provides routing capabilities for Port Authority Internet access.
- A pair of fault tolerant 10 Gbps links on IOS are installed to provide the required bandwidth between the data centers at Telecenter and PATC.

1.8 Approved Servers

Only IBM servers may be connected to PAWANET.

This includes turnkey, distributed systems, where Application servers are being used. Any replacement 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).

TEC will assign static IP addresses for servers, printers, faxes and/or IP enabled device (e.g. CCTV Cameras etc.) that are to be connected to PAWANET.

1.10 Enterprise Network Monitoring Software

The Port Authority has a managed Network Monitoring Services to continually provide real time monitoring of PAWANET, and its data and voice link availability. To provide for real time network monitoring, the following software utilities are used by the Port Authority, respectively:

- Zenos Network Management software
- Cisco Works for Switched Internetworks
- Riverbed Cascade network performance monitoring software

2.0 Network Resources

2.1 Network Overview

The Port Authority has a modern distributed computing network, which is managed as an Enterprise resource. The network connects all individual PCs, servers, printers, and other devices in a unified computing infrastructure that makes it possible for the Port Authority to conduct its business. The Enterprise Network consists of the PAWANET (see Section 1.1) and connected Local Area Networks (LAN's). The line of demarcation between the cable and wiring is the responsibility of the carrier and the Port Authority's area of responsibility is usually a wiring closet. The Port Authority's Enterprise Network consists of the following components on the Port Authority side of demarcation:

Enterprise Devices

- Cabling
- Routers
- Switches

- Wiring Closets
- Communications Equipment Racks
- Server Racks
- File and Print Servers
- Application Servers
- Storage Area Networks (SAN)
- Network Printers
- Security Devices (Video Encoders, IP Cameras, ACS Panels)

LAN Devices

- Desktop PCs
- Workstations
- Voice Over IP Phones
- Laptops
- Video Conference Units
- Local Printers
- Scanners
- Copiers
- PC Peripherals

2.2 Enterprise Network Architecture

The Port Authority operates an extensive network of Enterprise file, print and application servers. These devices are linked to an Enterprise Wide Area Network. The flexibility provided by the use of multiple servers, server clusters and Storage Area Networks (SAN) offers users improved network response, greater reliability, increased data security and reduced operating cost. Adherence to the standards outlined in this section allows the Port Authority to manage their systems, applications and data in a way that best meets our business needs while maintaining interoperability and safeguarding Port Authority's information assets.

2.2.1 Server Operating System and Software

All Enterprise servers in the Port Authority are currently based on the Windows operating system. Microsoft Windows, RedHat Linux 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
- Systems Backup
- Uninterrupted Power Supply (If central UPS is not installed at the location)
- Current Service Packs and security patches

Note: All standard operating system and server software will be provided and configured, by the Technology Department, prior to connection to PAWANET.

2.2.2 Configuration

All network devices--including servers, workstations, network printers, and network faxes--must use IP addresses which conform to the standards outlined in sections, 1.9 Enterprise Addressing Scheme, and 2.3.1, Server Names.

2.2.2.1 Drive Mapping Conventions and Organization

Mapping of workstation drive pointers to SAN or server disk volumes or folders is accomplished through a Windows Active Directory Login Script. The following drive letters are reserved for Windows Active Directory installations:

Pointer	Volume or Folder
M:	Reserved
P:	Public Applications
Q:	Installation and Upgrade Utilities
S:	Departmental shared directories and files
T:	Reserved
U:	Users Private Home Directory

- Public (Shared) application software installed on a file and print server cluster must reside on a separate volume named "APPS".
Example: P:\APPS
- Each software application installed on the file and print server, or server cluster, must have its own sub-folder.
Examples: P:\APPS\EXCEL
P:\APPS\WORD
- Shared Data stored on a file and print server cluster, shall reside in a volume named Data, and shall be mapped to the "S:\" drive pointer.
Example <Cluster_name>\<DATA>\<Department_NAME>\SHARE on a server cluster
- Each Department's SHARE folder will contain at least three sub-folders titled Org, Everyone and Projects.
- Under the Projects folder will be two additional folders, one called "Active" and one called "Completed". Active projects reside in the "Active" folder.
- When staff identifies a project as being completed, the project folder will be moved to the "Completed" folder and all rights, except for "Browse" will be removed from the folder. This will ensure that the final project documents remain unchanged, while still allowing authorized staff to review the old documents and use them as templates for new documents if desired. The "Completed" folder will be set to archive its data.
- Under the "ORG" folder will be subfolders with names corresponding to the various divisions within the department. By default, only staff within a division will have access to a division's folder. These folders are intended to hold data for a specific division that would not normally be shared departmentally. Staff from other divisions would not have access to these folders unless the division manager of the owning division gives their approval. Having folders setup by divisions will simplify the process of identifying who is responsible for the contents of a folder.
- The "S" and "U" drives should only be used to store business related files.
- The Systems Administrator, at the direction of the 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 Windows file and folder security permissions and access will be granted through the use of groups. These groups will be named using the same name as the folder name.

- In general, rights to any folder will be granted through the use of a group having the same name as the folder. The group would have trustee rights to the folder, and users would be added to or removed from the group as needed. All rights would be granted or revoked through the use of form PA-3624A. Designated staffs in each department are required to approve these requests.
- A user "U" drive will be assigned to each standard Windows Active Directory account for use by each individual user to store business related data on the network. Access to the "U" drive is restricted to the account owner only. Users receive all rights to this folder". Users cannot share data on their "U" drive. Files should be shared only by using the Share, ("S") drive.
- Access to a user's home directory, by anyone other than the owning user is prohibited and will be removed after notifying the end-user.
- Installation files used in the installation of desktop software must reside in a sub-folder under the "APPS" volume

Example P:\APPS\Psoft

2.2.2.2 Connecting LAN Devices to the Enterprise Network

The Technology Department (TEC) is responsible for connecting all LAN devices to the Enterprise Network (PAWANET) provided they meet the Port Authority's standards.

2.2.3 Network Resources Security

2.2.3.1 Server Physical Security

All servers and communication equipment must be located in locked rooms or secured with a cable and lock with the keyboard secured or secured with access control technology to prevent tampering and unauthorized usage.

2.2.3.2 Server Logical Security

To safeguard the Port Authority's Information Technology (IT) systems and data, TEC has implemented a number of processes and procedures, including the requirement that all users accessing the Port Authority's networks authenticate to the Microsoft (MS) Windows Active Directory (Active Directory). The Active Directory Service is a database containing descriptions of all network devices including servers, workstations and user accounts.

In plain English, this means that by executing a login when you first power on your PC you are telling the network who you are. This is accomplished by providing your Windows Username and password. Just as you are issued an ID card for access to certain facilities, buildings or rooms you need to visit to perform your job, your Windows authentication grants you access to network resources, such as shared data volumes, software applications and network printers you use in performing your assigned tasks.

TEC is responsible for providing all enterprise servers with the following protection of their logical resources:

- Guard against unauthorized access.
- Perform daily incremental backups of servers and authorized workstations and full backups weekly.
- Store all monthly backups off site at a secure location and secure daily and weekly backups on-site in a locked area.

- Test recovery procedures annually.
- Use system and application passwords that conform to the Technology Services Department standards.
- Control all remote access using the Port Authority's Remote Access System.
- Maintain current patch levels and critical security updates.

2.2.4 Network Access and User Account Security

2.2.4.1 Account Creation

User accounts are created and managed in MS Windows Active Directory Services for the Windows network resources. Documentation for the creation of user accounts and authority for access is maintained by the Customer Service Desk Manager.

2.2.4.2 Time Restrictions

Due to the fact that The Port Authority serves its clients 24 hours a day, we do not have Login Time Restrictions. All staff may access their account 24 X 7.

2.2.4.3 Concurrent Logins

Login sessions will be limited to one connection per user. User accounts should not have the ability to login to multiple workstations after establishing one active connection to the network.

2.2.4.4 Login Management

These system-monitoring features are driven by group policy and must be active:

- Restrict the count of incorrect login attempts to three before the account is locked out.
- The time for which unsuccessful login attempts are retained to determine a possible intruder attack should be a minimum of 30 minutes before the counter is reset to zero.
- The time for which a user account remains disabled before the account can be used again should be a minimum of 30 minutes.

2.2.4.5 Password Management

All user accounts must have passwords conforming to the following standards:

- a minimum of 10 characters in length
- contain at least two upper and lowercase alphabetic characters,
- contain at least one number (0-9)
- contain at least one special character (e.g.,-+):>_?&\$%#).

Examples of safe passwords:

- an odd character in an otherwise familiar term, such as phnybon instead of funnybone;
- a combination of two unrelated words like cementhat
- An acronym for an easy to remember quote or phrase (see below)
- a deliberately misspelled term, e.g., Wdn-G8 (Wooden Gate) or HersL00kn@U (Here's looking at you).
- Replace a letter with another letter, symbol or combination, i.e. replacing o with zero or a "to" with 2 or i with 1.
- An easily phonetically pronounceable nonsense word, e.g., RooB-Red or good-eits .
- Two words separated by a non-alphabetic, non-numeric, or punctuation character, e.g., PC%Kat or dog,~1#

Choose a password using a phrase:

One way to do this is to pick a phrase you will remember, pick all the first or last letters from each word and then substitute some letters with numbers and symbols. You can then apply capitals to some letters

(perhaps the first and last, or second to last, etc.)

Examples Phrase	First Letters	Password
"Double, double, toil and trouble; Fire burn, and cauldron bubble!"	ddtatfbacb	Ddt@t:fb@cb
"Every time I try to get out, they pull me back in."	etittgotpmbi	3t1ttgoTpmb1
"You Can't Have Everything. Where Would You Put It?"	ychewwypi	Uch3Wwup1?

- Smartphones, where capable, shall leverage biometric access to provide the most security for the least inconvenience.
- User passwords will require a change every 90 days.
- All accounts will be granted the minimum level of access and permissions necessary to perform an assignment.
- If a system account fails to satisfy the requirements of this policy, an administrator may place the account in "disabled" status until remedied.
- Changes to an account's access privileges require the appropriate managers to request new or modified access.
- All users are required to read the Agency Computing Resource Administrative Instruction and sign an acknowledgement of the Agency IT Acceptable Use Code of Conduct policy prior to account activation.
- Annually, all managers are required to certify that only authorized employees have accounts on Agency systems. Technology and the Office of the CSO will work with managers to provide them with the lists of employees and their accounts.

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.

2.2.4.3. Modems and Switches

Staff is prohibited from connecting dial-up modems and switches including wireless switches (e.g. Linksys wireless switches) to workstations that are simultaneously connected to PAWANET or another internal communication network unless approved by the Technology Department (TEC).

Where modems have been approved, users must not leave modems and/or switches connected to personal computers in auto answer mode, such that they are able to receive in-coming dial-up calls.

2.2.5 Remote Access System

The use of local modems to establish direct dial connections to devices on the Port Authority's network is prohibited. Exceptions to this policy require the approval of the Technology Department's Chief Technology Officer.

The approved mechanism for remote access to the Port Authority network is through the Remote Access System (RAS). The Remote Access System utilizes an Internet-based Virtual Private Network (VPN) tunnel established over the Internet linking remote users to the Port Authority Wide Area Network (PAWANET) (remote client to PA site). It is designed to provide authorized Port Authority users with secure access to corporate applications and to files available on their departmental file servers. Once connected to the PAWANET, users with PA-supplied laptops will have access to computing resources as if connected directly to the network. For users using non-PA remote desktops/laptops, once connected to the network, access to applications and resources is delivered through a thin-client environment consisting of a farm of Citrix XenApp/Microsoft Terminal Services servers capable of supporting 200 or more simultaneous users each.

There is no provided access to the user's office PC desktop. Port Authority offices without direct connection to the Port Authority Wide Area Network (PAWANET) can use this system to establish remote access to corporate applications located on PAWANET.

RAS provides multiple security mechanisms to ensure that only authorized users gain access to the Port Authority's computing resources and systems. Through multiple security steps, the user must respond to security challenges. After successful authentication verification, authorized users are provided with access to corporate applications and their departmental network resources.

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

Remote access is authorized on a case-by-case basis by the Chief Technology Officer.

2.2.6 Hardware Standards

The TEC Enterprise Architecture team is responsible for setting the Agency hardware standards. As of August 2015, the hardware standards are as follows:

Desktop, Laptop, CAD*	Lenovo, Microsoft, Panasonic Tough Books
High End Multimedia Workstation*	Apple
Printers	HP, Lanier
Routers and Switches	Cisco
Servers*	IBM
Smart Devices	iPhone/iPad
Storage Area Network (SAN)	IBM (Entry Level and Mid-Range)

*Note: To maintain optimal operating efficiency of the computing environment a standard "Refresh" age has been adopted. The Agency standard refresh age is greater than or equal to 5 years. TEC is responsible for the automatic replacement/upgrade of hardware that has exceeded the Agency standard age limit.

2.2.6.1 Standard Servers

A representative sample of standard servers is as follows (As of August 2015):

Server Description	IBM Model
WEB Server, Small applications server	xSeries 3550M4
Medium applications server	xSeries 3650M4
Database Server, Multiple and Large application server	xSeries 3850X5
VMWare Clusters	NEC Express 5800 series or IBM as stated above

Each server shall have at least two (2) network interface ports to support a production, management and backup network, and redundant power supplies.

The Port Authority manages servers models via a lifecycle process with a minimum 'in service' life of five (5) years.

2.3 Network Naming Conventions

2.3.1 Server Names

The Port Authority employs a naming convention for all servers within PAWANET. That convention will be discussed during a solution implementation phase.

2.4 Directory Services and Structure

The Port Authority uses Windows Active directory to manage network resources and user access. Port Authority departments are designated as organizational units (OU) and servers are network objects contained within the OU.

All network printers should be created using Printer Properties Pro utility.

Applications are distributed using Microsoft System Center Configuration Manager (SCCM).

Applications are distributed based on the type of workstation and user definitions.

Scheduling of distributions is performed in conjunction with client departments.

2.5 System Backup and Recovery

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

- **Upstream Reservoir** is a centralized backup tool used to create data backups for all distributed systems.
- **FDR Upstream** is a Mainframe based tool used to backup all Mainframe data.

Backup data is stored on disk storage for prompt backup and restore. Encrypted tape backup is stored remotely at a secure facility, and is required to assure off-site disaster recovery data storage. All backup media and records must be treated with the same level of security and confidentiality as the original data.

The System Administrator is responsible for verifying that system backups, both local and remote backups, can be used to restore the data. Tests of the ability to successfully restore from both backup systems should be performed annually. It is recommended that:

- Tests of the ability to restore system and application files will be performed on a non-production server.
- When incremental or differential backups are routinely used, the test restore procedure should incorporate both.
- Immediately prior to performing the test restore procedure, do a special full backup on the directories being tested.

2.5.1 Backup Logs

The System Administrator will maintain the following logs for a period of two years:

- Back-up activity
- Rotation of back-ups
- Usage/rotation of back-up media
- Off-site data storage

2.5.2 Backup Scheduling

The System Administrator is responsible for performing back-ups of data, application and system files. This must be as follows:

- Weekly full back up of each server. A full back-up is a back up of all files on the server.
- Daily differential, incremental or full back up of each server or server cluster. The type of back-up performed is dependent on time constraints and the amount of data to be backed up. Incremental back ups are back-ups of all files changed since the last back up. Differential back ups are back-ups of all files changed since the last full back-up.
- A Grandfather, Father, Son (GFS) scheme based on a 33 tape rotation should be used to ensure complete back-up and recovery.

2.6 Business Resumption Plan

The vendors, providing IT services to the PA, shall work with the Technology Department (TEC) to develop a disaster recovery and contingency plan. The System Administrator will participate in the planning, design, implementation, testing, updating and documentation of the plan. [Appendix 1](#) shows a recommended outline for such a plan. The Business Resumption Plan shall be updated and tested at least annually.

2.7 Telecommunications Standards for Enterprise Network Resources

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

- [Appendix 2](#) - Communication Rooms/Closets Standards
- [Appendix 3](#) - Standard Cabling Schemes
- [Appendix 4](#) - Unified Wiring Specifications
- [Appendix 5](#) - Telephone Closet / IDF Termination Blocks
- [Appendix 6](#) - Workstation Jacks
- [Appendix 7](#) - Standard Switches
- [Appendix 8](#) - Workstation and Lateral Cable Identification Management
- [Appendix 9](#) - Fiber Optics Specifications for Network Services - PAWANET

2.7.1 Closet and Telecommunications Room Access

The following standards must be followed regarding access to closets and communication rooms:

- All telecommunications rooms must be physically secured. Remote locations, which are not secured, by a guard or within line of sight of personnel, must be secured by a card access system and/or video cameras.
- The Network Connections (NC) group is responsible for installing routers, switches (along with Cisco Staff when applied) and station drops. They also patch connections and troubleshoot LAN cabling.
- System Administrators requiring routine maintenance of data communications equipment should call the Customer Support Desk when new devices or reconfigurations are required.

2.7.2 Telecommunications Installation Contractor's Responsibilities

1. Adherence to all of the above specifications
2. Assurance of labor harmony
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/6 cabling in the proper manner, with the appropriate number of twists, to maintain Category 5e/6 integrity and capabilities, as outlined in the TIA/EIA 568-B.2 standard.
6. The contractor must ensure that cable connections are in accordance with standard telecommunications practices and that all cabling maintains normal connectivity and continuity.
7. All materials must be agreed upon by PA Network Services prior to the start of installation.
8. All computer or network communication rooms and closets are to be isolated, locked, and secured. No other equipment, storage area, or smoking area are to be located in this room. This room must provide appropriate cooling and ventilation. Access to this room will be reserved to TEC staff and an agreed upon Facility Manager or designee of the site where the PAWANET equipment is located. This procedure is to ensure the security and the integrity of the Port Authority's computer network and its users.

2.7.3 Electrical Requirements

The following power and receptacles should be installed to support different equipment requirements such as:

- Standard 110/120 volt power receptacles
- Standard and/or NEMA L6-30P 220/240 volt 30 amp power receptacles
- Dedicated circuit breaker per AC feed, with alternate power source.
- Server rack electrical requirements are specified in the appropriate design document.

Currently, services obtained through the PA's contract are required to have the APC (American Power Conversion) UPS included in the delivered service.

2.7.4 Telephone Company Interface

The following items are needed for the telephone company interface, if needed for a specific vendor solution:

- a) Install a dedicated wallboard for Telco demarcs (if none available for implementation)
- b) Standard Telco demarcs:
 - P66 Block
 - Network Termination Unit (Rj48 interface) Smartjacks
 - Network Termination Unit (DB15-pin female interface)
 - Network Termination Unit (V.35/V.36 female interface)
 - Digital Signal X-connect (DSX)
 - Basic T1 CSU/DSU
 - Basic DS3 handoff coax/HSSI unit
 - High-speed dialup modems for network trouble-shooting when needed

2.8 Documentation

It is the responsibility of the System Administrator to update and maintain a library of all documentation designated as standard by the Port Authority. These include archived system files and system backups. Vendors will be provided our "Guide to Systems Administration" during the implementation phase of a project. The "Guide to Systems Administration" covers the provisioning and setup of computing &

networking resources to successfully implement a project within the Port Authority. Vendors will work with TEC during implementation to ensure proper setup, configuration and connectivity to PAWANET.

3.0 Virus Scanning & Management

3.1 Overview

This section describes the standards for the prevention, detection and removal of computer viruses, (malware). Its purpose is to minimize the risk and negative impact of computer virus infections in the work environment by establishing clearly defined roles, responsibilities and procedures for the effective management of computer viruses.

3.2 Standards

Standard virus protection software must be installed on all network servers and personal computers, and updated on a regular basis. The Port Authority currently uses McAfee ePolicy Orchestrator (ePO) to monitor, manage and maintain the virus definition (DAT files) of the Agency desktop computing platform. The McAfee ePO Management Agent, and VirusScan / AntiSpyware Enterprise, are part of the standard desktop core image.

3.3 Acquisition and Installation

The Technology Department maintains current versions of standard virus protection software and virus detection files, (DATs), including configuration-specific instructions for downloading and installing the software on network servers and desktops.

3.4 Virus Detection and Response

The Technology Department 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 Technology Department 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 Technology Department will report on all such outbreaks on a weekly basis. The report must include:

Support Ticket Number
User Name
Virus Name
Information which was lost, (if any)

Time to correct the problem, (lost staff time)
Virus Origin, (if this can be determined; Diskette, CD, Internet)

4.0 Electronic Mail

4.1 E-Mail Overview

The Port Authority's Electronic Mail System (E-Mail) is designed to facilitate business communication among employees, job shoppers, contractors, consultants, and outside business associates. This E-Mail system is comprised of Microsoft Outlook desktop software accessing e-mail stored on Microsoft's Office 365 Exchange Online servers. This solution also includes group calendaring and workgroup collaboration.

4.2 E-Mail System Architecture

The Port Authority's E-Mail system is hosted by Microsoft as part of its Office 365 government cloud services offering. Authorized Port Authority staff access their corporate e-mail through Microsoft Outlook desktop software as well as via Outlook Web App and through mobile devices. The Office 365 Exchange Online system has multiple Exchange servers containing mailboxes and Public Folders, and performs Internet-based e-mail services including anti-spam and anti-virus e-mail checking. More in-depth knowledge about the Microsoft Office 365 government cloud can be found on the Microsoft website.

Office 365 is accessed using the Port Authority's corporate user account which is hosted on the Port Authority's active directory platform. In addition, the Port Authority hosts DNS servers to satisfy requests from the Outlook client as needed.

High-speed, secure, and redundant network connections provide access to the Internet including to the Office 365 cloud from the Port Authority network.

4.3 E-Mail Environment: Design Considerations and Infrastructure

The Office 365 e-mail environment is further described below:

- The e-mail system is comprised of Microsoft Outlook 2007 desktop software accessing e-mail stored in Microsoft's Office 365 government cloud service. A current project will update the desktop environment to Office 365 Pro-Plus (Office 2013) and is tentatively expected to be completed by 12/31/2015.
- E-mail is protected by Microsoft's Exchange Online Protection.
- There are several forms of SMTP addresses used at the Authority.
- Exchange Active Sync and a cloud-based MaaS360 Mobile Server is used to provide e-mail and calendar access and control to Apple iPads/iPhones and Windows Mobile devices.
- Exceptions are governed by the Authority's directory services structure and user account requirements.
- Each individual e-mail message and its file attachments, the overall mailbox size limitations, and additional features are governed by the current Microsoft Office 365 government cloud specifications which can be found on Microsoft's web sites.
- 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. Email-enabled public

folders have been phased out and replaced by Office 365 Shared Mailboxes. Static documents like corporate policy statements are placed on the corporate intranet (EmployeeNet) and not on the Public Folders. Documents requiring long-term storage are stored elsewhere such as on Windows file servers.

4.4 Integrating Applications Server with Port Authority Email System

4.4.1 Requesting SMTP Services

The vendor will request SMTP services from and coordinate its work with the Technology Department.

Port 25 needs to be available to utilize it for SMTP services.

4.4.2 Email Restrictions

The following restrictions are in place to protect the SMTP system and the “reputation” of Agency mail servers on the Internet:

- Forged email headers are STRONGLY discouraged, but applications for circumvention will be entertained, and valid business justifications must be included. The “From” and “Reply-to” fields should be valid users on the system sending email.
- Settings: The maximum number of recipients per email is currently 90. This includes “To”, “cc”, and “bcc”; maximum size with attachments is defined by O365 Limitations. Emails that do not conform to these restrictions will be rejected by the SMTP servers.
- Mail will be relayed only if your server has an entry in the SMTP access database.

Note: SMTP logs are checked periodically for policy violations. Repeated violations and failure to correct them will result in SMTP services being disabled for the offending system.

5.0 Intranet

5.1 Intranet Overview

The Port Authority EmployeeNet (eNet) is intended to provide timely information and resources to employees via the web browser on their desktops. eNet is a decentralized collection of web pages, data lookup services and applications that are managed as if they were a centralized enterprise resource. It is accessible to all personal computer workstations on the Port Authority Wide-Area Network (PAWANET). eNet is housed on servers at the Teleport and PATC Data Centers.

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 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

Category	Software Name
Browser:	Microsoft Internet Explorer
Browser Plug-in:	Windows Media Player
	Adobe Acrobat Reader
	Macromedia Shockwave Player
Web Server Software:	Sun One Web Server
	Microsoft IIS
Media Server Software	Microsoft Media Server
Application Server Software:	Adobe Cold Fusion 10
Development and Design Tools:	Adobe CS5
Database	Oracle Database
	MS SQL Server
	MS Access
Programming Language/Scripts	ColdFusion MX 10 JavaScript
Search Engine	UltraSeek (software)
	Google Mini Search Appliance (hardware)

Category	Software Name
	MaxxCAT Search Appliance (hardware)
Web Performance Monitoring:	Google Analytics WebTrends Marketing Lab 2
Content Management:	Open Text Website Management

5.3.1 Design Standards

We have developed the following standards to ensure that all web pages on eNet have a consistent look, feel and navigation scheme, while providing creative flexibility.

Departmental Web Site Standards

Prescribed standards are assigned to only the following items:

Resolution:	Pages are designed for optimal viewing at the 1024x768 setting.
Page Width:	Each page has a fixed page width of 960 pixels.
Page Justification:	The entire page is center-justified within the browser window.
Page Layout:	Each web page will follow the same, basic layout: A Global Navigation strip; A Masthead; A Local Navigation strip; A Body area (with a 1-column, 2-column or 3-column layout); A Footer.

5.3.2 Accessibility Standards

TEC'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 standards and applicable legal requirements, contact the Webmaster via email at webmaster@panynj.gov, or call 212-435-3294.

6.0 Workstation Hardware and Operating System Software

6.1 Overview

The Port Authority makes extensive use of computers (workstations) networked into an Enterprise Wide Area Network to accomplish its business objectives. For the purpose of this section, the term computer and/or workstation will be used to reference desktop, laptop and CAD computing devices. In order to ensure compatibility with the agency's enterprise network and to make optimal use of its resources, this section defines the standards governing workstations and their configuration and use.

6.2 Workstation Operating System Standard

The Port Authority's standard operating system for workstations is Microsoft's Windows 7. The following are operating systems used within the Agency:

- Microsoft Windows 7, Enterprise
- Apple OS X

6.3 Workstation Configuration

6.3.1 Workstation Naming Conventions

All departmental workstations must contain a unique computer name which is the machine's serial number.

Example: Workstation name: 23AAH86

System Administrators are responsible for naming workstations and maintaining an up-to-date inventory of equipment and names used.

6.3.2 Automated Software Distribution for Computers

The Port Authority currently uses Microsoft System Center Configuration Manager (SCCM) 2012 to, at a minimum, do the following:

- Install new, or upgrade existing, software on Agency desktop, laptop, and CAD computers.
- Create packages to automate system tasks (e.g. data migrations of desktop computers, eDiscovery requests, etc.).
- Bare Metal Provisioning of Servers.

6.3.3 Remote Workstation Management

The Port Authority also distributes software applications and upgrades via Microsoft's SCCM. Each workstation should have Microsoft System Center 2012 R2 Remote Control Viewer installed as part of the workstation client. This will enable remote distribution and updates of software, hardware inventory and workstation troubleshooting. Microsoft security patches are distributed through a PatchLink agent.

6.3.4 Drive Mappings

Computer drive mappings are automatically accomplished using a Microsoft login script. The script is executed upon successful login to the Agency's Microsoft domain.

6.3.5 Standard Workstation Hardware Configurations

The Technology Department is responsible for setting the computer hardware standards. Standards are typically set annually, or as exceptions to meet business requirements. The standards specify the approved hardware components required by the Agency for a specific computing platform (e.g. desktop, laptop, CAD). The following is current workstation standard:

Lenovo ThinkCentre M93p Tower 10A6S19900-PA (PC)
Lenovo ThinkStation P500 30A6S0MM00 (CAD)
Lenovo ThinkPad T440 20AWS2EV00-PA (LAPTOP)
Microsoft Surface pro
MONITORS
NEC AccuSync AS203WMI-BK (20 Inch Wide Flat Panel)

NEC MultiSync EA244WM1-BK (24 inch Wide Flat Panel)

6.3.6 Standard Workstation Software

The following software is the standard Port Authority software for departmental workstations. New computer installations should conform to the existing standard.

6.3.6.1 Standard Workstation Software

The following list is a compilation of the core software components found on each computer (commonly referred to as an image).

- Windows 7, Windows 8.1
- McAfee Antivirus
- Internet Explorer
- Microsoft Office Professional
- Printer Pro
- Java
- Lumension End-Point Protection
- Remote Access Software (for laptops)

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

6.3.7 Enterprise Software

The following is a list of standard enterprise application software used in the Agency. These applications are supported by third-party service providers:

- PeopleSoft
- SAP
- Enterprise Connect (Livelink) Content Management
- One Drive for Business
- SharePoint/Online
- Skype for Business

6.3.8 Other Business Applications

Other Enterprise applications are deployed on occasion to user workstations. This includes systems like BudgetPro. System Administrators are responsible for deploying the workstation clients and network server software according to standards provided by Technology Department:

Current list of Enterprise applications, is shown below –

- AutoCAD
- BudgetPRO
- Cognos Client Software
- EBS (Emergency Broadcast System)
- Enterprise Connect (Livelink)
- HIDS,
- Lumension (PatchLink),
- McAfee Virus Scan and AntiSpyware Enterprise
- MS SQL

- Oracle
- PeopleSoft
- Primavera
- SAP
- Schedulesoft
- TRIM

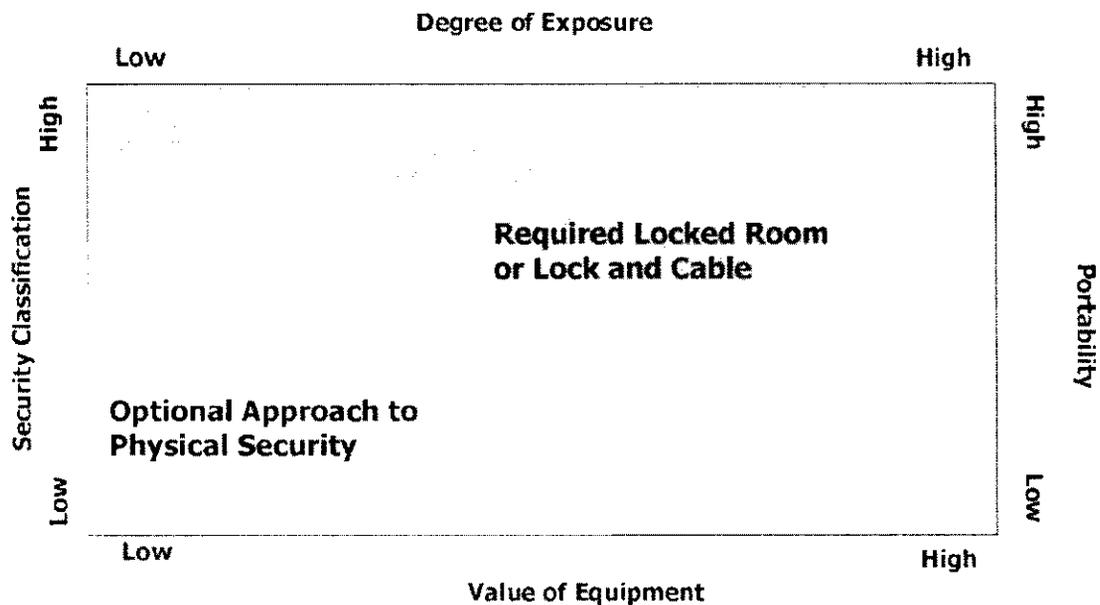
6.4 Workstation Security

Workstation users and their managers are responsible for the security of computer equipment and safeguarding critical corporate data and access to Port Authority network resources. This includes both the physical securing of equipment as well as logical safeguarding equipment and data.

6.4.1 Physical Security

The method of control should be based on the value of the equipment, the sensitivity of the data, its portability and the degree of exposure to theft. The department’s Business Manager should make the appropriate determination of physical security required based on their best business judgment.

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



In all cases, laptops must be secured with a Lock/Cable product (e.g., Kensington).

6.4.2 Logical Security

The Technology Department (TEC) is responsible for providing for the security of computer resources and devices:

- Workstations are protected with Microsoft directory security mechanisms.
- Screen saver passwords are implemented with a maximum of a fifteen (15) minute time-out.
- All critical data on a network drive are backed up nightly onto either external media or a network storage.

7.0 Distributed Systems Environment

7.1 Overview

A number of enterprise servers provide critical application and system services. Different operating systems and configurations may be required for specific applications. This section provides information on the standards 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 2008 Server (Enterprise) and 2012 Server are currently supported Operating Systems for application servers.

7.2.1 Virtual Environment

The standard for Virtualization Computing is IBM host servers. The Port Authority will provide a VMware ESXi-based Guest Virtual Machine (VM) to operate all Contractor-provided applications software.

All applications software will be capable of operating in a virtual environment under VMware ESXi server and will operate in a VMware ESXi-based Guest Virtual Machine (VM) on a 'shared' host-computing platform for Contractor application, unless performance or other requirements mandate a dedicated system.

7.2.2 Windows Data Encryption

For those applications that require additional data security measures, TEC offers additional tools that provide encryption services to protect the data stored in the application's database or file and folders, even from authorized individuals that have physical access to the applications and database servers but not the decryption key.

7.3 Unix

Sun/Oracle Solaris and RedHat enterprise Linux are the currently supported UNIX operating system for infrastructure and corporate servers.

7.3.1 Unix Security

Unix and Linux servers must be physically and logically secured from unauthorized access. Operating system logical security is defined by the Technology Department (TEC).

7.3.2 Backup

Critical system backup must be performed regularly (daily and/or weekly) utilizing our centralized backup strategy and associated tools. Extra copy of backup is kept offsite for disaster recovery purposes if required.

7.3.3 Download Scripts in the Unix/Linux Environment

- The script must be written in a generally supported language: Perl, Korn shell, PowerShell. PowerShell will be consistent with Microsoft standards and best practices.
- The script must be limited in access, as well as the script's owner's user account. The owner of the script should be able to read, edit, and execute the script, but no one else (with the exception of the root or administrator accounts).
- If the content being downloaded is public information or widely available on the Internet, File Transfer Protocol (FTP) may be used.

- For all other content, Secure FTP must be used, and a key exchange made with the entity who is providing the content. A username and password must be used when retrieving the content.
- If the entity cannot accommodate the use of SFTP, ftp may be used as long as the content is encrypted with a secure, widely used utility like PGP.
- Information and guidance on securing passwords should follow Recommendations of the National Institute of Standards and Technology.

7.4 z/OS

z/OS (currently release 1.5) is the IBM-supplied operating system on the IBM Z096-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. The Agency is dis-investing from this operating system and it will not be used to support additional applications.

7.4.1 Databases

Oracle 11gR2 or higher and MS/SQL Server 2008/2012 or higher are the supported database platforms for Port Authority systems. Auditing trail enabled for all database accounts with administrator privileges.

7.4.2 Geographic Information System

The Geographic Information Systems (GIS) is built on an ESRI platform using ArcGIS for Desktop version 10.2 and ArcGIS for Server version 10.2. GIS data are stored in geodatabases using SQL Server 2012.

7.5 Application Security

TEC recognizes the critical importance of application security and maintains a Best Practices document containing rules and recommendations for purchased applications, and those developed in-house.

7.6 Server Physical Security

All servers and communication equipment must be located in locked rooms or secured with a cable and lock with the keyboard secured to prevent tampering and unauthorized usage. The Business System Manager is responsible for determining the appropriate access control method (receptionist, metal key lock, magnetic card door locks, etc.) This person must also maintain a list of persons authorized to enter secured areas. Technology Department staff is available to provide technical assistance in making this determination.

7.7 Load Balancing – Failover Architecture

Depending on the requirements of the application, load balancing and failover architectures are supported.

8.0 Vendor Provided Dedicated Systems

8.1 Overview

Vendor Provided Dedicated Systems refers to the application software and possibly the computer hardware that may be furnished and/or installed by an outside contractor. These systems are usually procured through either a Request for Proposal (RFP), or a “Low Bid” contract and are specifically engineered to support a dedicated application.

These systems generally support Capital Projects, which are usually large scale, multi-year engagements, requiring specialized technical and management staff, as well as, Systems Integration support. These projects normally have significant construction components and require the coordination, design and support from many diverse Engineering and Technology disciplines.

On all technology related projects a representative from the Technology Department (TEC) provides a single point of contact for technology oversight, accountability, adhering to standards and systems integration, which is required under the Roles and Responsibilities of the Director and is expected by our client departments.

To ensure a successful project implementation and honoring our responsibility to the Agency and our customers, one of the steps undertaken by TEC is to provide guidance and focus attention on, adherence to and compliance with the Port Authority Technology Standards.

By following the Technology Standards, it enables the Port Authority to

- Leverage large discounts negotiated in the various requirements contracts.
- Ensure that the seamless integration of equipment with other existing systems.
- Ensure that long-term maintenance and systems administration contracts are focused on the same product lines.
- Ensure that the relevant sections of the Technology Standards are included in either, the basic design of a low bid contract or as requirements in an RFP. Responses to RFP's shall be reviewed for their compliance with the Technology Standards.
- Deployment, integration and testing shall be monitored by TEC to ensure that equipment or infrastructure is not duplicated, that the integration and migration plan will not adversely affect existing systems, and to integrate new systems under existing maintenance contracts where applicable.

In cases where a specific vendor or system is so specialized that it normally does not adhere to the hardware, software, infrastructure and operations standards of the Technology Standards, the vendor shall be directed to work with TEC in exploring all options. If an exception is required, the vendor should work with TEC to prepare the necessary business case scenarios to receive written concurrence from the CTO for this deviation from the Port Authority Technology Standards.

8.2 Physical Security Technology Standards

8.2.1 Agency Standard for Digital Video Recording, Access Control and Alarm Monitoring

Based upon the Agency's investment and positive experience with commercial leaders in access control and alarm monitoring application, CCTV and Digital Video recording technologies. The Agency has developed a standard for these business functions.

The Port Authority has long recognized the need for a corporate architecture for its security systems that would allow us to integrate digital video and access control recording compatible technologies agency-wide. Using these standards will improve the Agency's security posture and will permit us to leverage additional operations and business benefits while keeping our operations resources, maintenance and support costs at a minimum.

The standard will also improve:

- Access to and the sharing of information from a centralized location
- Centralized monitoring of all facilities from an Emergency Operations Center

- The operational and cost-effectiveness of adding a variety of modular features to the core systems, such as paging, e-mail, fire systems, facility management, etc.
- Alarm notification, response, and acknowledgement
- Operational flexibility for facility and Public Safety staff
- Single learning curve
- Reduce the cost for maintenance and system administration

8.2.2 Situational Awareness Platform Software

The Situational Awareness Platform Software (SAPS), is a software application that allows multiple, independently manufactured and installed security, life safety, and building systems to all interoperate under a single, common operating picture, giving a user access to information spreading across multiple systems as if they were all one single system. This “common view” is made even more valuable by the incorporation of powerful, rules-based tools within the SAPS system, which allows intelligent linking of seemingly unrelated events into “Situations” that represent patterns of activity that pose a threat to security or site-wide operations.

The SAPS objective is to monitor the identity and event data from the various systems, identify incidents and anomalies, and detect trends that could be a threat to our facilities. SAPS turns data into actionable intelligence when an incident is detected. SAPS have the capability to automatically alert the security operations staff and push the information to security control centers and first responders.

- Provide a software platform to enable integrating the various electronic systems across all agency sites
- Provide a single software perform solution for situational awareness.
- Provide a single system database for reports
- The SAPS will provide transparent notification of security related events for all agency security systems.

8.3 Communications Infrastructure Standards

The Port Authority Standard for Communications Infrastructure is Cisco. This applies to all future systems, as well as, upgrades to existing systems. This standard ensures the interoperability of all deployed systems and permits the full integration of systems into PAWANET. In addition, all Cisco equipment either designed in a low bid contract or specified in an RFP must be purchased through the Cisco Requirements contract, which is administered by TEC 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 CTO.

8.4 Server Infrastructure Standard

The Port Authority’s standard platform for File & Print and Application servers is IBM.

Technology Department has contracted discounted pricing with our service provider for its servers and hardware support. In order for the agency to take full advantage of these savings, any new Application servers or File & Print servers must be built using IBM hardware purchased by TEC. 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 CTO or his designee.

9.0 Wireless Technologies

9.1 Wireless Standards

9.1.1 Purpose and Scope

This section references the standard policies and procedures for all wireless devices and technologies including voice and data capabilities that store, process, transmit or access data. This includes but is not limited to commercial and unlicensed wireless networks and laptops, cellular devices, scanning devices, messaging devices (email devices) and PDAs.

9.1.2 General Policy

Employees will only use PA owned wireless devices to store, process, transmit or access PA data.

9.1.3 Personal Area Networks - PAN

PAN technologies should not be used for transmitting information without encryption.

Bluetooth security alone is unacceptable because it is not encrypted and does not use Federal Information Processing Standardization (FIPS) 140-1/2.

9.1.4 Wireless Local Area Networks – WLANs

9.1.4.1 Overview

Business requirements have arisen throughout various Port Authority locations for the improved use of Wireless LAN technology to facilitate local user mobility. Research performed on the different technologies support the use of Cisco as opposed to various wireless vendors in an attempt to produce a standard that will provide the agency with a secure, robust and scalable solution as WLAN's continue to grow within the agency.

In summary, the current Port Authority Wireless LAN standards are based upon IEEE 802.11n draft 2.0 technologies. (802.11n is backwards-compatible with existing 802.11a/b/g network adapters.)

The physical infrastructure is now based upon a centralized WLAN architecture that relies upon Cisco wireless bridges, access points, mesh routers and newly implemented controllers. WLAN's should be standardizing on the 4404 and 4402 controllers at this time as described further in this document.

Wireless LAN technology is continually developing with rapidly evolving industry standards, government regulations, and vendor products. As a result, the WLAN Standard presented in this document will likely be superseded in the future as the technology and products change.

9.1.4.2 Scope

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

9.1.4.3 Principles

At the highest level, the principles for the Wireless Standard are based upon the following attributes:

- Security - use of strong encryption (e.g. WPA-TKIP / WPA2- AES) for use as authentication of all traffic on a port-to-port basis, with the use of credentials stored on a back-end RADIUS server utilizing key distribution.

- Scalability - with LWAPP access points & use of LWAPP tunnels
- Reliability - via authentication of users to the networking enterprise mode.
- Manageability - via secured ports and VPN / FW access.

9.1.4.4 *Compliance Requirements*

All specifications defined in this section may be effective upon approval of and complete concurrence with TEC's CTO, to update wireless standards and policies as per IEEE and Wi-Fi Alliance Standards

9.1.4.5 *Device Specifications*

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

9.1.4.6 *Access Point (AP) Standard*

Standards Details:

- 3600 AP's are the agency standard for WLAN deployment. These AP's have 802.11n 2.0 radios. Backward compatible to 802.11 a/b/g.
- 1310 AP/ Bridge is certified for use in unique situations where both internal and external antennae are supported. The major distinction is that of a more rugged chassis designed for higher-stress outdoor-type conditions. 3250 mobile routers for mesh deployments.
- AP Deployments will be Lightweight Access Point (LWAP)
- AP Standard Summary:
 - a) Two cables per pull during wiring for wired to wireless.
 - b) AP's & controller placements via RF propagation results.
 - c) PA supported standard AP's need to be verified with TEC
 - d) If wireless is primary connection-'load-balance' AP' cabling connection to two different network switches
- WLAN Controller Standard
This standard is in the process of being upgraded to Network Control System (NCS) & Identity Services Engine (ISE) Appliance to accommodate more advanced wireless deployments.

9.1.4.7 *Best Practice*

The following information is industry best practices for wireless hardware implementation used for the Agency's deployments, not for wireless device configuration practices.

WLAN Best Practices Add-ons:

1. Ensure that the PA maintains an up-to-date wireless hardware inventory.
2. Identify rogue wireless devices via wireless intrusion prevention systems (IPS)
3. Enable automatic alerts on the wireless IPS
4. Perform stateful inspection of connections.
5. Augment the firewall with a wireless IPS
6. Mount AP in location that do not permit easy physical access
7. Secure handheld devices with strong passwords
8. Enable WPA and WPA2 under ENTERPRISE mode
9. Synchronize the AP's clocks to match networking equipment.
10. Manage remote physical locations of all access points which support an isolated network that needs access to PAWANET for server farms and internet access.
11. Maintain cryptographic strength range from 128-bits to 256-bits with matching symmetric algorithms AES-128 to AES-256

Wireless Control System (WCS):

1. Single license
2. Secure “WIRELESS LOCATION APPLIANCE” with real-time client tracking & RF fingerprinting
3. Secure Windows-Based deployment as minimum, for example, windows server 2003; intel dual-core; 3.2 GHz; 4-GB RAM; 80-GB hard drive; IPS devices; IOS firewall routing; HTTP port 80; HTTPS port 443.
4. Multi-homed server (i.e., two NIC cards)
5. Secure WCS and IIS (i.e., internet information service), installation sequence
6. Create configuration group (configure multiple controllers)
7. Secure auto provisioning with filtering
8. Secure WCS with RF modeling for heat map planning
9. Secure 15 second alarm summary refresh

9.1.4.8 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 is not permitted to operate wirelessly at the same time. Wireless solutions could create backdoors 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 are required on devices and workstations that are used to synchronize/transmit data, if available. Where not available on a device, 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 is required.
- PEDs need to be capable of being erased or overwritten to protect data. If the device is no longer needed and cannot be erased or overwritten, it must be physically destroyed.

9.1.4.9 Cellular and Wireless Email

Cellular and wireless e-mail devices are subject to several vulnerabilities (e.g. interception, scanning, remote command to transmit mode, etc). Therefore, the following procedures apply:

- 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 will be used.
- The use of LANS and Wireless transmitters, i.e. Bluetooth etc. by PANYNJ personnel using PANYNJ equipment is strictly prohibited

9.1.4.10 Synchronization

Some synchronism systems will operate even if the workstation is locked and the wireless or handheld device is not registered with the sync application on the workstation. As long as the workstation is on, the user is logged on, the data application client (e.g. MS Outlook) is active, and the “hot sync” cable is attached to the workstation; any person can place a compatible wireless or handheld device in the “hot sync” cradle and download data. Therefore, the following procedures apply:

- “Hot sync” cable or cradle has significant security risks, therefore perform “hot sync”, and then remove immediately once “hot sync” operation is complete.
- Secure “hot sync” cables and cradles.
- Use only PA approved third party sync access control software installed on all workstations.
- PA owned devices may only be synchronized with PA owned computer systems

9.1.4.11 Responsibilities of Technology Department

- Monitor and provide oversight of all PA wireless activities, insure interoperability of wireless capabilities across the agency.
- Develop appropriate technical standards 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.
- Adhere to wireless procedures and standards, establish procedure for reviewing and approving requests for using wireless devices to store, process, or transmit information.
- Establish procedures for periodically reviewing approved wireless devices and services to ensure that the business requirement for device/service/system is still valid and meet current PA guidance.
- Establish procedures for inventory and control of wireless devices and equipment.
- Establish procedures and implementation plans for auditing wireless connections to the network.
- Provide user training.

9.1.4.13 Responsibilities of Wireless and Handheld Device Users

- Coordinate all requests through Technology Department...
- Read and follow standards.
- Access information systems using only approved wireless hardware, software, solutions and connections.
- Take appropriate measures to protect information, network access, passwords and equipment.
- Use approved password policy and bypass automatic password saving features.
- Use extreme caution when accessing PA information in open areas where non-authorized persons may see PA info (airport lounge, hotel lobby).
- Protect PA equipment and information from loss or theft at all times, especially when traveling.
- Keep current anti-virus software on devices.
- Use appropriate Internet behavior (e.g. approved downloads).
- Exercise good judgments in efficient cooperative uses of these resources and comply with current and future standards of acceptable use and conduct at all times.
- Report any misuse of wireless devices, services or systems to management.

9.2 Cellular Phone & Wireless Modem

The Port Authority obtains cellular service under governmental contracts. All orders for cellular service or equipment must be placed under these contracts. If the contract service provider cannot meet the requirements, a memorandum requesting approval to obtain cellular service outside of the contracts must be sent to the CTO.

9.3 Technology Mobile Device Policy

9.3.1 Introduction

Mobile devices are a class of handheld computers that currently offer limited functionality with compact size and portability. Additional functionality such as Word and Excel are already included in many Mobile devices, with further enhancements predicted.

In order to better serve the PA, and to limit the expense of supporting a wide variety of Mobile device hardware and software, Technology Department will support the use of the Windows and Apple IOS based devices.

With a Mobile device, a user can maintain their calendar, address book, to-do list, and e-mail on a platform that is very portable and easy to use. Integration with Outlook makes it possible for users to keep identical, synchronized copies of data on both the desktop application and the Mobile devices.

9.3.3 Software

The current version of Apple IOS software are supported.

Microsoft ActiveSync is used for connecting to the corporate E-Mail system.

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

9.3.4 Support

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

9.3.5 Training

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

9.3.6 Acquisition

The PA will purchase Mobile devices for employees with a business need for the mobile device. Employees are responsible for obtaining management approval. TEC also recommends that a protective case (preferably a zippered case) be purchased to reduce damage to the units.

Since the PA owns the device, if an employee leaves the PA, the device is returned to the Director's office of their department.

9.3.7 Personal Acquisition

Employees, who purchase their own mobile devices, will not be allowed to connect to the PA corporate network or equipment, unless approved by Technology Department.

Customer Support Desk personnel will support all PA owned and authorized mobile devices.

9.3.8 Data Security Considerations

Users should carefully consider what type of information they store on their mobile. Extreme caution should be taken when using company confidential data on the mobile units.

All mobile devices accessing corporate resources are to be password protected.

9.3.9 Data Backup

Though it does not happen often, it is possible to lose or damage the data that resides in the mobile devices. Technology Department will provide assistance in attempting to recover files or data from data corruption.

Appendices

Appendix 1 -- Business Resumption Plan Document Format

I. PURPOSE

- Goals and objectives of plan
- Benefits obtained if plan properly implemented

II. SCOPE OF PLAN

- Planning assumptions
- Facilities and resources included in plan

III. NOMENCLATURE

- Recovery terms
- Definitions and acronyms

IV. DISASTER SEVERITY DEFINITION

Define level of potential disaster based on impact to critical functions. Explain what degree of operational disruption would constitute each level of disaster:

- catastrophic
- serious
- major
- limited

V. OPERATIONS RECOVERY PROCEDURES (Procedures for recovering services)

1. Indicate time frames in which essential operational/business functions must be resumed.
2. Specify sequence of operations recovery events and individuals responsible for activity. Note any specific activities required for particular levels of disaster severity. For example:
 - Notifications
 - Preliminary evaluation
 - Activate operations recovery personnel
 - Coordinate with emergency personnel
 - Evaluate recovery options and issue directive which details:
 - Assigned tasks
 - Project schedule/time frame
 - Coordination required
 - Identify relocation activities, if required
 - External/internal status updates
3. Identify items required for backup of critical functions. For example:
 - Alternate work site
 - Hardware/software

- Personal computers
- Necessary software packages
- Documentation
- Peripherals (printers, modems, etc.)
- Databases
- Emergency equipment
- Communications
- Transportation
- Supplies
- Security
- Operations and procedures manuals

VI. OFFICE/FACILITY BUSINESS SITE RESTORATION PROCEDURES

(Procedures for restoring physical facilities)

- Identify restoration responsibilities
- Assess damage
- Develop restoration plan/time frames

VII. BRP UPDATE PROCEDURES

- Specify responsibility for updating and communicating BRP changes
- Indicate frequency of review/update

Appendix 2 -- Communication Rooms/Closets Standards

SPACE

All data communication rooms must be designed with required and estimated space to meet immediate requirements, as well as, future growth.

ENVIRONMENTAL

The following conditions must be met:

- a) Doorways/Entrances must be designed to support at least the minimum space requirements of 90"Hx72" Wx60" D.
- b) The room's cooling capabilities must be sufficient to support the heat dissipation requirements for the equipment. This requirement will be measured in minimum and maximum BTUs powered by AC-powered systems. Equipment specs will be supplied by TEC 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.
- f) Cables trays must also be installed in the communications room ceiling where appropriate, to support the routing of data communications and Telco cables.
- g) Basic 24"W/30"D/84"H cabinets with 19" racks must be installed to house communications equipment such as: routers, switches, hubs, DSUs/CSUs and monitors.
- h) To create more wall space the use of wall mount racks can be installed, however, all wall cabinets must support rear access to the equipment. Appropriate sized plywood must be installed prior to mounting racks.
- i) Category 5e/6 cable must be terminated in wall/rack mounted patch panel.
- j) Fiber patch panel must be installed in fiber IDF panel with SC female interface.
- k) The fiber must be neatly tie wrapped and enclosed in flexible inner-duct.
- l) Telephone access must be installed in the appropriate location to provide for basic troubleshooting and vendor support.
- m) All communications equipment and cabinets must have ample room for easy access and proper ventilation.

Appendix 3 – Standard Cabling Schemes

- a) Teflon-coated cables will be installed per fire code regulations.
- b) Overhead cable trays and drop post must be installed for cable routing.
- c) Cabling scheme must be used to label and identify all cables. All cables must be neatly tie-wrapped.

Appendix 4 -- Unified Wiring Plan

To satisfy existing and future voice and data communications requirements, while minimizing the need for wiring changes and additions, the Port Authority has adopted the following lateral wiring specifications for all workstations being constructed. This plan is applicable to all PA locations, except when specifically noted.

LATERAL CABLE:

Voice and data telecommunications requirements for each workstation will be provided by a combination of three individual cables, installed between the workstation and the serving telephone closet / intermediate distribution frame (IDF), in a "home run" configuration. All cabling installed will be of plenum type, fire retardant (FEP) rated.

Cable specifications:

(3) Cables capable of supporting Category 5e/6 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/6 cable is as follows.

TECHNICAL DATA--ELECTRICAL				
Frequency MHz	Horizontal		Patch	
	Attenuation dB/100 m max.	Next dB min.	Attenuation dB/100 m max.	Next dB min.
1	2	62.3	2.4	62.3
4	4.1	53.2	4.9	53.2
10	6.5	47.3	7.8	47.3
16	8.2	44.2	9.8	44.2
20	9.3	42.7	11.1	42.7
31.25	11.7	39.8	14.1	39.8
62.5	17	34.3	20.4	34.3
100	22	32.3	26.4	32.3

TECHNICAL DATA--PHYSICAL			
	CMR	CMP	CM (Patch)*
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 Propagation	72% nom. Non Plenum	72% nom.
Input Impedance	100 + 15% 0.7772-100 MHz	100 + 15% 0.772-100MHz
	ISO/IEC 11801	

COLOR CODE			TEMPERATURE RATING	
Pair 1	White/Blue	Blue	Installation	0 degrees C to +50 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 5 -- Telephone Closet / IDF Termination Blocks

Lateral Data cabling serving each workstation will be terminated on a CAT5e/6 patch panel (RJ45 face, 110 punch rear) in the telephone closet. For analog phone service, termination is to be on 110 blocks in telephone closet, allowing access to the telephone riser. For data, a patch cord is installed between patch panel and IT device. The patch panel can be mounted on the wall with a wall mount kit or in a rack if one is needed and should be appropriately numbered with the workstation number. The patch panel must be capable of supporting Category 5e/6 the TIA/EIA-568-B.2 standard. The patch panel shall have a swing away faceplate or rack mountable.

NOTE: The Category 5e/6 patch panel should be equivalent to the AMP SL series 110Connect Category 5e/6 patch panel or approved Category 6 patch panel. The number of ports may vary.

Each workstation shall be assigned a unique station identification number.

Appendix G – Workstation Jacks

Workstations will be equipped with various components of the AMP Communications Outlet system (AMP equivalent can be used with TEC approval). Each workstation will be installed with (1) double-gang jack housing box and matching face plate, capable of securely mounting three Category 5e cables or Category 6 and four modular data connectors, maintaining the integrity of category 5e/ Category 6 capabilities as outlined in the TIA/EIA-568-B.2 standard. All workstation jacks will be wired in accordance with the TIA/EIA-568-B.2 standard. All modular jacks are to be labeled in accordance with TEC number schema.

Appendix 7 -- Standard Switches Inside the Department

Any switches in the following Cisco series are acceptable (Vendors will consult with the Technology Department (TEC) to determine the appropriate switch configuration at the time of proposal submission):

- Cisco 3000 series – low capacity

- Cisco 4000 series – medium capacity

- Cisco 5000 series – medium capacity

- Cisco 6000 series – high capacity

- Cisco Nexus 7000 series – high capacity

- Cisco Nexus 9000 series – medium and/or high capacity

Appendix C – Workstation and Lateral Cable Identification Management

WORKSTATION AND LATERAL CABLE IDENTIFICATION/MANAGEMENT (Facility)

All lateral cabling installed to workstations at the Port Authority Facilities must be designated in accordance with the Port Authority's workstation and lateral cable identification code: This code consists of two elements, as follows:

- 1 - Room number or department name (acronyms are acceptable).
- 2 - Workstations (3 numeric digits)

The cable identification code for Workstation 10 in room 3801 at LGA CTB is 3801-010. The cable identification code for Workstation 15 in PA Automotive shop is Auto-015

Appendix 9 – Fiber Optic Specification for Network Services - PAWANET

General Scope of Work

1. Conduct a walk thru based on the specific Scope of Work for the job in question.
2. Note that all diagrams and or sketches that may be provided are approximates and not to scale.
3. All fiber optic cable is to be installed in rigid conduit or, where applicable, in plenum rated flexible inner duct.
4. Contractor shall furnish and install fiber optic cable as designated in the specific Scope of Work.
5. Fiber optic cable type for interoffice use shall be loose tube, with aramid yarn water block:
 - Singlemode Fiber – 8.3/125/250 micron diameter (core/cladding/coating) manufactured by General Cable or approved equal.
6. Fiber optic cable attenuation from the factory, before installation, shall not exceed:
 - Singlemode – 4db per km @ 1310nm/.3 db per km @ 1550nm
7. All fiber optic cable is to be labeled on each end and at any junction or patch panel with, 28 gauge, 2” wide embossed with ¼” high letters. The labels are to be fastened to the fiber optic cable using sealed wrap around labels or pliable Velcro ties.
8. Fiber optic cable shall be installed in accordance with the manufacturer’s specifications. Any portion of the cable damaged during installation will be repaired or replace by the contractor without any additional cost to the Port Authority of New York New Jersey.

Fiber Optic Terminations

1. Fiber optic terminations will use **SC** connectors unless otherwise specified in the Scope of Work.
2. Fiber optic terminations shall not yield more than 1db per mated (at the bulkhead) connector.

Fiber Optic Testing

1. Fiber optic testing shall be performed by the contractor and certified fiber optic technicians.

Fiber optic technicians will be prepared to complete test procedures with the following equipment:

- Source and power meter testing to provide optical loss measurements.
 - Reference test cables and mating adapters that match the cables to be tested.
 - Cleaning materials – lint free cleaning wipes and pure alcohol.
 - OTDR test set with the proper launch cables and adapter types.
 - Power loss testing from both ends.
2. Fiber optic technicians will perform OTDR test on all terminated fibers unless otherwise noted in the Scope of Work.
 3. Fiber optic test results shall be recorded, and reports provided to the PA in hardcopy and via a readable txt file (PDF or RTF is acceptable).

Appendix 10 -- Public Telephone Ordering Standards

Technology Department (TEC) staff is responsible for the management of the permit for public telephone service are available to answer any questions and provide direction for any matter relating to public telephones.

General Standards

All public telephone requests – that is both coin and non coin in any Port Authority space or any area of the tenant space – both “public” and “club” locations will be coordinated by the Port Authority to cover both New York and New Jersey.

Process

When the Facility, Property Manager, tenant or their representative (e.g. designer, architect, general contractor) has a public telephone requirement, they will contact the Technology Department (TEC) whom will review the request and provide coordination with the appropriate service provider.

ATTACHMENT H

PART II Cyber Security Guidelines

**CYBER SECURITY
GUIDELINES FOR THE PORT
AUTHORITY OF NY & NJ
V 3.4**

Prepared by: Technology Services Department (TSD)

As of August 15, 2011

Table of Contents

- Introduction**..... 3

- 1. User Authentication**..... 3
 - a. User Accounts..... 3
 - b. Password Authentication..... 3

- 2. Information Assurance**..... 4
 - a. Computer Devices (Desktops, Laptops, CAD Workstations)..... 4
 - b. Mobile Computing Devices..... 5
 - c. Servers..... 6
 - d. Virtual Environment..... 6
 - e. Portable Media..... 7
 - g. Cyber Scrubbing..... 8

- 3. Data Center**..... 8

- 4. PAWANET**..... 9
 - a. Network Devices..... 9
 - b. Firewalls and Intrusion Detection Appliances..... 10
 - c. Proxy Service..... 11
 - d. Remote Access (Client-to-Site)..... 12

- 5. Virtual Private Network (VPN) (Site-to-Site)**..... 13

- 6. Internet Access**..... 14
 - a. Outbound Traffic Requests..... 14
 - b. Inbound Traffic Requests..... 14

- 7. E-Mail**..... 15
 - a. E-Mail Hosted Environment..... 15
 - b. E-Mail Virus and Spam Protection and Content Scanning..... 15

- 8. Desktop Patch Management**..... 16

- 9. Server Patch Management**..... 16

- 10. Content Management**..... 16

Introduction

The Port Authority significantly relies on Information Technology (IT) to support its various businesses and achieve its strategic mission. To ensure that information and systems are safe, the Technology Services Department (TSD) has developed a formal IT Security Program and Cyber Security Guidelines, focused on protecting the Agency from all types of security threats to the Agency's IT infrastructure.

The Cyber Security Guidelines encompass all systems, automated and manual, for which the Agency has administrative responsibility, and identifies measures taken to protect a network, system, computer device, etc., against unauthorized access or attack.

1. User Authentication

a. User Accounts

- i. The Agency uses the Request for Access to Information Systems (Form PA 3624A), which can be found online on ENet, for all user account and systems access adds, changes and deletions. The form is submitted by a Port Authority employee and is approved by the departmental approver.
- ii. Upon approval from the department, the form reaches TSD and is reviewed by TSD for approval or denial.
- iii. If elevated rights (i.e., Administration Rights) are requested with expiration date identified, Assistant Director of Technology Infrastructure approves; if requested not to expire, Director of TSD approval is required before processing.
- iv. Both Daily and Weekly personnel additions and terminations are forwarded to TSD. TSD ensures that 3624A's exist, or are processed for, each change. Submission of personnel transfers, however, are the sole responsibility of the Business Manager.
- v. All users accessing the Port Authority's network must authenticate to the Agency's Directory Services. Directory Services is a database containing descriptions of all network devices including servers, printers, shared devices and user accounts.

b. Password Authentication

- i. A "strong" password should be created:
 1. User accounts should be changed every 30 days; You must change every 90 days
 2. Administrator accounts must be changed every 30 days
 3. At least eight characters is preferred; Six characters is the minimum
 4. Should include both alpha and numeric characters
 5. May include at least one special character
 6. May include both upper and lower case letters
 7. Cannot reuse password within a one-year period
- ii. Accounts on servers, desktop and laptops are locked after five (5) unsuccessful login attempts. Accounts on BlackBerry devices are locked after ten (10) unsuccessful login attempts.
- iii. Initial password for systems and applications access should be changed on first login and may only be changed once a day.

- iv. Never write it down
- v. Never share it
- vi. Cannot be stored in clear text
- vii. Cannot be stored in an automated logon process (e.g., macro, application code, etc.)
- viii. Notify the Customer Support Desk, 10-7469, immediately if you suspect your password has been compromised

2. Information Assurance

Downloading and printing Confidential Information carries with it the responsibility to protect that information in accordance with the requirements of the Agency's Information Security Handbook (<http://eNet.panynj.gov/home/pdf/Corporate-Information-Security-Handbook.pdf>). In addition, possession of electronic files containing Confidential Information assumes full responsibility for the proper handling, storage and transmittal of this type of information in the same manner as hard copy requirements.

Users who possess electronic files containing Confidential Information shall adhere to the following guidelines to maintain the proper protections of this material.

Electronic equipment that has a storage device or persistent memory, such as desktop computers, laptops, CAD desktop computers, portable computing devices (e.g., BlackBerry devices) must adhere to the following guidelines to maintain the proper protections of this material.

a. Computer Devices (Desktops, Laptops, CAD Workstations)

- i. All computing for the Agency is performed on PA approved computer devices. To protect them against viruses and malicious software, (e.g., Trojan Horses), McAfee VirusScan Enterprise & AntiSpyware is installed. In addition, software restriction policies are fully integrated with Active Directory and applied on all computer devices to prevent unauthorized installation of non-standard applications. Agency approved software, which can be found on the TSD Department eNet site, is installed by TSD. Each Line Department is responsible for maintaining a current inventory of their approved Line Department specific software licenses and for providing proof of license to the TSD at time of installation request.
- ii. TSD oversees the System Administration and day-to-day operational support for PA approved computer devices.
- iii. The automatic lock/screen saver feature will activate after a period of fifteen (15) minutes of non-use.
- iv. TSD maintains a "chain of custody" process surrounding all hard drives. Currently, all removed hard drives are managed and stored off-site at a secure location. Required exceptions are in place with the Office of the Inspector General (OIG) and Public Safety (PSD).

- v. User Responsibilities:
 - 1. Individuals granted access to the Port Authority's network or information systems shall secure computer devices from unauthorized access.
 - 2. When leaving a computer device unattended, users should apply the "Lock Workstation" feature (Ctrl/Alt/Delete, Enter).
 - 3. Unattended computer devices should be secured from viewing by password protected screen savers.
 - 4. Confidential Information must be stored on a networked drive directory rather than the computer device's hard drive. (Note: Due to the nature of the functions of the Office of Inspector General [OIG], there will be occasions when OIG must deviate from this practice.)
 - 5. Computer devices and monitors should be turned off at the end of each workday.
 - 6. Users must not disable or alter security safeguards (e.g., virus detection software) installed on the PA approved computer device.
 - 7. Users must not load non-Agency software or proprietary non-Agency data onto an Agency owned computing device.

b. Mobile Computing Devices

- i. All mobile computing resources (e.g., laptops, BlackBerry devices, mobile phones, etc.) and information media must be secured to prevent compromise of confidentiality or integrity while on or off Agency premises. Information contained on these mobile computing devices is governed by the Information Security Handbook (ISH).
- ii. Personal Mobile Computing Devices are not allowed to connect to the Agency's corporate network or infrastructure, unless pre-approved by the Director of TSD.
- iii. To protect data information and hardware, a password is required on every BlackBerry device. An inactivity timeout value is set to lock the device after 30 minutes of inactivity.
- iv. TSD maintains a "chain of custody" process surrounding all hard drives. Currently, all removed hard drives are managed and stored off-site at a secure location. Required exceptions are in place with the Office of the Inspector General (OIG) and Public Safety (PSD).
- v. User Responsibilities:
 - 1. Care must be taken when using mobile computing devices in public places, meeting rooms and other unprotected areas outside of the Agency's facilities. Protection must be in place to avoid the unauthorized access of information stored and processed by these devices. *Please contact TSD to discuss protection measures if you identify a device/scenario meeting such criteria.*
 - 2. It is important that when such devices are used in public places, care must be taken to avoid the risk of unauthorized persons viewing information on the screen.
 - 3. Mobile computing devices must be physically protected against theft, especially when in transit (e.g., car, train, plane, etc.) or at rest (e.g., hotel rooms, conference rooms, etc.).

4. Equipment carrying important, sensitive and/or critical information must not be left unattended and must be physically locked away and secured.
5. Mobile computing devices must not be checked in airline luggage systems. These devices must remain in the possession of the Port Authority employee at all times.
6. By default, Wireless Detection (e.g., Bluetooth, WiFi, Wireless Networks, etc.) must be turned off on all mobile computing devices, *unless* it is required. Only when required should the Wireless Detection be turned on for use. Once completed, the Wireless Detection should be immediately turned off.
7. Users must not load non-Agency software or proprietary non-Agency data onto an Agency owned computing device.

c. Servers

- i. The standard for general purpose Application servers, Database servers and File and Print Computing is IBM. Microsoft (MS) Windows 2003 and 2008 R2 64-bit Server (Standard and Enterprise) are the supported Operating Systems for these servers.
- ii. Fault Tolerant Application servers and Database servers is NEC FT. MS Windows 2003 and 2008 R2 64-bit servers are the supported Operating Systems for these servers.
- iii. Operating system settings and configuration will be performed by TSD to ensure compliance to appropriate security policies based on server roles, e.g., Web, Database, Fax, etc..
- iv. All servers and communication equipment must be located in access controlled/locked rooms (or secured with a cable and lock at the very least), in data cabinets with dual power, with the keyboard secured to prevent tampering and unauthorized use, with appropriate environmental cooling and monitoring oversight.
- v. TSD maintains a "chain of custody" process surrounding all hard drives. Currently, all removed hard drives are managed and stored off-site at a secure location. Required exceptions are in place with the Office of the Inspector General (OIG) and Public Safety (PSD).

d. Virtual Environment

- i. All ESX servers and associated storage components must be located in access controlled/locked rooms (preferably the Agency Data Center environments), in data cabinets with dual power, with the keyboard secured to prevent tampering and unauthorized use, and with appropriate environmental cooling.
- ii. All ESX server implementations must implement a management framework consistent with our PA ESX Administration Guide, which from time-to-time will be updated to reflect Standard Operating Procedures.
- iii. All ESX server implementations must provide "as built" documentation consistent with the framework established in our VMware Infrastructure Documentation For the Port Authority. This document must be kept current as changes to the environment are implemented.

- iv. All ESX server implementations (i.e., ESXi Operating System) must be patched on a regular basis using the management framework established in our PANYNJ ESX Patch Management document, which from time-to-time will be updated to reflect current patching procedures.
- v. All ESX-based Guest Virtual Machines must implement Operating System configurations and security settings, consistent with those identified in the Standards and Guidelines, System Administration and Windows Server Installation documents.
- vi. Access to ESX Operating System must be limited to System Administrators who have received ESX training and certification in the appropriate VMware components.
- vii. Storage Devices or Storage Area Network (SAN) should be configured based on ESX implementation purpose/application needs:
 - 1. Switch Zoning and/or Volume Partitioning – used to separate servers/storage based on the functionality and/or data criticality.
 - 2. SAN-to-SAN Replication – used to provide extra level of protection and high availability for mission critical data by block level replication between physical locations.

e. Portable Media

The risk of unauthorized disclosure of highly sensitive data is very high when such data is stored on individual-use electronic devices (e.g., flash drives, portable hard drives, DVDs, CDs, memory cards, etc.) and media, as these items are easily stolen or misplaced.

- i. Personal portable media devices are not allowed to connect to the Agency's corporate network or infrastructure, unless pre-approved by the Director of TSD.
- ii. It is important that portable devices offer strong protection, e.g., hardware encryption. Additionally, the encryption key must be protected with strong user authentication. *Please contact TSD to discuss protection measures if you identify a device/scenario meeting such criteria.*
- iii. The Agency strictly limits the circumstances under which highly sensitive data may be stored on these individual-use electronic devices and electronic media. It further mandates that strict security requirements be met when highly sensitive data must unavoidably be stored on individual-use electronic devices or electronic media. *Please refer to the Agency's Information Security Handbook (<http://eNet.panynj.gov/home/pdf/Corporate-Information-Security-Handbook.pdf>).*
- iv. User Responsibilities:
It is the responsibility of individuals to determine if they have sensitive data on their device(s) and/or media, and, if so, to ensure compliance with the following guidelines:
 - 1. The Director of the Department with which the individual is primarily affiliated must state, in writing, that such storage is an essential business need and must file the written statement and approval in a secure location for subsequent audit purposes. The Department Director must also ensure the individual has a signed Electronic Access Agreement on file with TSD.

2. Highly sensitive data must be securely encrypted on the individual-use electronic devices or electronic media according to encrypted methods recommended by TSD. Login password must be enabled for the individual-use electronic device, and if available, the electronic media. The password must meet or exceed appropriate complexity levels stated by the Agency. The password must not be shared with anyone.
 3. The data must be deleted from the individual-use electronic devices or electronic media as soon as it is no longer required, using secure methods according to the Agency's Information Security Handbook.
 4. Management of the individual-use electronic devices or electronic media may not be outsourced to any party external to the Agency without written approval from the Director responsible for the department with which the individual is primarily affiliated.
 5. All individual-use electronic devices and electronic media should be stored in a secure location or locked cabinet when not in use.
 6. Users must not load non-Agency software or proprietary non-Agency data onto an Agency owned computing device.
- f. **Centralized Data Backup**
 Approved standard software products are used to perform centralized and scheduled server backups, to be managed automatically, logged and stored remotely with encryption.
- i. The backup strategy for servers connected to the Port Authority network (PAWANET) reflects the intent to protect data, files and electronic records stored on these servers in the event of data loss or corruption.
 - ii. Media containing backed up data is stored off-site at a secure location, to be retrieved for disaster recovery purposes, if required.
- g. **Cyber Scrubbing**
- i. On a file-by-file basis, Cyber Scrubbing may be used to permanently delete Confidential Information only in accordance with the Port Authority's Records Retention Policy.
 - ii. Once contacted, TSD will utilize the CyberScrub suite of software to remove Confidential Information as requested.

3. Data Center

- i. Located in a gated campus that controls access via numerous layers of physical and electronic security devices.
- ii. Protected with fire safety system, leak detection system and is equipped with fully redundant backup systems for communications, power and cooling infrastructure.
- iii. Threat and risk assessment reviews and audits of security standards, operating procedures, and other protective measures are performed regularly to ensure we provide a secure, reliable and available centralized information systems environment to house the Agency's information and computing equipment.

4. PAWANET

The Port Authority has a modern distributed computing network, which is managed as an Enterprise resource. The network connects all individual computing devices, servers, printers and other devices in a unified computing infrastructure that makes it possible for the Port Authority to conduct its business. Please also reference the TSD Standards and Guidelines document, from the TSD eNet Home Page, for additional detailed information.

a. Network Devices

- i. All users accessing the Port Authority's network must authenticate to the Agency's Directory Services. Directory Services is a database containing descriptions of all network devices including servers, printers, shared devices and user accounts.
- ii. Access to network devices such as routers and switches is limited by the use of Access Control Lists (ACLs). Access to network routers and switches is authenticated by Cisco's TACACS (Terminal Access Controller Access Control System).
- iii. The SNMP V3 (Simple Network Management Protocol) Security Feature has been applied to all routers and switches to deny unauthorized access.
- iv. All router and switch configurations are updated regularly based on the Cisco Security Best Practice policy. This policy, as well as the PA Standard Configuration policy, is available upon request.
- v. Modems and wireless devices must be pre-approved by the Director of TSD and follow all security and encryption best practices referenced within and in the TSD Standards and Guidelines.
- vi. Penetration tests are conducted twice a year.
- vii. The Enterprise Network consists of the PAWANET and connected Local Area Networks (LANS). 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 secure limited access wiring closet. The Port Authority's Enterprise Network consists of the following components on the Port Authority side of demarcation:
 1. Enterprise Devices
 - a. Cabling (both copper and fiber optics)
 - b. Routers
 - c. Switches
 - d. Wireless Access Points (WAP)
 - e. Wireless Bridges
 - f. Fiber Optic SONET Nodes
 - g. Wiring Closets
 - h. Communications Equipment Racks
 - i. Server Racks
 - j. Servers
 - k. Storage Area Networks (SAN)
 - l. Network Printers
 - m. Video Encoders and Decoders

2. LAN Devices

- a. Workstations (Desktops and CADs)
- b. Laptops
- c. Local Printers
- d. Scanners
- e. Copiers
- f. PC Peripherals
- g. VOIP (Voice Over Internet Protocol) Telephones
- h. Voice Analog Gateways
- i. Cameras
- j. Security Card Access Devices

b. Firewalls and Intrusion Detection Appliances

- i. The Agency uses several layers of stateful inspection firewalls to control traffic between the PAWANET, Public and Private DMZs, directly connected vendors and the Internet. In addition to stateful inspection, the firewall technology offers application intelligence, which allows for deeper protocol-specific traffic inspection and protection against IP spoofing, Denial of Service (DoS) and other kinds of attacks. The access is controlled by policy sets, which limit the source, destination, port, protocol and in some cases, certain functionality of the protocol. The traffic that is not explicitly allowed is denied. Both allowed traffic and denied traffic are logged. The rule usage is reviewed on a periodic basis.
- ii. The Agency uses a multi-layered network-based Intrusion Detection (IDS/IPS) solution to protect the perimeter against intrusions. The updated attack signatures are automatically downloaded from the vendor's repository on an hourly basis and are automatically applied to the intrusion prevention system units. The IPS architecture allows for the centralized mining of the events across multiple IPS nodes and email-based alerts for high-priority events. Events are monitored and correlated on a regular basis. Correlation is also performed between the application protection policy of the firewall and the IDS layers of defense.
- iii. Host-based Intrusion Detection (HIDS) is installed and activated by TSD based on the purpose and physical location of the server. The technology protects the host against network attacks by examining incoming and outgoing traffic as well as the events on the host. The technology has the same log management and email alerting functionality as network-based intrusion detection. Events are monitored and correlated on a regular basis.
 1. Examples include:
 - a. Servers having a legal/regulatory obligation to ensure their security.
 - b. Servers housing information, that if disclosed, could pose a security threat.
 - c. Servers supporting a business process that must be available 24 x 7, such as physical access control.
 - d. Servers that are accessible to the outside world, firewalls, VLANs enforcing internal zone/domain separation.

- iv. All layers of perimeter security appliances offer several layers of intra-site and inter-site redundancy with automatic failover. The performed capacity planning and gathered experience over multiple years of maintenance guarantee seamless failover and adequate capacity of the remaining system to provide full functionality and no performance degradation in case of scheduled or ad-hoc failover.
- v. In the event of a security perimeter breach and/or the internal networks being compromised, the intrusions will be reported to the Office of the Corporate Information Security Officer and the Office of the Inspector General. We will retain the applicable logs from the perimeter security devices bearing the details of the perimeter breach.

c. Proxy Service

The proxy appliances and services offer extensive management, monitoring and reporting capabilities.

- i. The Agency has deployed multi-layered Web security appliances from one of the leading security vendors. The appliance performs the following tasks:
 - 1. Allows authenticated users to access Internet sites in accordance with the access policy
 - 2. Caches frequently used content
 - 3. Performs filtering of the malicious and inappropriate Web sites based on:
 - a. Site Database
 - b. Reputation Database
 - c. Proximity Vector
 - 4. Reputation Filters in place analyze more than 200 different web traffic and network-related parameters to accurately evaluate the trustworthiness of the course of the Web content.
 - 5. Performs deep application content inspection of the request and return traffic with several anti-virus and anti-malware engines. The solution employs sophisticated object parsing and streaming techniques as well as hardware optimization and acceleration to enforce security policies.
- ii. All device databases are being continuously and automatically updated with the new content via subscription service. The subscription service taps into the vendor's security event and signature database, which is updated by the 24/7 security team and cross-correlated with the events across the Internet. Such an approach allows for protection against the attacks that were initiated across the globe but have not yet spread to North America (including time-dependent outbreaks of viruses).
- iii. The proxy appliances provide hourly, daily, weekly and monthly statistics of the vital usage and performance parameters, which are stored on the appliances and periodically mailed to the members of the maintenance and management team. The technology also comes with the management application that allows for log consolidation and log mining on a separate server. The access logs are profiled on a regular basis and mined for specific usage per request of OIG and/or Public Safety representatives to assist with internal investigations.

d. Remote Access (Client-to-Site)

i. Infrastructure

1. The Port Authority corporate Remote Access System (RAS) provides authorized users with access to the Port Authority network resources and applications.
2. Access to a number of Port Authority public servers is protected either by a secure reverse proxy solution or by a managed VPN solution, each of which requires user authentication against Directory Services as well as masks the internal address space of the corporate network and the DMZ infrastructure.
3. The operating system of the Port Authority servers is hardened with all unneeded services being disabled.
4. Administrative access to the server is encrypted with SSL/TLS certificates.
5. All servers are monitored by a central monitoring server which generates E-Mail notifications when problems are discovered.
6. Server and application access logs are collected and processed on a regular basis.
7. Both the OS and the applications are patched with the most recent service packs and hot fixes on a scheduled basis. In the case of virtualized servers, the underlying host OS is also patched and secured.

ii. VPN Access

1. Remote access from external sources (such as a user's home) is achieved through an Internet-based managed VPN service.
2. It utilizes client software and proprietary hardware and software.
3. The servers are located at each of the Agency's secured Data Centers.
4. Requests for remote access are handled via the Request for Access to Information Systems (Form PA 3624A), which can be found online on ENet.

iii. Agency Application(s) Access

1. Single sign-on and remote authentication services to access internal web-based applications from the Internet have been established.
2. Identity-based Web security service and a two-form factor secure authentication device are required for authorized users to securely authenticate to the network over the Internet.

5. Virtual Private Network (VPN) (Site-to-Site)

Because the Internet is inherently insecure and provides no security mechanisms, dial-up access to the Internet is prohibited from any device that is attached to any part of the Agency's PAWANET Network. This includes accounts with third party Internet service providers. Users will not use the Agency's Internet accounts to establish connections to these third party services, unless authorized in advance to do so by the Agency's management and the security of the connection is reviewed and approved by the Director of TSD.

- i. The Director of TSD must approve all other connections from PAWANET to external networks, in advance. Connections will be allowed only with external networks that have been reviewed and found to have acceptable security controls and procedures, or where appropriate security measures have been implemented by the Agency to protect the Agency's resources. All connections to approved external networks will pass through an approved Agency firewall and intrusion detection sensor. Remote access to PAWANET and resources will be permitted provided that authorized users are authenticated, data is encrypted across the Internet and privileges are restricted.
- ii. External networks must adhere to the PA Standard Configuration policy, available upon request.
- iii. Audit trails and system logs for external connections will be reviewed weekly. The Network Manager will require the business managers to validate the need for all such connections on a quarterly basis. When notified and confirmed in writing, to both the business manager and the Director of TSD that the need for connection to a particular network is no longer required, all accounts and parameters related to the connection will be deleted within one working day.
- iv. Any connection between firewalls over public networks must use encrypted Virtual Private Networks (VPNs) to ensure the privacy and integrity of the data passing over the public network. All traffic emerging from the VPN tunnel should pass through the layers of firewall and IDS/IPS traffic inspection. The Director of TSD, prior to implementation, must approve all VPN connections. Appropriate means for distributing and maintaining encryption keys must be established prior to operational use of VPNs.

6. Internet Access

a. Outbound Traffic Requests

- i. The Agency encourages authorized employees to use the Internet for appropriate Agency business use. They offer valuable resources for employees and provide business value to the Agency. However, some web sites contain material whose content is clearly inappropriate for anyone using the Agency's resources. Therefore, access to inappropriate sites from Agency's computing devices is disabled. Such sites include: sexual content, violence, weapons, hacking, drugs, etc.
- ii. Misuse of Agency resources will not be tolerated. All Agency Employees and Non-Employees are responsible to follow the requirements outlined in Agency's Computing Resources Policy (<http://eNet/resources/ai/ai15403.pdf>). Examples of behavior that could result in disciplinary action include use for:
 1. Personal gain or profit
 2. Spoofing (representing yourself as someone else)
 3. Copying or posting the Agency's or third party's information without permission
 4. When it interferes with the operation of the Internet gateways
 5. Unauthorized attempts to break into any computing system whether the Agency's or another organization's
 6. Theft or unauthorized copying of electronic files
 7. Posting sensitive Agency information to unauthorized personnel
 8. Creating or forwarding chain letters
 9. Personal communication using "instant messaging" or similar technology
 10. Downloading or uploading malicious code
 11. Downloading or uploading inappropriate material for "sniffing" (i.e., monitoring network traffic); except if authorized as job responsibilities
- iii. Internet usage is monitored through use of proxy logs and reviewed with the Director of TSD on a monthly basis.
- iv. Outbound traffic is provided via both FTP (File Transfer Protocol) and SFTP (Secured File Transfer Protocol).

b. Inbound Traffic Requests

- i. Access to the PA-hosted Web sites in the DMZs is regulated by the firewall rules, which deny all traffic that is not explicitly allowed.
- ii. The access to the PA-hosted Web sites is further controlled by the several layers of IDS/IPS technology and by host-based intrusion detection running on the host (as described in Outbound Traffic Requests section).
- iii. High priority events generate E-Mail based alerts to the TSD perimeter security team.
- iv. Inbound traffic is allowed over SFTP (Secured File Transfer Protocol) from specific IP addresses. The data must be encrypted.

7. E-Mail

a. E-Mail Hosted Environment

- i. The Port Authority E-Mail environment is hosted by AT&T at a secured data center on dedicated servers. The data center is connected to the Port Authority network at our Network Operations Centers using two dedicated circuits. There are firewalls and other network equipment at each end of the circuits maintained separately by each party (AT&T and the Port Authority).
- ii. Both the Port Authority and AT&T employ network intrusion detection and other security controls.
- iii. Remote access to E-Mail is provided via a secure VPN system, through Outlook Web Access (OWA) access using Secure Socket Layers (SSL) with 128-bit encryption and via corporate mobile devices.

b. E-Mail Virus and Spam Protection and Content Scanning

- i. The E-Mail servers utilize anti-virus software. All anti-virus software signature files are automatically updated regularly. This software scans E-Mails and removes detected viruses entering and leaving the E-Mail environment.
- ii. The Port Authority uses additional anti-virus protection and anti-spam protection from a third party service provider which utilizes several industry-leading anti-virus engines, as well as proprietary software to identify and remove viruses from E-Mails and to quarantine E-Mails suspected of being spam.
- iii. E-Mail Quarantined Reports are provided to each user. The user can access a secure web site to safely access these quarantined E-Mails in order to delete or release as appropriate. E-Mail is quarantined for 14 days prior to automatic deletion.
- iv. Content filtering is used to identify potential spam E-Mail and when required, for handling certain forms of E-Mail related issues, e.g., E-Mail attacks, etc.
- v. Following industry best practices to mitigate risk, certain attachments in E-Mails are blocked.

8. Desktop Patch Management

- i. The Agency patching philosophy includes every security patch that can be applied to the Windows Operating System and the Microsoft Office suite of products.
- ii. On the second Tuesday of every month, Microsoft releases hot fixes/patches/security bulletins for private and publicly reported vulnerabilities identified in their operating system and office suite of products. The monthly patches are pushed to the primary patch management distribution server within the Agency. TSD reviews all patches with a severity rating of Critical or Important. In addition, TSD performs lab testing to ensure no adverse effect is experienced during the deployment of the security updates.
- iii. Once lab testing has been successfully completed, the monthly deployment is executed in three stages:
 1. Pre-Pilot Deployment
 2. Pilot Deployment
 3. Agency Deployment
- iv. A feature of our patch management system is the “mandatory baseline” that will deploy the patches to any computer that is recently added to PAWANET as new or re-imaged.

9. Server Patch Management

- i. The Agency patching philosophy includes every security patch that can be applied to the Windows Operating products.
- ii. On the second Tuesday of every month, Microsoft releases hot fixes/patches/security bulletins for private and publicly reported vulnerabilities identified in their operating system and office suite of products. The monthly patches are pushed to the primary patch management distribution server within the Agency. TSD reviews all patches with a severity rating of Critical or Important.
- iii. All servers deployed within the Agency must be patched on a regular basis using the management framework established in our Standard Operating Procedure For Applying Desktop and Server Patches Within the Port Authority Enterprise document, which from time-to-time will be updated to reflect current patching procedures.
- iv. All servers deployed within the Agency must have the appropriate patches tested prior to deployment into a production setting.
- v. All servers patched within the Agency must have a ‘Change Control’ log entry documented and a ‘Maintenance Window’ identified.

10. Content Management

- i. The Port Authority's Content Systems (a.k.a., PACS) provides a highly scalable and secure platform for the storage and management of electronic documents, collaboration and automated workflow for varying business applications across

the Agency. The PACS platform consists of a series of best-in-breed applications that when combined manage documents, drawings, forms, photos, video and architectural models. The PACS provides the following services:

1. Storage and Archival
 2. Permissions and Privileges
 3. Client-less Viewing
 4. Full Text Search
 5. Forms and Data Collection
 6. Digital Visual Rights Management
 7. Workflow
 8. Collaboration Services
- ii. PACS is the primary method for sharing in-process and milestone documents with partners, consultants, contractors and other Agencies via external Internet-based access. The PACS repositories are layered with the protections best suited for the information managed, as follows:
1. Proposed users of the system must request access via a uniform process that requires both business unit and TSD approval and coordination.
 2. Access is linked directly to the PAWANET based authentication protocols and policies.
 3. Users external to the Authority must sign NDA's and operate within contract requirements pledging compliance with PANYNJ information handling procedures.
 4. Both external and internal users may undergo background checks prior to being granted access to PACS repositories or content. *Please refer to the Agency's Information Security Handbook (<http://eNet.panynj.gov/home/pdf/Corporate-Information-Security-Handbook.pdf>).*
 5. User based activity, for both common users and administrators, are captured in a detailed and unalterable Audit Trail that is accessible by authorized individuals via the standard user interface.
 6. PACS repositories may be physically isolated from one another due to specific business needs or enhanced security requirements.
 7. Separate internal and external authentication schemes are maintained and monitored for security and reliability providing additional controls for external clients.
 8. All PACS servers are located in PANYNJ Data Centers that provide for fault tolerance, physical and environment security systems.

9. Utilizes Agency's standard virus protection to ensure that documents passed into the PACS and maintained in the repository are scanned at multiple points in the information life-cycle.
10. Internet-based access is controlled by additional layers of authentication managed via reverse proxy and remote access protocols (further described within these Guidelines).
11. Multiple firewalls allow for specific access across approved ports between each of the application servers and in-line authentication devices (further described within these Guidelines).
12. Application servers are physically separate from Database servers and have no direct communication to external connections.
13. Dual form factor authentication is utilized for external access.
14. Database, Document Store and Index encryption technologies are utilized for parts of the PACS.
15. Intruder detection systems are employed to detect unauthorized access internally or externally to PACS application servers.
16. Server hardening and testing protocols are reviewed for each new piece of hardware introduced into the environment and periodically throughout its life.
17. PACS operates within the Agency's Change Management and Patch Management programs and policies.

ATTACHMENT H

PART III Computing Resources Policy

Office of the Executive Director

Revised: April 6, 2012

COMPUTING RESOURCES

I. Introduction

- A. Computing resources provide the Port Authority with significant benefits in productivity and efficiency. The provision of computing resources is intended and designed to facilitate the official business of the Port Authority. Port Authority rules and regulations that govern the responsibilities of employees apply to employee use of computing resources. This Instruction is intended to clarify and ensure that computing resources are used in a professionally responsible manner and appropriate steps are taken to safeguard the confidentiality, integrity and availability of business systems, data and equipment.
- B. For purposes of this Administrative Instruction, computing resources include, but are not limited to, personal computers, software, peripherals, data storage and devices, personal digital assistants, local and wide area network components, Port Authority provided connections, E-mail, internet access, laptops, terminals, remote access and any other means of automated information exchange or data access.

II. Instruction

- A. Computing resources provided to employees and other authorized persons are Port Authority property and intended for Port Authority business. Computing resources are not to be used for personal gain or in support of any purposes not related to Port Authority business. Because the use of computing resources is both extensive and an efficient and convenient method of communication and data processing, it is understood that there may be incidental personal and non-commercial use of these resources. Such incidental use is subject to this Instruction, and authorized users are expected to use prudent judgment to ensure that all computing resources are used for the intended purpose of Port Authority business.
- B. When necessary for official or business purposes, the Port Authority reserves the right to monitor and/or log all computing activity. Requests for monitoring will be made to and authorized by the Executive Director in writing and only then for limited justified and reasonable cases. Further,

the Port Authority reserves the right to inspect computer resources to ensure that actual use is consistent with this Instruction. The Port Authority may use data, logs, diaries, and archives in accordance with its normal business practices and instructions (including compliance with requests from appropriate legal and regulatory authorities and agencies) and for adherence with this Instruction.

1. The Port Authority, through supervisors or other management employees authorized in writing by the Executive Director only, may access or monitor a user's assigned computing resources with justifiable reason.
 2. The Port Authority may inventory and inspect all data storage devices and other computing resources for the sole purpose of ensuring their continued proper maintenance and operation.
- C. Depending upon content, data stored within computing resources may constitute records of the Port Authority and the organizational data retention schedules (Record Retention Manual) and instructions on access to such data (the Freedom of Information Policy) are applicable. However, users should be aware of the limited retention period for e-mail messages described in Par. IV of the Instruction.
- D. Directors are responsible for implementation of this Instruction within their departments.

III. Procedures

A. Passwords

1. Users should be aware that the existence of individual confidential passwords does not suggest that computing resources may be used for personal confidential purposes, or that any data or information is the property of the individual user or is personally confidential.
2. Employees are responsible for maintaining the confidentiality of passwords and may be held accountable for use of computing resources in their name accessed with their password.
3. Passwords should be difficult to guess and changed at least once every 90 days or in accordance with information system standards.

B. Usage Requirements

1. Authorized users of Port Authority computing resources, when communicating with others, are required to:

- a. Identify themselves honestly, accurately and completely.
 - b. Maintain a professional demeanor.
 - c. Protect Port Authority data from unauthorized use or disclosure.
2. At all times, authorized users must respect the legal protection provided to programs and data by copyright and license.

C. Prohibited Uses

1. Authorized users of Port Authority computing resources may not utilize them:
 - a. For transmitting, retrieving, creating, viewing, displaying or storing any pornographic, harassing, threatening, abusive, defamatory, obscene, or sexually explicit materials or materials which contain ethnic slurs or racial epithets, or which generally disparage others based on race, national origin, sex, sexual orientation, gender identification, age, disability, religious beliefs, or political affiliation, or which contain other unlawful material.
 - b. To transmit confidential, proprietary or business sensitive information.
 - c. To interfere with or disrupt network users, services or equipment either within the Port Authority or on the Internet.
 - d. To access other computing resources without authorization or attempt to circumvent authorization procedures or controls.
 - e. For private purposes such as marketing or business transactions.
 - f. For religious, political or outside business purposes.
 - g. For unauthorized not-for-profit business activities.
 - h. For advertising of products or services.
 - i. For personal gain.
 - j. To obtain or utilize unauthorized entertainment software, music or games.
 - k. To permit access by unauthorized users.

- l. To send material in violation of the copyright.
 - m. For solicitation of funds.
 - n. For employee organization business.
- 2. Electronic mail practices such as “spamming” (unauthorized mass mailings to Port Authority employees or external recipients or postings to bulletin boards), hostile communications, “chain letters”, “spoofing” (taking the identity of another person for the purpose of concealing one’s own identity), or knowingly transmitting software containing harmful components such as a virus, are prohibited.
- 3. Allegations of misuse of computing resources may be made to supervisors or managers, consistent with existing Port Authority instructions applicable to misuse of property or improprieties or inappropriate or illegal behavior in the workplace.

IV. Retention of Electronically Stored Data

- A. E-mail messages are generally of short-term import and should be discarded routinely. E-mail is automatically deleted from a user’s mailbox and backup storage 120 days from the date of receipt or creation, without notice.
 - 1. Depending on the content of the message and/or its attachments, it may be desirable to retain the information for longer periods. Such messages or attachments should be stored on local or server drives as necessary.
 - 2. As suggested in Par.II.C., depending on the content of the message and/or its attachments, care and consideration should be given as to which documents should be retained based on the appropriate record retention schedules.
- B. Users should take appropriate steps to ensure that important Port Authority data other than e-mail is backed up in case of equipment failure. This includes data stored on Port Authority computing resources in the office and, where authorized, at home. Data stored on shared devices which are part of the Port Authority’s enterprise wide network system are backed up and retained for a period of time in accordance with standards issued by the Port Authority.
- C. Users should also be aware that deletion of an e-mail message or attachments or other data may not automatically delete the message from

electronic storage devices. The data may continue to reside in the user's local or network drives, or may be stored in backups of the system.

V. Applicability to Employees and Other Users

A. This Computing Resources Instruction applies to all employees, volunteers, contractors, supplemental staff, consultants, and other individuals who are provided access to any or all Port Authority computing resources.

B. Employees

1. Employees of the Port Authority (or its subsidiaries) whose employment is terminated or suspended have no right to access any Port Authority computing resource, including Internet access and e-mail accounts and content.
2. The misuse of computing resources privileges may subject the employee to disciplinary action in accordance with Port Authority rules, and/or other applicable rules or laws, and may be grounds for loss of such privileges, dismissal from employment, or other administrative action. In addition, violations of this Computing Resources Instruction or other misuse of computing resources may be referred for criminal prosecution.

C. Non-employees

1. Third parties (i.e., individuals who are not employees of the Port Authority or its subsidiaries) should only be provided access to Port Authority computing resources as necessary for the business purposes of the Port Authority and only if they comply with all applicable rules.
2. Non-employees who are in violation of the provisions of this Computing Resources Instruction will be removed from access to all Port Authority computing resources. In addition, other legal remedies, civil (including contract revocation) or criminal, may be pursued.

DISCLAIMER

Although issued in revised format, the information contained in these Administrative Instructions (AIs) reflects the content of previously issued Administrative Policy Statements (APs) and, in certain limited instances, Port Authority Instructions (PAIs). The rules set forth in these AIs will remain in effect until changing conditions require their revision. This body of instructions is not intended to be exhaustive with respect to all the responsibilities of employees and it does not constitute a contract. These AIs will be updated from time to time to reflect changes or additions as appropriate, at the direction of the Executive Director.

ATTACHMENT H

PART IV Cloud Computing Framework

THE PORT AUTHORITY OF NEW YORK & NEW JERSEY

Cloud Computing Framework

Technology Department

Updated:

2/3/2016

Version:

1.2

THE PORT AUTHORITY OF NY&NJ

The Agency's Cloud Framework consists of components and/or controls that must be addressed when selecting a Public Cloud service or Software as a Service (SaaS) vendor. The elements in this framework are dynamic and will evolve over time to ensure a secure and robust Cloud Computing environment for the Agency's business

Intentionally Left Blank

REVISION HISTORY

Version	REVISION DATE	REVISION DESCRIPTION	REVISION TRACKING NOTES
1.0	12/14/2015	Baseline Draft Version	
1.1	12/17/2015	Reformatting Document	Added Document Template
1.1.1	12/17/2015	Incorporated Department Comments	Included new Password Policy Language
1.2	02/03/2016	Incorporated Audit Document Revised Checklist (1/26/2016)	Modified Cover page

The Agency's Cloud Framework consists of components and/or controls that must be addressed when selecting a Public Cloud service or Software as a Service (SaaS) vendor. The elements in this framework are dynamic and will evolve over time to ensure a secure and robust Cloud Computing environment for the Agency's business. The Framework elements consist of the following components and/or controls:

1. Cloud Offering:

- a. Government Cloud Service offering instead of Commercial Cloud.

2. The Agency Cloud Framework:

The Framework is meant to ensure that all physical, logical and information assets are secure and that security and privacy are maintained using de-facto best practices aligned with Federal Information Processing Standards (FIPS) as well as NIST Publications. To that end, Cloud Solutions should be compliant with the latest versions of the following best practices (as appropriate for application risk), to name a few:

- a. NIST 800-144: Guidelines on Security and Privacy in Public Cloud Computing
- b. FIPS 199: Standards for Security Categorization of Federal Information and Information System
- c. FIPS 200: Minimum Security Requirements for Federal Information and Information Systems
- d. NIST 800-53: Recommended Security Controls for Federal Information Systems and Organizations
- e. NIST 800-146: Cloud Computing Synopsis and Recommendations
- f. Cloud Security Alliance: Cloud Controls Matrix Version 3.0 (CCMv3)

3. For Software-as-a-Service (SaaS), excerpt from NIST 800-146:

- a. **Data Protection.** Analyze the SaaS provider's data protection mechanisms, data location configuration and database organization/transaction processing technologies, and assess whether they will meet the confidentiality, compliance, integrity and availability needs of the Agency.
- b. **Client Device/Application Protection.** Consistent with the FIPS 199 impact level of the data being processed, protect the Agency's client device (e.g., a computer running a Web browser) so as to control the exposure to attacks.
- c. **Encryption.** Require that strong encryption using a robust algorithm with keys of required strength be used for Web sessions whenever the subscribed SaaS application requires the confidentiality of application interaction and data transfers. Also require that the same diligence be applied to stored data. Federal agencies must employ government-approved cryptographic algorithms for encryption and digital signature, and the implementations need to be FIPS 140-2 validated. Understand how cryptographic keys are managed and who has access to them. Ensure that cryptographic keys are adequately protected.
- d. **Secure Data Deletion.** Require that cloud/vendor providers offer a mechanism for reliably deleting data at the Agency's request.

4. Data Location:

- a. Must be US-based, in multiple locations for redundancy and administered by US Citizens.

5. Electronic Discovery:

- a. A cloud/vendors information archival capabilities must preserve the original metadata of 'client data' so as to not adversely affect the Agency's litigation risk

6. Data Ownership:

The Agency retains exclusive ownership over all its data:

- a. That the cloud/vendor provider acquires no rights or licenses to that data, including intellectual property rights or licenses.
- b. The cloud/vendor may not use the Agency's data for its own purposes;
- c. and that the cloud/vendor does not acquire and may not claim any interest in the data due to security.

7. Availability:

- a. Must meet 99.9% uptime

8. Physical Security:

- a. 24-hour monitoring of data centers.
- b. Multi-factor authentication, including biometric scanning for data center access.

- c. Internal data center network is segregated from the external network.
- d. Role separation renders location of specific customer data unintelligible to the personnel that have physical access.
- e. Faulty drives and hardware are demagnetized and destroyed.

9. Logical Security:

- a. Lock box processes for strictly supervised escalation process greatly limits human access to your data.
- b. Servers run only processes on whitelist, minimizing risk from malicious code.
- c. Dedicated threat management teams proactively anticipate, prevent, and mitigate malicious access.
- d. Port scanning, perimeter vulnerability scanning, and intrusion detection prevent or detect any malicious access.

10. Data Security:

- a. Encryption at rest protects the Agency's data on cloud/vendor servers.
- b. Encryption in transit with SSL/TLS protects Agency's data transmitted between the Agency and cloud/vendor application.
- c. Threat management, security monitoring, and file/data integrity prevents or detects any tampering of data.

11. Compliance Standards:

- a. **Health Insurance Portability and Accountability Act (HIPAA)**: HIPAA imposes, under law, certain requirements for security, privacy, and reporting regarding the processing of electronic protected health information.
- b. **Federal Information Security Management Act (FISMA)**: requires U.S. federal agencies to develop, document, and implement controls to secure their information and information systems. Federal Risk and Authorization Program (FedRAMP) is a federal risk management program that provides a standardized approach for assessing and monitoring the security of cloud products and services.
- c. **ISD 27001 Certification**: Along with NIST 800-53, ISO 27001 is one of the best security benchmarks available. Cloud/vendor should comply with the set of physical, logical, process and management controls defined by ISO 27001:2013, inclusive of ISO 27018 Privacy controls.
- d. **European Union (EU) Model Clauses**: The EU Data Protection Directive, a key instrument of EU privacy and human rights law. The EU model clauses are recognized as a preferred method for legitimizing the transfer of personal data outside the EU for cloud computing environments. Supporting the EU model clauses involves investing and building the operational controls and processes required to meet the exacting requirements of the EU model clauses. Unless a cloud/vendor service provider is willing to agree to the EU model clauses, the Agency might lack confidence that it can comply with the EU Data Protection Directive's requirements for the transfer of personal data from the EU to jurisdictions that do not provide "adequate protection" for personal data.
- e. **U.S.-EU Safe Harbor framework**: The U.S.-EU Safe Harbor framework also enables the Agency, as needed, to legally transfer personal data outside of the EU under the EU Data Protection Directive.
- f. **Statement on Standards for Attestation Engagements No. 16 (SSAE 16)**: Cloud/vendor has been audited by independent third parties and can provide SSAE16 SOC 1 Type I and Type II and SOC 2 Type II reports on how the service implements controls.
- g. **Canadian Personal Information Protection and Electronic Documents Act (PIPEDA)**: The Canadian Personal Information Protection and Electronic Documents Act pertains to how private sector organizations collect, use, and disclose personal information in the course of commercial business.
- h. **Gramm-Leach-Bliley Act (GLBA)**: The Gramm-Leach-Bliley Act requires financial institutions to put processes in place to protect their clients' nonpublic personal information. GLBA enforces policies to protect information from foreseeable threats in security and data integrity.

12. Audit Control Requirements¹:

a. General:

1. Documented procedures, flowcharts and process maps for the application.
2. Conduct regular audits, vulnerability testing, and security scanners.
3. SSAE 16 SOC 2 Type II (previously known as SAS 70 Level 2)
4. Federal Risk and Authorization Management Program (FedRAMP) Certification
5. ISO27001 Certification
6. Criminal Justice Information Services (CJIS) security policies and procedures compliant for law enforcement information and systems.
7. Background check should be performed on all personnel.

b. System/Security Administration

1. Administrative personnel should receive training.
2. Administrative staff should receive general security awareness training before access is provided. All security training must be reinforced at least every three years and must be tracked as per the PA Information Security Handbook.
3. System and security administration procedures should be documented and distributed.
4. Administrator(s) roles and responsibilities should be documented.
5. Developers and/or programmers should not have access to the production server.
6. Operating system administrators should not have access to the production database and application.

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

1. Disable and/or remove unnecessary ports/services.
2. Remove all manufacturer samples from the production system. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.
3. Default, public, and guest accounts should be secured/locked/removed.
4. Change all default passwords; delete all default content and login scripts.
5. Limit administrative and user account privilege and access.
6. Document system accounts like administrator, root, oracle, and sys.
7. Document user/group access rights
 - a. Users/groups should be setup with least access required to perform job responsibilities.
8. Implement access control at the database level (i.e. user roles and permissions, passwords, secure links)
9. Use secure encrypted remote access methods.
10. If the application is a web application, log (and monitor) web traffic and trend the activity looking for abnormal activity.
11. Ensure that appropriate security and vulnerability assessment tools are running.
12. At login, last user login should not display.
13. Inventory listing of hardware and software should be current and maintained.

d. License Management:

1. Ensure that application licensing requirements are documented, reviewed and maintained.
2. 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.

e. Logical Access Controls:

1. All users are required to read the Agency Policy Computing Resource Administrative Instruction (AI 15-4.03) and sign an acknowledgement of the Agency IT Acceptable Use Code of Conduct policy prior to account activation.
2. Procedures to grant/modify/delete access should be documented.
 - a. Access request forms for adding/modifying/deleting users should be used.
 - b. Account expiration for contractors and consultants.
 - c. Accounts adequately identify the user – no generic accounts

¹ Audit Department 1/26/2016 Update, with TEC Department modifications to password policies

3. Ensure that security administrator procedures exist to:
 - a. Create/remove application access in a timely manner
 - b. Review user roles/permissions
4. Validate that all users have accessed the application within the past 90 days.
 - a. Review dormant accounts
 - b. Inactive accounts should be removed.
5. Each user has a unique user ID as described in the Port Authority Standard and Guidelines.
 - a. All user accounts profile should include Employee ID# and full user name.
6. Roles are setup with least access required to perform job responsibilities.
7. Roles should have a segregation of duties/roles.
8. All accounts must have an individual or business group assigned to be responsible for account management.
9. Segregation of duties and areas of responsibility must be implemented where appropriate.
10. Whenever segregation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision. The PA must approve these compensating controls.
11. Review of audit trails and system approvals must be performed independent and retained to document the implementation of these security controls
12. Access Control List (ACL) should include:
 - a. Current list of ACL
 - b. Creation and updates to ACL
 - c. Testing and approvals of ACL
13. The application should have the PA's warning banner on the login screen. The application has a warning banner, terms of use, and/or privacy statement that was approved by the Port Authority on the login screen.
14. The system should have an access role that would allow real only access to all application, database and operating system screens, functions, logs and reports.
15. Remote access should be approved, secured, and documented in accordance with PA policy. Remote access, at a minimum, must consist of multifactor authentication mechanisms, secured communications (TLS/ VPN encryption methodology), access control mechanisms and logging of user activity.

f. Password Controls: (see Section 14. Port Authority Password Policies and Requirements)

g. Application Controls:

1. Data Validation & Input Controls
 - a. The application should have input controls to verify the validity of the data entered.
2. Data Retention and Management
 - a. All data should be classified according to its sensitivity (confidential, etc) and protected accordingly.
 - b. Data archive strategy should be documented and in place.
 - i. Should specify how long active data is kept.
4. Data integrity and Security
 - a. Sensitive data, such as credit card #s and social security #s, should be encrypted.
 - b. Data should be restricted and audit trails should be available to identify all user activity include view access to sensitive data.
 - c. Data should be stored in the database encrypted and blocked from user views in the application unless it is authorized.
 - d. Encryptions level at a minimum should be AES 256bit when encryption is used.
5. Application Interfaces:
 - a. Interface file should be secured and archived.
 - b. Reconciliation of data should be done on a batch record and totals. Detail data reconciliations should be completed on periodic basis.

6. Processing Controls:

- a. Application databases/interfaces should have the necessary controls to prevent processing of inaccurate, duplicate, or unauthorized transactions and producing inaccurate outputs.
- b. Controls to ensure that all data is processed and accounted for should be in place.
- c. Rejected items should be logged, tracked and resolved in a timely manner.

h. Change Management:

1. Processes and tools should be used to report, track, approve, fix, and monitor changes on the application.
2. The application and all changes to the application should be tested before being put into production.
 - a. Documentation of approval for change and evidence of testing should be in place.
 - b. Specific timetable/schedule should be documented.
3. Emergency procedures should be documented and distributed.
4. Separate environments are required for development, test, quality assurance, production.
5. Procedures should require that no changes be made directly in the production environment without going through the development/test/quality assurance environments.
6. Formal change control procedures for all systems must be developed, implemented and enforced.
7. Where technically feasible, development software and tools must not be maintained on production systems.
8. Source code for application or software must not be stored on the production system running that application or software.
9. Privileged access to production systems by development staff must be restricted.

i. Application Logging, Audit Trails and Record Retention:

1. Audit trails for operating, application, and database systems should exist and reviewed.
2. Users and roles should be tracked and reviewed
 - a. Maintain documentation
3. All failed logon attempts should be logged.
4. All sensitive transactions and changes should be logged and an audit trail created.
5. Audit trails should contain who made the change, when it was made, and what was changed.
6. Only the security administrator should have access to change or delete these logs or audit trails.
7. Audit trails should be reviewed by the business owner(s) and security administrator.
8. Management reporting should be produced through the application.
9. Access reports by user and privilege should be produced and reviewed periodically including access violation reports and exception transaction reporting.

j. Contingency Planning, Disaster Recovery and Backup Management:

1. A business contingency plan and a disaster recovery plan for the application should be documented and stored off-site, including escalation plan and current call tree.
2. Plans should be tested and the outcomes of the tests (success/failure) should be documented.
3. Regular backups of the application and the application data should be stored off-site.
4. Application executables should be stored off-site or in escrow.
5. Application configurations should be documented and backed-up.
6. Full system backup should be encrypted.
7. Backup procedures should be documented.
8. Tape maintenance should include:
 - a. Periodically testing integrity of tape
 - b. Procedures for tape destruction due to faulty or scratched hardware.

k. Performance Monitoring:

1. Incident monitoring procedures should be documented and incidents logs should be reviewed to ensure that appropriate action is taken.
2. Performance statistics should be examined and reviewed periodically by system administrators/business owner(s).

3. If vendor(s) support the application, a service level agreement for uptime, performance monitoring, updates, etc should be confirmed.
4. Baseline tools or security products should be used and checked on a quarterly basis.

l. Patch Management:

1. Patch management procedures and documentation
 - a. Procedures should include testing, approvals, and distribution.
 - b. Documentation should include emergency procedures.
2. Apply all new patches and fixes to operating system and application software for security.
3. All security patches must be reviewed, evaluated and appropriately applied in a timely manner. This process must be automated, where technically possible.

m. Physical Protection:

1. Physical access to the application hardware should be appropriately restricted.
 - a. Physical access secured by single authentication mechanism i.e. swipe card.
 - b. Physical security adequate for equipment (locked cabinets)
2. Appropriate fire suppression systems should be in place.
3. Environmental condition adequately controlled (no water, dirt, clutter) and monitored.
 - a. Temperature and humidity monitoring should be implemented.
4. Security cameras installed in sensitive areas
5. Power surge protection and emergency power backup are in place.
6. All hardware and software assets must be inventoried.
7. Visitors including maintenance personnel, to data center, server and network equipment storage facilities must be escorted at all times.

n. Anti-virus Management / Integrity / Vulnerability Software Management:

1. Virus patch management procedures must be documented, including emergency update procedures.
2. Anti-virus and software integrity checkers must be implemented to prevent and detect the introduction of malicious code or other threats.
3. Virus software engines and definitions must be implemented and up-to-date.
4. A remote distribution server should be implemented for virus software updates and documentation on remote distribution should be current and maintained.
5. Intrusion detection system must be in place,
6. All systems must have vulnerability scans performed before going into production and periodically thereafter. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities.
7. Host-based intrusion detection/ firewalls software must be installed and enabled on all systems to protect from threats and to restrict access. Incident response procedures must be in place to address any alerts identified and system owner should be notified of alerts and what action was taken to mitigate the issues.
8. Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic network locations to monitor inbound, outbound and internal network traffic.
9. Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.
10. Procedures must be established to maintain information security during an adverse event.
11. Firewalls should be implemented.
12. Firewall rules documentation should be up-to-date.
13. Network management connections must be performed from a secure, dedicated network.
14. Network authentication is required for all devices connecting internal networks.

o. Wireless Device:

1. Devices should be using WPA/WPA2 and AES encryption or better.
2. Devices should disallow broadcasting of the SSID.
3. All default parameters should be changed.
4. Devices should have MAC address filtering enable or some type of authentication mechanism in place.

p. Web Application Vulnerabilities and Controls:

1. Best Practice and Standards:
 - a. The Open Web Application Security Project (OWASP) - www.owasp.org
 - b. www.webappsec.org (a consortium of web application security professionals)
 - c. Center for Internet Security (CIS) – www.cisecurity.org
2. Perform data validation & integrity checks for field values and ensure the HTML special characters are stripped for all HTML request.
3. Do not allow site pages to be cached by user browsers.
4. All sensitive, personal or confidential data (including SSN, passwords, session IDs for sensitive applications, confidential or sensitive business transactions, etc.) should be transmitted between browser and server within an SSL-encrypted session (or other encrypted transmission) and are encrypted in the database at rest.
5. All sensitive and personal data should be masked and encrypted where possible.
6. Legal Issues:
 - a. The site should have a privacy statement and term of usage.
 - b. American Disability Act – Section 508 should be considered during the development process due to the requirement that federal agencies' electronic and information technology is accessible to people with disabilities.
7. Web Authentication: To prevent passwords from being passed in the clear, have authentication occur within an TLS encrypted tunnel. Use TLS (certificate) to protect the password.
8. Password Reset:
 - a. For internal applications, reset passwords via the helpdesk or security administrator of the site
 - b. For external applications, send temporary password to known e-mail address, that must be changed upon login and/or
 - c. Have customer service reset after the user has been validated.
 - d. If possible, use two factor authentication like Secure ID fobs.

q. Credit Card Processing Checklist:

1. If credit cards are accepted, PCI Standards (PCI DSS v3.1) should be followed and the process should be PCI compliant. Ensure all vendors and consultants are required to be PCI compliant. Attachment - The payment card application should be PCI compliant (PA-DSS v3.1).
2. A segregated network and/or an approved Point of Sale terminal should be in place for the system or terminal used to process credit card transactions.
3. The credit card processor standard and requirements should be followed, i.e. maintain transaction data for two years.
4. Maintain the security of the customer information, including not storing credit numbers, the cardholder CVC/CVV numbers or any of the data from the magnetic strip on the credit card.
5. Maintain the transaction data for contesting chargebacks, ensure that the processor fees are appropriate and do reconciliations of the transactions processed and the money deposited in the Port Authority bank accounts.
6. The appropriate Port Authority functional areas should be made aware credit card processing activity and should be involved applying for the Merchant ID for MasterCard/Visa, Discover and American Express.
7. Create a privacy policy and procedure for staff and consultants.
8. Perform quarterly vulnerability scans of the network that contains the credit card processing, annual PCI reviews according to the PCI DSS, and annual system penetration testing.
9. Perform the appropriate annual assessment and provide a report on compliance (ROC) which state shows compliance.

r. Credit Card Processing Checklist:

1. The Disaster Recovery plan should include at a minimum the following areas.
 - a. Business Impact Analysis
 - b. Critical Time Frame
 - c. Application System Impact Statements

- d. Recovery Strategy & Approach
 - e. Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems.
 - f. Disaster Definition
 - g. Detailed Recovery Steps for each Disaster Definition
 - h. Escalation Plans and Decision Points
 - i. System Components- An inventory of the criticality of systems (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment).
 - j. Disaster Recovery Emergency Procedures
 - k. Plan Procedure Checklist
 - l. Disaster Recovery Team Organization
 - i. Salvage Team & Team Responsibilities
 - ii. Disaster Recovery Responsibilities
 - iii. Essential Position – Require back-up personnel to be assigned.
 - m. Contacts information Disaster Recovery Team and critical vendors - this area should be reviewed semi-annually for updates and changes.
 - n. Post-Disaster – Detail what steps need to be taken to move from disaster mode back to normal operations.
2. Contingency plans (e.g., business continuity plans, disaster recovery plans, and continuity of operations plans) must be established and tested regularly.
 3. Backup copies of procedures, software, and system images should be taken regularly and moved offsite.
 4. Backups and restoration must be tested regularly.

13. Criminal Justice Information Services (CJIS) Compliance (as appropriate).

14. Port Authority (PA) Password Policies and Requirements:

These requirements applies to all PA information technology systems regardless of whether they are administered by (or on behalf of) the PA.

1. End user accounts will be disabled (not deleted) after 60 days of non-use;
2. All information technology system account passwords will be complex:
 - a. a minimum of 10 characters in length
 - b. contain at least two upper and lowercase alphabetic characters,
 - c. contain at least one number (0-9)
 - d. contain at least one special character (e.g. - +) : > _ ? & \$ % #)²
 - e. Smartphones, where capable, shall leverage biometric access to provide the most security for the least inconvenience.
3. User passwords will require a change every 90 days.
4. All accounts will be granted the minimum level of access and permissions necessary to perform an assignment.
5. If a system account fails to satisfy the requirements of this policy, an administrator may place the account in “disabled” status until remedied.
6. Changes to an account’s access privileges require the appropriate managers to request new or modified access.
7. All users are required to read the Agency Computing Resource Administrative Instruction and sign an acknowledgement of the Agency IT Acceptable Use Code of Conduct policy prior to account activation.
8. Annually, all managers are required to certify that only authorized employees have accounts on Agency systems. Technology and the Office of the CSO will work with managers to provide them with the lists of employees and their accounts.

² Example: W0nD3rFull

9. Passwords must not be shared.
10. Accounts should be locked after a three logon failures.
11. Passwords should not be the same account name.
12. No concurrent login capabilities.
13. Password file should be securely stored with limited access and encrypted.
14. Application forces initial passwords to be changed and the initial passwords should not be easily guessable.
15. Set "automatic session timeout" to 15 minutes of inactivity and require user to log back in with valid ID and password.

Purpose of the following items:

- (1) so we don't create 'islands' of users without a centralized mechanism to manage accounts and
- (2) protecting our *information* assets, regardless of where it may reside (in cloud, on premises, etc..)

15. Integration with the Agency's Active Directory platform for centralized account/application user management

16. Integration with the Agency's Information Rights Management Framework which will leverage Microsoft Azure Rights Management Services

ATTACHMENT H

PART V Audit Department Controls Requirement Contract Checklist

Audit Department Controls Requirement Contract Checklist

General

- Documented procedures, flowcharts and process maps for the application.
- Conduct regular audits, vulnerability testing, and security scanners.
- SSAE 16 SOC 2 (previously known as SAS 70 Level 2)
- Federal Risk and Authorization Management Program (FedRAMP) Certification
- ISO27001 Certification
- Criminal Justice Information Services security policies and procedures (CJIS) compliant for law enforcement information and systems.
- Background check should be performed on all personnel.

System/Security Administration

- Administrative personnel should receive training.
- Administrative staff should receive general security awareness training before access is provided. All security training must be reinforced at least every three years and must be tracked as per the PA Information Security Handbook.
- System and security administration procedures should be documented and distributed.
- Administrator(s) roles and responsibilities should be documented.
- Developers and/or programmers should not have access to the production server.
- Operating system administrators should not have access to the production database and application.

Hardening of operating system/database that supports the application:

- Disable and/or remove unnecessary ports/services.
- Remove all manufacturer samples from the production system. Scripts must be removed from production systems, except those required for the operation and maintenance of the system.
- Default, public, and guest accounts should be secured/locked/removed.
- Change all default passwords; delete all default content and login scripts.
- Limit administrative and user account privilege and access.
- Document system accounts like administrator, root, oracle, and sys.
- Document user/group access rights
 - Users/groups should be setup with least access required to perform job responsibilities.
- Implement access control at the database level (i.e. user roles and permissions, passwords, secure links)
- Use secure encrypted remote access methods.
- If the application is a web application, log (and monitor) web traffic and trend the activity looking for abnormal activity.
- Ensure that appropriate security and vulnerability assessment tools are running.
- At login, last user login should not display.
- Inventory listing of hardware and software should be current and maintained.

License Management

- Ensure that application licensing requirements are documented, reviewed and maintained.
- Application licenses should be current/valid and individuals/groups with application access should have completed the necessary access request forms and adhere to licensing requirements.

Logical Access Controls

- All users are required to read the Agency Policy Computing Resource Administrative Instruction (AI 15-4.03) and sign an acknowledgement of the Agency IT Acceptable Use Code of Conduct policy prior to account activation.
- Procedures to grant/modify/delete access should be documented.
 - Access request forms for adding/modifying/deleting users should be used.
 - Account expiration for contractors and consultants.
 - Accounts adequately identify the user – no generic accounts
- Ensure that security administrator procedures exist to:
 - Create/remove application access in a timely manner
 - Review user roles/permissions
- Validate that all users have accessed the application within the past 90 days.
 - Review dormant accounts
 - Inactive accounts should be removed.
- Each user has a unique user ID as described in the Port Authority Standard and Guidelines.
 - All user accounts profile should include Employee ID# and full user name.
- Roles are setup with least access required to perform job responsibilities.
- Roles should have a segregation of duties/roles.
- All accounts must have an individual or business group assigned to be responsible for account management.
- Segregation of duties and areas of responsibility must be implemented where appropriate.
- Whenever segregation of duties is not technically feasible, other compensatory controls must be implemented, such as monitoring of activities, audit trails and management supervision. The PA must approve these compensating controls.
- Review of audit trails and system approvals must be performed independent and retained to document the implementation of these security controls
- Access Control List (ACL) should include:
 - Current list of ACL.
 - Creation and updates to ACL
 - Testing and approvals of ACL
- The application should have the PA's warning banner on the login screen. The application has a warning banner, terms of use, and/or privacy statement that was approved by the Port Authority on the login screen.
- The system should have an access role that would allow real only access to all application, database and operating system screens, functions, logs and reports.
- Remote access should be approved, secured, and documented in accordance with PA policy. Remote access, at a minimum, must consist of multifactor authentication

mechanisms, secured communications (SSL/ VPN encryption methodology), access control mechanisms and logging of user activity.

Password Controls

- Ensure that password controls for the system are consistent with this requirements or more stringent
 - Passwords must be at least 10 alphanumeric characters long
 - Passwords must be changed every 90 days (administrators every 30 days)
 - Passwords must not be shared
 - Password complexity enable (capital letter, number, special character)
 - contain at least two upper and lowercase alphabetic characters,
 - contain at least one number (0-9)
 - contain at least one special character (e.g.-+}:>_?&\$%#).
 - Accounts should be locked after a three logon failures
 - Passwords should not be the same account name
 - No concurrent login capabilities
- End user accounts will be disabled (not deleted) after 60 days of non-use.
- Password file should be securely stored with limited access and encrypted.
- Application forces initial passwords to be changed and the initial passwords should not be easily guessable.
- Maintain a password dictionary and password history should be set to 5.
- Set “automatic session timeout” to 15 minutes of inactivity and require user to log back in with valid ID and password.
- Smartphones and smart device, where capable, shall leverage biometric access to provide the most security for the least inconvenience.

Application Controls

Data Validation & Input Controls

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

Data Retention and Management

- All data should be classified according to its sensitivity (confidential, etc) and protected accordingly.
- Data archive strategy should be documented and in place.
 - Should specify how long active data is kept.

Data Integrity and Security

- Sensitive data, such as credit card #s and social security #s, should be encrypted.
- Data should be restricted and audit trails should be available to identify all user activity include view access to sensitive data.
- Sensitive data should be stored in the database encrypted and blocked from user views in the application unless it is authorized.
- Encryptions level at a minimum should be AES 256bit when encryption is used.

Application Interfaces

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

Processing Controls

- Application databases/interfaces should have the necessary controls to prevent processing of inaccurate, duplicate, or unauthorized transactions and producing inaccurate outputs.
- Controls to ensure that all data is processed and accounted for should be in place.
- Rejected items should be logged, tracked and resolved in a timely manner.

Change Management

- Processes and tools should be used to report, track, approve, fix, and monitor changes on the application.
- The application and all changes to the application should be tested before being put into production.
 - Documentation of approval for change and evidence of testing should be in place.
 - Specific timetable/schedule should be documented.
- Emergency procedures should be documented and distributed.
- Separate environments are required for development, test, quality assurance, production.
- Procedures should require that no changes be made directly in the production environment without going through the development/test/quality assurance environments.
- Formal change control procedures for all systems must be developed, implemented and enforced.
- Where technically feasible, development software and tools must not be maintained on production systems.
- Source code for application or software must not be stored on the production system running that application or software.
- Privileged access to production systems by development staff must be restricted.

Application Logging, Audit Trails and Record Retention

- Audit trails for operating, application, and database systems should exist and reviewed.
- Users and roles should be tracked and reviewed
 - Maintain documentation
- All failed logon attempts should be logged.
- All sensitive transactions and changes should be logged and an audit trail created.
- Audit trails should contain who made the change, when it was made, and what was changed.
- Only the security administrator should have access to change or delete these logs or audit trails.
- Audit trails should be reviewed by the business owner(s) and security administrator.
- Management reporting should be produced through the application.

- Access reports by user and privilege should be produced and reviewed periodically including access violation reports.

Contingency Planning, Disaster Recovery and Backup Management

- A business contingency plan and a disaster recovery plan for the application should be documented and stored off-site, including escalation plan and current call tree.
- Plans should be tested and the outcomes of the tests (success/failure) should be documented.
- Regular backups of the application and the application data should be stored off-site.
- Application executables should be stored off-site or in escrow.
- Application configurations should be documented and backed-up.
- Full system backup should be encrypted.
- Backup procedures should be documented.
- Tape maintenance should include:
 - Periodically testing integrity of tape
 - Procedures for tape destruction due to faulty or scratched hardware.

Performance Monitoring

- Incident monitoring procedures should be documented and incidents logs should be reviewed to ensure that appropriate action is taken.
- Performance statistics should be examined and reviewed periodically by system administrators/business owner(s).
 - If vendor(s) support the application, a service level agreement for uptime, performance monitoring, updates, etc should be confirmed.
- Baseline tools or security products should be used and checked on a quarterly basis.

Patch Management

- Patch management procedures and documentation
 - Procedures should include testing, approvals, and distribution.
 - Documentation should include emergency procedures.
- Apply all new patches and fixes to operating system and application software for security.
- All security patches must be reviewed, evaluated and appropriately applied in a timely manner. This process must be automated, where technically possible.

Physical Protection

- Physical access to the application hardware should be appropriately restricted.
 - Physical access secured by single authentication mechanism i.e. swipe card.
 - Physical security adequate for equipment (locked cabinets).
- Appropriate fire suppression systems should be in place.
- Environmental condition adequately controlled (no water, dirt, clutter) and monitored.
 - Temperature and humidity monitoring should be implemented.
- Security cameras installed in sensitive areas
- Power surge protection and emergency power backup are in place.
- All hardware and software assets must be inventoried.

- Visitors including maintenance personnel, to data center, server and network equipment storage facilities must be escorted at all times.

Anti-virus/Malware/ Integrity/Vulnerability Software Management

- Virus patch management procedures must be documented, including emergency update procedures.
- Anti-virus and software integrity checkers must be implemented to prevent and detect the introduction of malicious code or other threats.
- Virus software engines and definitions must be implemented and up-to-date.
- A remote distribution server should be implemented for virus software updates and documentation on remote distribution should be current and maintained.
- Intrusion detection system must be in place,
- All systems must have vulnerability scans performed before going into production and periodically thereafter. Appropriate action, such as patching or updating the system, must be taken to address discovered vulnerabilities.
- Host-based intrusion detection/ firewalls software must be installed and enabled on all systems to protect from threats and to restrict access. Incident response procedures must be in place to address any alerts identified and system owner should be notified of alerts and what action was taken to mitigate the issues.
- Monitoring systems must be deployed (e.g., intrusion detection/prevention systems) at strategic network locations to monitor inbound, outbound and internal network traffic.
- Monitoring systems must be configured to alert incident response personnel to indications of compromise or potential compromise.
- Procedures must be established to maintain information security during an adverse event.
- Firewalls should be implemented.
- Firewall rules documentation should be up-to-date.
- Network management connections must be performed from a secure, dedicated network.
- Network authentication is required for all devices connecting internal networks.

Wireless Device

- Devices should be using WPA/WPA2 and AES encryption or better.
- Devices should disallow broadcasting of the SSID.
- All default parameters should be changed.
- Devices should have MAC address filtering enable or some type of authentication mechanism in place.

Web Application Vulnerabilities and Controls

- The following best practice and standards from these three web sites shall be followed:
 - The Open Web Application Security Project (OWASP) - www.owasp.org
 - www.webappsec.org (a consortium of web application security professionals)
 - Center for Internet Security (CIS) – www.cisecurity.org
- Perform data validation & integrity checks for field values and ensure the HTML special characters are stripped for all HTML request.
- Do not allow site pages to be cached by user browsers.

- All sensitive, personal or confidential data (including SSN, passwords, session IDs for sensitive applications, confidential or sensitive business transactions, etc.) should be transmitted between browser and server within an SSL-encrypted session (or other encrypted transmission) and are encrypted in the database at rest.
- All sensitive and personal data should be masked and encrypted where possible.
- Legal Issues:
 - The site should have a privacy statement and term of usage.
 - American Disability Act – Section 508 should be considered during the development process due to the requirement that federal agencies' electronic and information technology is accessible to people with disabilities.
- Web Authentication: To prevent passwords from being passed in the clear, have authentication occur within an SSL encrypted tunnel. Use SSL (certificate) to protect the password.
- Password Reset:
 - For internal applications, reset passwords via the helpdesk or security administrator of the site
 - For external applications, send temporary password to known e-mail address, that must be changed upon login and/or
 - Have customer service reset after the user has been validated.
 - If possible, use two factor authentications like Secure ID fobs.

Credit Card Processing Checklist

- If credit cards are accepted, PCI Standards (PCI DSS v3.0) should be followed and the process should be PCI compliant. Ensure all vendors and consultants are required to be PCI compliant. Attachment - The payment card application should be PCI compliant (PA-DSS v3.0).
- A segregated network and/or an approved Point of Sale terminal should be in place for the system or terminal used to process credit card transactions.
- The credit card processor standard and requirements should be followed, i.e. maintain transaction data for two years.
- Maintain the security of the customer information, including not storing credit numbers, the cardholder CVC/CVV numbers or any of the data from the magnetic strip on the credit card.
- Maintain the transaction data for contesting chargebacks, ensure that the processor fees are appropriate and do reconciliations of the transactions processed and the money deposited in the Port Authority bank accounts.
- The appropriate Port Authority functional areas should be made aware of credit card processing activity and should be involved in applying for the Merchant ID for MasterCard/Visa, Discover and American Express.
- Create a privacy policy and procedure for staff and consultants.
- Perform quarterly vulnerability scans of the network that contains the credit card processing, annual PCI reviews according to the PCI DSS, and annual system penetration testing.
- Perform the appropriate annual assessment and provide a report on compliance (ROC) which state shows compliance.

Disaster Recovery

- The Disaster Recovery plan should include at a minimum the following areas.
 - Business Impact Analysis
 - Critical Time Frame
 - Application System Impact Statements
 - Recovery Strategy & Approach
 - Recovery Time Objectives (RTO)/Recovery Point Objectives (RPO) for all critical systems.
 - Disaster Definition
 - Detailed Recovery Steps for each Disaster Definition
 - Escalation Plans and Decision Points
 - System Components- An inventory of the criticality of systems (including but not limited to software and operating systems, firewalls, switches, routers and other communication equipment).
 - Disaster Recovery Emergency Procedures
 - Plan Procedure Checklist
 - Disaster Recovery Team Organization
 - Salvage Team & Team Responsibilities
 - Disaster Recovery Responsibilities
 - Essential Position – Require back-up personnel to be assigned.
 - Contacts information Disaster Recovery Team and critical vendors - this area should be reviewed semi-annually for updates and changes.
 - Post-Disaster – Detail what steps need to be taken to move from disaster mode back to normal operations.
- Contingency plans (c.g., business continuity plans, disaster recovery plans, continuity of operations plans) must be established and tested regularly.
- Backup copies of procedures, software, and system images should be taken regularly and moved offsite.
- Backups and restoration must be tested regularly.