Torres Rojas, Genara FOI #13605

From: creis@greensavits.com
Sent: Friday, November 30, 2012 5:03 PM
To: Duffy, Daniel
Cc: Torres Rojas, Genara; Van Duyne, Sheree
Subject: Freedom of Information Online Request Form

Information:

First Name: Claudia
Last Name: Reis
Company: Green Savits & Lenzo
Mailing Address 1: 25 Airport Road
Mailing Address 2: Suite 200
City: Morristown
State: NJ
Zip Code: 07960
Email Address: creis@greensavits.com
Phone: 973-695-7777
Required copies of the records: Yes

List of specific record(s):
Contract entered into by and between Port Authority of NY NJ and KratosHBE or Kratos Defense Security Solutions, Inc. on or about November 28, 2007 concerning the installation and maintenance of video surveillance and security systems on the George Washing Bridge, Lincoln Tunnel, and the Holland Tunnel.

THE PORT AUTHORITY OF NY & NJ

FOI Administrator

May 22, 2013

Ms. Claudia Reis
Green Savits & Lenzo
25 Airport Road, Suite 200
Morristown, NJ 07960

Re: Freedom of Information Reference No. 13605

Dear Ms. Reis:

This is a response to your November 30, 2012 request, which has been processed under the Port Authority's Freedom of Information Code (the "Code") for a copy of the contract between the Port Authority and KratosHBE or Kratos Defense Security Solutions, Inc. on or about November 28, 2007 concerning the installation and maintenance of video surveillance and security systems on the George Washington Bridge, Holland Tunnel and Lincoln Tunnel.

Material responsive to your request and available under the Code can be found on the Port Authority's website at http://www.panynj.gov/corporate-information/foi/13605-C.pdf. Paper copies of the available records are available upon request.

Certain material responsive to your request is exempt from disclosure pursuant to exemptions (1) and (4) of the Code.

Please refer to the above FOI reference number in any future correspondence relating to your request.

Very truly yours,

Daniel D. Duffy
FOI Administrator

225 Park Avenue South, 17th Floor
New York, NY 10003
T: 212 435 3642
F: 212 435 7555

THE PORT AUTHORITY OF NY & NJ

November 30, 2007

DHL Overnight Mail - 201 794-6500
Henry Bros. Electronics, Inc.
17-01 Pollitt Drive
Fair Lawn, NJ 07410

Attn: Mr. Ted Gjini, VP. Operations – New Jersey Office

RE: **REQUEST FOR PROPOSALS (RFP) NO. 13071 MAINTENANCE OF ACCESS CONTROL SYSTEM AND SYSTEM ADMINISTRATION SERVICES FOR THE GEORGE WASHINGTON BRIDGE (GWB), LINCOLN TUNNEL (LT), HOLLAND TUNNEL (HT) AND STATEN ISLAND TELEPORT – AWARD LETTER PURCHASE ORDER #4500054655 CONTRACT #4600007087**

Dear Mr. Gjini:

The Port Authority of New York and New Jersey ("the Authority") hereby accepts the proposal of Henry Bros. Electronic, Inc. (HBE) for Maintenance of Access Control System and System Administration Services for the George Washington Bridge (GWB), Lincoln Tunnel (LT), Holland Tunnel (HT) and Staten Island Teleport, with a term commencing at 12:01 AM on December 8, 2007 and, unless sooner terminated, expiring at 11:59 PM on/about December 7, 2010 inclusive of a 30 day transition period. During the transition period, the Authority will waive the Liquidated Damages as set forth in Section 10, entitled: "Required Service Levels and Damages for Non-Performance" set forth in the Contract document. Henry Bros. shall be responsible for rendering the services required hereunder effective, December 8, 2007. The Authority shall have the option to extend the Contract for up to two (2) additional two-year periods and one additional 120-day period.

The Contract between the parties shall consist of the following Items, 1 through 8; in case of conflict between any of the items, the prior listed item shall take precedence over the later listed item:

This letter of Acceptance including the following attachments:

1. Henry Bros. Electronics Inc. response to question dated September 20, 2007, including Part III – Cost Proposal Sheets "Exhibit E – Revised June 22, 2007" and Exhibit F.

Procurement Department
One Madison Avenue, 7th Floor
New York, NY 10010
T: 212 435 7000

2. Henry Bros. Electronics Inc. response to question from meeting held on September 10, 2007.

3. Henry Bros. Electronics' Best and Final Offer and Additional Clarifications response dated September 7, 2007; including Part III – Cost Proposal Sheets, Exhibit A through D; excluding Part III – Cost Proposal Sheets Exhibit #E and Exhibit F.

4. Henry Bros. Electronics' response for Questions and Answers dated August 23, 2007, excluding Part III – Cost Proposal Sheets Exhibit A through C and Exhibit A Price Summary Sheet.

5. Henry Bros. Electronics Inc. response to Clarifications and Additional Information dated July 23, 2007.

6. Henry Bros. Electronics Inc. Copy of Presentation dated July 12, 2007; Response to Request for Clarifications for Questions and Answers dated July 6, 2007. The Authority's letter to Henry Bros. for presentation meeting and additional clarification dated June 28, 2007

7 Henry Bros. Electronics Inc. Proposal dated June 4, 2007, excluding Part III – Cost Proposal Sheets Exhibit A through G.

8. The Authority's Request for Proposal for Access Control System and System Administration Services for the George Washington Bridge (GWB), Lincoln Tunnel (LT), Holland Tunnel (HT) and Staten Island Teleport Collective #13071, dated December 2006, as amended by Addendum No. 1 dated April 25, 2007; Addendum No. 2 dated May 9, 2007; Addendum No. 3 dated May 17, 2007; Addendum No. 4 dated May 25, 2007; Addendum No. 5 dated May 29, 2007.

No other document shall form a part of these agreements.

For payment, invoicing and administrative purposes refer to the Purchase Order **#4500054655**. The Contract Manager is Mr. John Garbarini who can be reached at 201 346-6061.

Except for those identified above, no other documents or submissions by the Contractor, and no oral discussions or statements are to be considered a part of these agreements.

THE PORT AUTHORITY OF NY & NJ

If you are in agreement with the above, please so indicate by signing at the lower left and returning both signed originals to the attention of Ms. Jeanette Santos, Procurement Department, 7th Floor at the above address. The Port Authority will return one fully executed original of this letter to you following execution by the Port Authority. If you have any questions, please contact Ms. Santos at (212) 435-3930.

Very truly yours,

The Port Authority of NY & NJ

By: _____

Title: Director, Procurement Department

Date: 12/14/07

APPROVED:

FORM	TERMS

Agreed:

Henry Bros. Electronics, Inc.

By: Ted Spini

Title: GM + VP Operations

Date: 12-5-07

JS

Attachments

HENRY BROS. ELECTRONICS, INC.
17 01 Pollitt Drive Fair Lawn, NJ 07410
Phone: 201.794.6500 www.hbe-inc.com Fax: 201.794.8341

September 20, 2007

Ms Jeanette Santos
Senior Purchasing Manager
Purchasing Services Division
The Port Authority of NY/NJ
1 Madison Avenue
Seventh floor
New York, NY 10010

Re: Responses to PANYNJ questions dated September 17, 2007

Dear Ms. Santos:

Enclosed please find HBE's responses to the Port Authority's questions dated September 17, 2007.

We trust that this information will prove helpful to the Port Authority.

If you should have any questions regarding this submittal or need any further information regarding any aspect of HBE's proposal, please do not hesitate to contact me.

Very truly yours,

Bernard J. Drury
VP, Sales & Marketing, Aviation
Henry Bros. Electronics, Inc.

Maintenance of Access Control System and System Administration Services for the George Washington Bridge, Lincoln Tunnel, Holland Tunnel and Staten Island Teleport

Responses to PANYNJ questions dated September 17, 2007

Question #1

Please confirm that Henry Brothers agrees to a maximum of up to 3% escalation per year for the option periods exercised for the following areas:

Exhibit A, Preventive and Corrective Maintenance of the ACS System, and Exhibit C, System Administration.

The following exhibits will not receive additional compensation during any exercised option period: Exhibit B, Computerized Maintenance Management System, Exhibit D, Miscellaneous Cost, Exhibit E, Maintenance of Traffic.

HBE Response:

HBE agrees to the limits on escalations during the option periods as listed above.

Question #2

Please resubmit the Exhibit E, Maintenance of Traffic, recalculate and resubmit Exhibit F, Pricing Summary.

HBE Response:

Please see attached.

Maintenance of Access Control System and System Administration Services for the George Washington Bridge, Lincoln Tunnel, Holland Tunnel and Staten Island Teleport

Responses to PANYNJ questions dated September 17, 2007

Question #3

If the Authority exercises its right to add Staten Island Bridges (SIB) at anytime during the term of this contract, it is the Authority's understanding that the price quoted in Exhibit G will be Henry Brothers monthly compensation for services described in the RFP for Staten Island Bridges (SIB).

In addition, escalations for any options exercised for SIB will be adjusted up to 3% maximum per year for the following: Exhibit A, Preventive and Corrective Maintenance of the ACS System, and Exhibit C, System Administration Services.

The following exhibits will not receive additional compensation during any exercised option period: Exhibit B, Computerized Maintenance Management System, Exhibit D, Miscellaneous Cost, Exhibit E, Maintenance of Traffic.

HBE Response:

HBE agrees to the limits on escalations during the option periods as listed above.

PART III - COST PROPOSAL SHEETS

EXHIBIT E - Revised June 22, 2007

Maintenance of Traffic - Three Year Base Term

(A)	(B)	(C)	(D)	(E)
Description	**Lane Closures per Month**	**Estimated Price Per Lane Closure**	**X 12 Months**	**Estimated Total Annual Price**
George Washington Bridge	3	**$1,350.00**	x 12	$48,600.00
Holland Tunnel	2	**$1,350.00**	x 12	$32,400.00
Lincoln Tunnel	2	**$1,350.00**	x 12	$32,400.00

Total Estimated Annual Maintenance of Traffic Cost $ 113,400.00
(Sum of Item in Column D)

Note: Normal working hours are between the hours of 11 PM - 6 PM , unless otherwise directed by the Contract Manager or Facility Manager.

Note: The Proposer shall refer to the section titled Maintenance of Traffic Attachment C - Scope of Work.

Note: Work may be requested at the sole discretion of the Contract Manager at any time during the term of this contract. No work will be started without prior authorization. No work is guaranteed.

PART III - COST PROPOSAL SHEETS

EXHIBIT F

Price Summary

(A)	Estimated Total 3 Year Price - Preventive and Corrective Maintenance of the Access Control System (Multiply total estimated annual price from Exhibit A by 3 years)	$	2,265,012.00
(B)	Estimated Total 3 Year Price - Computerized Maintenance Management System (Multiply total estimated annual price from Exhibit B by 3 years)	$	18,000.00
(C)	Estimated Total 3 Year Price - System Adminstration Services (Multiply total estimated annual price from Exhibit C by 3 years)	$	514,800.00
(D)	Estimated Total 3 Year Price - Miscellaneous Costs (From Exhibit D)	$	40,670.00
(E)	Estimated Total 3 Year Price - Maintenance of Traffic (Multiply total estimated annual price from Exhibit E by 3 years)	$	340,200.00

(The Proposer shall refer to the Extra Work sections in Part II for explanation of compensation)

TOTAL ESTIMATED CONTRACT PRICE
(Total items (A), (B), (C), (D) & (E) $ 3,178,682.00

Santos, Jeanette (Procurement)

From: Bernie Drury [BDrury@hbe-inc.com]
Sent: Thursday, September 13, 2007 9:06 AM
To: Santos, Jeanette (Procurement)
Cc: John Batsch; Barbara Campolieto; Bernie Drury
Subject: Answers to questions from meeting on Monday, September 10th
Importance: High

Jeanette,

Attached please find an outline of the Transition Plan that goes into a bit more detail than what was previously submitted.

Additionally, we have come to an agreement regarding the issue of escalations during the Option Period(s), as follows:

HBE agrees to a maximum of 3% per year of the Preventive/Remedial Maintenance and System Administration dollars only and not miscellaneous costs (i.e. Maintenance of Traffic, etc).

We have not yet received the list of references who have been difficult to contact but will respond promptly when we do get it.

Lastly, we are compiling a list of items that HBE would like to get from the Port Authority to ease the transition process and will submit it shortly.

Bernie Drury
Henry Bros. Electronics, Inc
17-01 Pollitt Drive
Fair Lawn, NJ 07410
201-805-1410 (cell phone)

HENRY BROS. ELECTRONICS, INC.
17-01 Pollitt Drive Fair Lawn, NJ 07410
Phone: 201.794.6500 www.hbe-inc.com Fax: 201.794.8341

INTER-OFFICE MEMO

TO: File

FROM: J. A. Batsch

SUBJECT: GWB/HT/LT Maintenance Transition Plan

DATE: September 11, 2007

As stated in HBE's "Response to PANYNJ questions dated July 5, 2007" the Transition Plan will commence 60 days prior to the contract taking effect. During this 60 day period, this Transition Plan would include, but not be limited to, weekly meetings with the current service provider to achieve the following objectives:

- Define and capture service routines
- Conduct an audit of the existing equipment/systems to baseline operation and functionality
- Review routines with PA Operations personnel to improve processes currently in place
  - HBE's Management Staff
  - System Administrator
- Interview incumbent service/maintenance staff as potential candidates to augment HBE's personnel assigned to program
  - Request PA input on incumbents
- Submit revised Maintenance Plan and Organization to PA for review and concurrence 30 days prior to contract taking effect
- Augment existing staff with new qualified personnel
  - Complete all badging requirements
  - Review routines
  - Conduct orientation sessions (familiarization of facilities, equipment, staff, etc.)
  - Conduct site visits (utilize HBE consultants and PA)
  - Train / certify staff on equipment
- Meet with PA to review Plan and Organization
- Conduct formal "Hand Off" session from incumbent to HBE

DRAFT

HENRY BROS. ELECTRONICS, INC.
17-01 Pollitt Drive Fair Lawn, NJ 07410
Phone: 201.794.6500 www.hbe-inc.com Fax: 201.794.8341

September, 2007

09-07-07P02:02 RCVD

Ms Jeanette Santos
Senior Purchasing Manager
Purchasing Services Division
The Port Authority of NY/NJ
1 Madison Avenue
Seventh floor
New York, NY 10010

Re: BAFO
Project # 13071

Dear Ms. Santos:

Please find the attached answers to the questions posed in your letter dated September 4, 2007. Additionally, please reference the attached revised pricing sheets which reflect the HBE Best And Final Offer.

We will see you on Monday, September 10th at 2:30 to review this information and answer any other questions you may have.

If you should have any questions, please contact me at 201-805-1410.

Sincerely,

Bernard J. Drury, Jr.
VP Sales & Marketing, Aviation
Henry Bros. Electronics, Inc.
17-01 Pollitt Drive
Fair Lawn, NJ 07410

September 7, 2007

Maintenance of Access Control System and System Administration Services for the George Washington Bridge, Lincoln Tunnel, Holland Tunnel and Staten Island Teleport

Responses to PANYNJ questions dated September 4, 2007

Question #1

Please provide a breakdown and cost reduction associated with the Maintenance of Traffic (MOT) per facility. HBE may have overestimated in this area.

HBE Response:

The pricing for this service is based upon recent experience providing exactly this service at the Brooklyn Battery Tunnel. A lane closure would include (1)Arrowed attenuator truck, with driver, including tolls during the identified time periods. The number of lane closures per month seems a bit high and that would be the area where reductions could be available.

Question #2

Please provide a breakdown and cost reduction for the System Administration Services.

HBE Response:

The System Administration will consist of an HBE, Lenel Enterprise certified, System Administrator on site three (3) days per week. Lou Avagnano is identified as the project System Administrator. His duties consist of: Performing system diagnostics, maintenance of database, archiving, analysis and integration functions.

Please see revised Exhibit C.

September 7, 2007

Maintenance of Access Control System and System Administration Services for the George Washington Bridge, Lincoln Tunnel, Holland Tunnel and Staten Island Teleport

Responses to PANYNJ questions dated September 4, 2007

Question #3

Please provide a breakdown and cost reduction for the Preventative and Corrective Maintenance.

HBE Response:

The Preventative and Corrective Maintenance service for the facilities will be provided by three (3) dedicated, certified HBE technicians. The allocation of resources is as follows:

GWB	***- One technician***
LT	***- One technician***
HT	***- One technician***
Teleport	***- This site will be serviced by a rotation of the technicians from the LT and HT***

The Preventative and Corrective Maintenance costs also include 24 hour Software Support from Lenel and Verint. Finally, the costs include spare parts as directed in the last communication from the Port Authority.

Please see revised Exhibit A.

September 7, 2007

Maintenance of Access Control System and System Administration Services for the George Washington Bridge, Lincoln Tunnel, Holland Tunnel and Staten Island Teleport

Responses to PANYNJ questions dated September 4, 2007

Question #4

Confirm the responsibility and duration of individuals as cited in your organization chart and management plan. Briefly explain the roles and responsibilities of each individual for the duration of this project.

HBE Response:

Ted Gjini	-	*Overall responsibility for day to day Operations*
John Batsch	-	*Responsible for all Port Authority Service, Installations and Operations.*
Lou Avagnano	-	*Lenel Enterprise certified System Administrator. (see response to question #2)*
John Cameron	-	*Directly manages all Service personnel.*
Emily Kaneaster	-	*Contract management assistant, including documentation and service dispatch.*
John Marrinan *Dan Hordyszynski*	-	*Provide site specific information during transition Period.*

PART III - COST PROPOSAL SHEETS

EXHIBIT A

Preventive and Corrective Maintenance of the Access Control System - Three Year Base Term

(A)	(B)	(C)	(D)
Description	**Monthly Maintenance and Corrective Repair**	**X 12 Months**	**Estimated Total Annual Price** $
George Washington Bridge	$26,167.00	x 12	314,004.00 0
Holland Tunnel	$17,250.00	x 12	$207,000.00 0
Lincoln Tunnel	$17,500.00	x 12	$210,000.00 0
Staten Island Teleport - Servers and Workstations	$2,000.00	x 12	24,000.00 0

Total Estimated Annual Maintenance Cost $ $755,004.00 0
(Sum of Item in Column D)

Note: All prices will be inclusive of materials and labor including software patches and replacements parts and components if required.

Note: Software updates and new releases for which the software vendor normally charges will be compensated as Extra Work. Installation thereof will not be separately compensated.

PART III - COST PROPOSAL SHEETS

09-07-07P02:03 RCVD

EXHIBIT B

Computerized Maintenance Management System - Three Year Base Term

(A)	(B)	(C)	(D)	(E)	(F)
Software	**Cost per Authority Licensed User**	**Estimated Required Number of Authority Licensed Users**	**Monthly Total**	**X 12 Months**	**Estimated Total Annual Price**
Software Licenses (per user)	$250.00	2	$500	x 12	$6,000
Other		2	$0	x 12	$0
Other:		2	$0	x 12	$0.00
Other:		2	$0	x 12	$0.00
Other:		2	$0	x 12	$0.00
Other:		2	$0	x 12	$0.00
Other:		2	$0	x 12	$0.00

Total Estimated Annual Price for Computerized Maintenance Management System $ **$6,000.00**
(Sum of Item in Column F)

The Contractor's compensation will commence once the Authority has accepted the system.

09-07-07P02:03 RCVD

PART III - COST PROPOSAL SHEETS

EXHIBIT C

System Adminstration Services - Three Year Base Term

(A)	(B)	(C)	(D)
Description	**Monthly System Adminstration Services**	**X 12 Months**	**Estimated Total Annual Price**
George Washington Bridge	$5,600.00	x 12	$67,200.00 0
Holland Tunnel	$3,200.00	x 12	$38,400.00 0
Lincoln Tunnel	$3,200.00	x 12	$38,400.00 0
Staten Island Teleport	$2,300.00	x 12	$27,600.00 0

Total Estimated Annual System Adminstration Cost $ $171,600.00 0

(Sum of Item in Column D)

PART III - COST PROPOSAL SHEETS

09-07-07P02:03 RCVD

EXHIBIT D

Miscellaneous Costs - Three Year Base Term

(A)	Cost to add additional operator workstation to the preventive maintenance schedule	$ $250.00
(B)	Cost to add door security setup to the preventive maintenance schedule (for example, inside/reader, strike lock or magnetic lock, audio/visual device)	$ $400.00
(C)	Cost to add a camera and PTZ units to the preventive maintenance schedule	$ $400.00
(D)	Cost to add motion detector device to the preventive maintenance schedule	$ $200.00
(E)	Cost to add Access Control Panel cabinet to the preventive maintenance schedule	$ $500.00
**(F)	Fiber Optic Repair Cost = $180.00 /hr*36 hrs * 4 times/yr	$ $25,920.00
**(G)	Repositioning of Camera during Facility Cleanup = $180.00 /hr* 2 hrs/unit * 25 units/yr	$ $9,000.00
(H)	Purchase of security ID cards (Quantity of 1000)	$ $4,000.00
	Total Estimated 3 Year Price	$ **$40,670.00** (Sum of Items Rows

Provide rates as requested above. Work may be requested at the sole discretion of the Contract Manager at any time during the term of the Contract. No work will be started without prior authorization.

**** Note: Normal working hours are between the hours of 6 AM - 6 PM , unless otherwise directed by the Contract Manage or the Facility Manager.**

HENRY BROS. ELECTRONICS, INC.
17-01 Pollitt Drive Fair Lawn, NJ 07410
Phone: 201.794.6500 www.hbe-inc.com Fax: 201.794.8341

August 23, 2007

Ms Jeanette Santos
Senior Purchasing Manager
Purchasing Services Division
The Port Authority of NY/NJ
1 Madison Avenue
Seventh floor
New York, NY 10010

Re: Responses to PANYNJ questions dated August 15, 2007

Dear Ms. Santos:

Enclosed please find HBE's responses to the Port Authority's questions dated August 15, 2007. In addition to these submittals I would like to submit the following information for consideration:

1) Maximo MRO – CMMS (Computerized Maintenance Management System)

   HBE has purchased the system and has received the software. We are currently in the process of hiring the administrator for this system.

2) HBE has hired a corporate CIO

   I am attaching the professional resume of Christopher Peckham who has recently been hired as the CIO for Henry Bros. Electronics, Inc. Mr. Peckham will be joining HBE on September 10, 2007.

We trust that this information coupled with the responses to your questions will prove helpful to the Port Authority.

If you should have any questions regarding this submittal or need any further information regarding any aspect of HBE's proposal, please do not hesitate to contact me.

Very truly yours,

Bernard J. Drury
VP, Sales & Marketing, Aviation
Henry Bros. Electronics, Inc.

Maintenance of Access Control System and System Administration Services for the George Washington Bridge, Lincoln Tunnel, Holland Tunnel and Staten Island Teleport

Responses to PANYNJ questions dated August 15, 2007

Question #1

Regarding Question 2 for HBE's methodology for administering and maintaining the Lenel System: In Item 1.1.1 HBE proposes to subcontract Lenel PES (Professional Engineering Services) to do remote health checks over a WAN. At this time, TB&T and Public Safety does not encourage remote access. How would HBE perform the task without remote access capability?

HBE Response:

In the absence of remote capability HBE will collect data from the system during a regularly scheduled administrative visit (this data will be purged of any PANYNJ specific, security sensitive data) and will send the scripts to Lenel for analysis.

There will be no change in the HBE pricing for the System Administration.

Question #2

Metcomm, LLC is not currently certified as an M/WBE by the Port Authority. PJS is certified by the Port Authority. However, no dollar amounts or percentages are shown in your M/WBE plan. HBE must submit a plan that states the Firm and approximate dollar value and percentage against the contract. Credit is given only to vendors who are certified by the Port Authority. Provide an updated M/WBE Participation Plan for evaluation.

HBE Response:

Please see revised plan.

Maintenance of Access Control System and System Administration Services for the George Washington Bridge, Lincoln Tunnel, Holland Tunnel and Staten Island Teleport

Responses to PANYNJ questions dated August 15, 2007

Question #3

Regarding Part III – Cost Proposal Sheets – Exhibit A, HBE's proposal does not include the price for replacement of parts or equipment. As part of the evaluation, HBE must incorporate the cost to maintain and supply spare parts as part of the monthly preventive and corrective maintenance of the Access Control System. HBE must re-price and resubmit the pricing sheet to include the cost of spare parts replacement. HBE can replace the sum of the parts (i.e. camera lens, camera brackets) or the system in whole (e.g. camera).

HBE Response:

Please see revised Cost Proposal Sheet – Exhibit A.

Question #4

Operational Availability for Type I and Type II failures has been amended, see attached Amendment #1. Please revise your cost proposal sheets accordingly.

HBE Response:

Please see revised Cost Proposal Sheets.

HENRY BROS. ELECTRONICS, INC.
17-01 Pollitt Drive Fair Lawn, NJ 07410
Phone: 201.794.6500 www.hbe-inc.com Fax: 201.794.8341

Port Authority of New York and New Jersey
Request for Proposal

Maintenance of Access Control System and System Administration Services for the George Washington Bridge, Lincoln Tunnel, Holland Tunnel and Staten Island Teleport

MBE/WBE Utilization Plan
August 2007

HBE intends to perform the services of this contract primarily by utilizing HBE employees who have been trained and certified by Lenel and Verint.

When an opportunity arises, HBE will hire MBE/WBE/DBE Subcontractors identified on the Port Authority web site as Approved and Certified by the PANYNJ.

Two Port Authority Certified MBE/WBE/DBE firms who have worked with HBE on Port Authority projects are:

1) Maureen Data Systems, Inc (WBE & SBE)
Supplier of Cisco and other equipment
500 West 43rd Street
New York, NY 10036
212-290-1557
Certificate Number: PA-23100
Anticipated Participation - 5%

2) PJS Electric, Inc. – (Paul Scariano) (WBE & DBE)
Licensed Electrical Contractors
Brooklyn, NY 11232
718-832-9609
Anticipated Participation - 5%

HBE intends to make every "Good Faith Effort" in utilizing MBE/WBE/DBE firms when practical and has in the past achieved required goals on other public authority contracts.

Anthony R. Coscia
Chairman

THE PORT AUTHORITY OF NY & NJ

Anthony E. Shorris
Executive Director

Certified

by

Office of Business & Job Opportunity

Maureen Data Systems, Inc.

Certificate PA-23100

This certificate acknowledges that the above named firm is certified as a **Woman-owned Business Enterprise.** This company has met the criteria for ownership and control as established by the Port Authority's Policy for Revised Minority, Woman and Small Business Enterprise (M/W/SBE) Programs, dated June 10, 1993.

This certification will remain in effect for five years from the date of notice and may be extended only upon submission by you, and acceptance by the Port Authority of a recertification application attesting that the ownership and control of the business, on which this certificate is granted, has not changed. This office must be notified within 30 days of any material changes in the business which affect ownership and control. Failure to do so may result in the revocation of this certification and/or imposition of other sanctions.

Lash Green
Director
Certified: August 3, 2007

Rosemary Jenkins Varela
Manager, Certification
Scheduled Re-certification: August 2, 2012

Form: 6/10/93

THE PORT AUTHORITY OF NY & NJ

Anthony R. Coscia
Chairman

Anthony E. Shorris
Executive Director

Certified

by

Office of Business & Job Opportunity

Maureen Data Systems, Inc.

Certificate PA-23100

This certificate acknowledges that the above named firm is certified as a Small Business Enterprise (Community Program). This company has met the criteria for ownership and control as established by the Port Authority Policy for Revised Minority, Woman and Small Business Enterprise (M/W/SBE) Programs, dated June 10, 1993.

This certification will remain in effect for five years from the date of notice and may be extended only upon submission by you, and acceptance by the Port Authority of a recertification application attesting that the ownership and control of the business, on which this certificate is granted, has not changed. This office must be notified within 30 days of any material changes in the business which affect ownership and control. Failure to do so may result in the revocation of this certification and/or imposition of other sanctions.

Lash Green
Director
Certified: August 3, 2007

Rosemary Jenkins Varela
Manager, Certification
Scheduled Re-evaluation: August 2, 2012

Form: 6/10/93

Christopher Peckham

(Ex. 1)

Information Technology decision maker at the organizational level (CIO, VP, Director)

Customer Service • Business Process Improvement • Infrastructure
Hosting • Internetworking • Operations • Strategic and Tactical Planning
System Development and Integration • Project Management

Extensive management and technical expertise applied in a wide range of organizations including higher education, Internet service providers, professional services, and outsourcing.

AREAS OF EXPERTISE

- Demonstrated leadership and proficiency using Information Technology to aid business processes and improve organizational effectiveness.
- Ability to position technology to offer information and resources to a wide range of users.
- Successfully develop and implement system automation and workflow improvements.
- Ability to solve complex business issues at minimal cost, including the development and deployment of custom applications or open source packages. Work has included integration with commercial off the shelf software.
- Development and leverage of standard operating procedures and metric reporting across support functions.
- Planning and implementing solutions to address business needs, including the development of strategic and tactical plans.
- Management of diverse groups and teams ranging from 6 to 150 across technical and non-technical skill sets and geographic locations.
- Effective project management, problem solving, and demonstrated innovation in collaborative and dynamic environments.

EXPERIENCE

Director of Operations 2003 – present
SunGard Higher Education, Mercy College, Dobbs Ferry, NY

Manage a staff of eighteen in the areas of desktop support, helpdesk, networking, and telecommunications at a small/mid-size college with six campus locations, serving over 600 faculty/staff and 9000 students, with over 1800 servers, desktop, laptops, and computer laboratory systems.

Systems include Active Directory, Exchange, IIS, Apache, DNS, DHCP, MS SQL, Blackberry Enterprise Server, HEAT, CMS/ plone, academic support systems (Banner, Plus, WebCT, Sakai), tacacs/radius authentication, nagios/cacti monitoring servers, squid cache server, and wireless access.

- Re-designed staffing structure, process, and methodology to allow for increased support of the user community. Changes allowed for additional reporting and improvement of support metrics. Implemented systems to reward staff for suggestions and demonstrated improvements. Corresponding growth of ticket volume of 18% and a reduction in average response time of 50% over two years with no increased staffing.
- Increased service levels to reduce monthly SLA penalties running over $10,000 per month.
- Serve on a number of college advisory committees dealing with strategic and support issues. Worked to develop the technology strategic plan used in accreditation process.
- Successful project management and configuration of network and VoIP system for a new campus with over 350 systems and capital equipment budget exceeding $1.1 million.
- Creation of technology purchasing and tracking process based on SQL-Ledger that resulted in a reduction of like expenditures by 15%. Workflow process improvements allowed for 25%

decrease in hardware installation times.

- Developed MySQL based database system used to track hardware assets. Scripts poll network devices and SMS to audit the production environment.
- Integration between Avaya and Cisco telephone systems using Asterisk PBX and Active Directory to allow for uniform auto-attendant and 'dial by name' capabilities between platform and campus locations. System generates Excel, PDF, and WWW user directories.

Vice President, Engineering 2002 – 2003
SkipJam Corp, Greenwich, CT

Startup company in the consumer electronics space developing a "multimedia hub".

- Schematic design using Orcad and PCB layout using P-CAD.
- System benchmarking across linux systems including embedded Lineo and prototype drivers.

VP of Network Engineering & Operations / Senior VP of Information Systems 1999 – 2002
Globix – The Global Internet Exchange, New York, NY

Served in a role similar to the Chief Information Officer and managed the staff responsible for architecture and operation of the internal and client facing infrastructure. Groups included network and system engineering, operations, project management, datacenter, and call center. Staff ranged in size from 15 to 150 with annual salary budget up to $9.1 million. Duties included related capital/operating budgeting. Infrastructure served over 900 staff and the company's client base in over 20 US and international locations.

System development, operation, and integration was performed using a mix commercial and open source packages including Remedy, HP Openview, Micromuse Netcool, Concord Network Health, mrtg, cacti, nagios, Apropos ACD system, and Oracle Financials.

- Completed the initial network and system build out of three fully-redundant data centers (NYC, Santa Clara, and London, England). Successfully deployed, configured, and operated a large number of systems used for monitoring, billing, and support. Created network and system engineering laboratory modeling network backbone and data centers.
- Involved in the deployment and operation of Oracle Financials, used for core financial functions. Developed automated systems used for information interchange and reporting. Implemented workflow and integration of auditing and operational support systems. Created systems that allowed for staff and client access to operational and billing information.
- Led the integration of a number of COTS packages with open source and in-house software systems. These included billing, monitoring, vendor payment, telecommunication auditing, and workflow auditing/reporting. Developed "quote to collect" system used to create and approve sales quotations, orders, and invoicing.
- Developed systems that aligned data and workflow to the business process. Allowed for the tracking of telecommunications charges, billing/metric warnings to clients and trend analysis of network utilization. Allowed company to reduce telecommunications billing by over 20%.
- Maintained relationships with key vendors. Re-negotiated contracts with software vendors that saved over $3 million.
- Created operations and call center workflow and standard operating procedures that were used by networking and system staff in multiple locations. These served as a basis for uniform customer service from location to location.
- Supported the creation of sales and marketing materials as well as pre-sales and post-sales support. Standardized product codes were developed and used during provisioning and billing.
- Designed and implemented Apropos/ACD (automatic call distribution) scripts to fulfill requirements of various users. Delivered reporting and training based on relevant metrics.
- Aligned staff with organizational needs and business objectives through various market changes. Led changes when business and workflow process improvements were needed.

- Implemented redundancy and disaster recovery plans that allowed key systems to operate from multiple datacenters.

Manager of Network Engineering 1997 – 1999
Qwest Internet Solutions / ICon CMT Corp., Weehawken, NJ

Managed day-to-day project management, network planning, network monitoring systems, build-out, standards, and development of operating procedures.

- Supervised the redesign of BGP and OSPF configuration on a national multi-POP network connecting clients, transit, and major Internet peering locations.
- Led the design of networks, racks, and cable plant in multiple POPs and data centers.

Director of Network Operations 1995 – 1997
Bell Technology Group, New York, NY

Managed the day-to-day activities and long-term project planning for the technical staff; this included customer configuration, consulting management, personnel scheduling, telecommunication circuit provisioning, project management, project budgeting, etc.

- Developed and implemented trouble ticket system and standard operating procedures.
- Led migration of the production datacenter between two locations with minimal downtime.

Director of Technology – Interactive Media Division 1995
Database America Companies, Montvale, NJ

- Created a heterogeneous network of Unix, Microsoft Windows, and Macintosh systems.
- Performed analysis of DEC Alpha processor related to data-mining projects.

Systems and Networking Support – principal technical consultant to local ISP 1994 – 1996
INTAC Access Corporation, Palisades Park, NJ (concurrent)

- Installed and managed systems, routers, and switches in multiple points of presence (POPs).
- Developed WWW programs and scripts for various clients.

Senior Systems & Networking Administrator – Computing Services Dept. 1990 – 1995
New Jersey Institute of Technology, Newark, NJ 1987 – 1995

Management, installation, and support of over one hundred heterogeneous Unix systems.

- Installed and configured various Internet/Intranet software systems (client and/or servers).
- Created applications enabling easier access to resources (e.g. obtaining accounts, class registration, NSF grant information, backup restores at user request).

EDUCATION

Rutgers	M.B.A. (2007) with concentration in Management & Global Business
NJIT	Ph.D. (2000), MS (1989), and BS (1987) all in Electrical Engineering

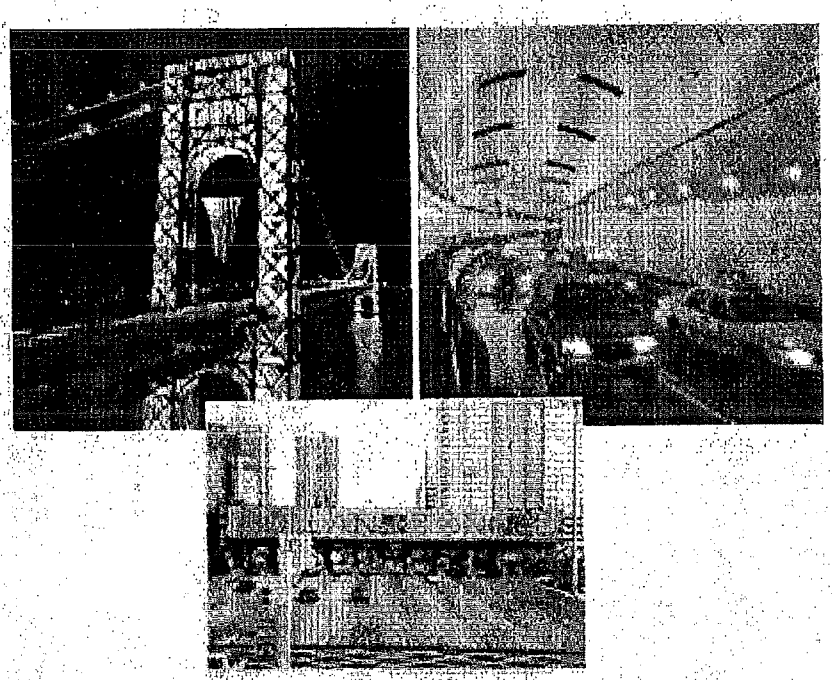
PROFESSIONAL CERTIFICATIONS, ORGANIZATIONS AND OTHER

- Member of the Advanced Computing Systems Association (USENIX), the System Administrators Guild (SAGE), and Institute of Electrical and Electronics Engineers (IEEE).
- Have participated in EDUCAUSE, the North American Network Operators' Group (NANOG) and the Internet Engineering Task Force (IETF) activities.
- Served on the NJIT Electrical and Computer Engineering Industry Advisory Board (2000 – 2006).
- Held Cisco Certified Internetworking Expert (CCIE #3094).
- Held Sun Microsystems Competency 2000/Enterprise certification (Examinations in the areas of Solaris 2.x NIS+, Network, System Administration and Solaris Volume Management).

Access Control System RFP #13071

Maintenance of Access Control System
and
System Administration Services

Response to Clarifications
Additional Informtion



Submitted by:

HENRY BROS. ELECTRONICS, INC.
17-01 Pollitt Drive Fair Lawn, NJ 07410
Phone: 201.794.6500 www.hbe-inc.com Fax: 201.794.8341

Bernie Drury (201) 794-6500 ext. 3037

July 23, 2007

Access Control System RFP # 13071

Henry Bros. Electronics, Inc. (HBE)

Questions based on July 12, 2007 Presentation Outline **Response Tab #**

1. **For system administration responsibilities, please submit.....Tab # 1**
   the following names and resumes:
   - **What is the name of the Database Administrator of Record?**
   - **The name of the person responsible to respond to server failure?**
   - **Is there an overall single point of contact? If so, please provide their name? If not, please advise how coordination is handled.**

2. **Describe HBE's methodology for administering and.....Tab # 2**
   maintaining the LENEL system?
3. **Describe what industry best practices you will be applying?**
   - **Information Technology Change Management Policy & Procedure.....Tab # 3a**
   - **Information Technology Security Policy.....Tab # 3b**
   - **Logical System Access Policy.....Tab # 3c**
   - **Operations Management Policy.....Tab # 3d**

4. **In the presentation HBE explained that each preventive.....Tab # 4**
   maintenance routine is performed four times in a calendar year. Please confirm this in writing and please provide schedule.

5. **Does HBE understand the response and repair times for.....Tab # 5**
   Type I (2 hours) and Type II (3 hours) failures? Are there any scenarios under which HBE may not be able to comply with these performance requirements? If so, what are they and how will they be addressed.

1. **For system administration responsibilities, please submit the following names and resumes:**

   a. What is the name of the Database Administrator of Record?
      i. Tom Shen (resume included in this section.)
      ii. Additional database support will be provided by the Gotham Technology Group. HBE engaged Gotham to assist in the design and implementation of our infrastructure upgrade to support our corporate headquarter needs at our new offices in Fair Lawn NJ and local offices located in eight states. We currently utilizes their "Gotham*Watch*" product offering to supplement our in-house database administration for our nationwide system. This service combines telephone support with a hosted software-based monitoring solution to provide enhanced support and service.

   b. The name of the person responsible to respond to server failure?
      i. Tom Shen; 201-704-6500 ext 3905; tshen@hbe-inc.com

   c. Is there an overall single point of contact?
      i. Lou Avagnano; 201-794-6500 ext 3035; lavagnano@hbe-inc.com

TOM SHEN

(Ex. 1)

CERTIFIED NETWORK CONSULTANT & PROJECT MANAGER

Professional Certifications:

Cisco Certified Internetwork Expert #8080 (Routing/Switching)
2001
Cisco Certified Internetwork Expert #8080 (Security)
2002
Microsoft Certified System Engineer 3.X, 4.X, 2000, and 2003 (MCSE)
1994
Cisco Certified Security Professional (CCSP)
1998
Cisco Certified Network Professional (CCNP)
1997
HP Accredited Systems Engineer (ASE)
1997
HP Accredited Integration Specialist (AIS)
1997
Certified Novell Engineer 3.x 4.x and 5.x (CNE)
1989

Education:

Chen Kong University (Taiwan, MS of Computer Science)
1985

Technical Experience:

Henry Brothers Electronics **05/2006-Present**
Chief Network Engineer

- In charge of JFK International Airport, including SONET and Network Security.
- Network design and project leader for Henry Bros Electronic for the new office in Fair Lawn, including VPN, PIX, MS servers, MS Exchange, Citrix and switches
- Network design for JFK to upgrade SONET from OC3 to OC48
- Architecture engineer and project leader for First Aviation to redesign and setup their new security in NJ
- Projects leader for La Guardia Airports Wireless network upgrading and wireless security.
- Projects leader for MTA/TBTA Bridges and Tunnels to link all Bridges and Tunnels to 2 Broadway. (MTA HQ)

- Project leader for Long Island Bus.
- In charge of projects for AW34 Port Authority of NY and NJ..
- Project leader for WTC Building number 7 security.
- Project leader for Denver City Security implementation.
- Project design and leader for JFK Guard Post Security.

MTM Technologies 09/2005-04/2006

Architecture Engineer/Design Engineer

- Architecture Engineer for NY, NJ, and CT areas with multiple client engagements.
- Design and implement network solutions and network security for clients.
- Design Engineer and project leader for Globix relocation project to XO Communications.
- Project manager for Network Audit and Systems Analysis (NASA) project for GFI Group.
- Network Implementation for TheDeal.com.
- Network redesign and implementation for World Learning Training Comclientny.
- Security Analyze and implementation for Bank Street College in NYC involving upgrade switches, firewall, and VPN
- Network design for Capital Management involving implementation of Cisco 6500 switch, 7206VXR routers and network security.
- Design Engineer and project manager for the Hospital for Special Surgery, project involving both an infrastructure upgrade and complete security implementation. This upgrade included Cisco 7206VXR router, Catalyst 6513, 4507R, and 3750G switches implementation, ASA 5520 IPS module, MARS, and Ciscoworks 2000 for LMS and VMS configuration.
- Design Engineer for Weight Watchers International involving the redesign of their HQ including LAN, WAN, SAN and network security.

US Army Picatinny Arsenal/AlphaInsight

5/2004-8/2005

Network Manager

- Project leader to upgraded Picatinny network for VOIP.
- Provided architecture leadership and support in migrating ATM based core network to MPLS technology across the United States and other countries.
- Project leader for IAVA, a project initiative which provided level of security trust to the local switch port. It involved using the new LAN switch platform and the newer level of IOS code; integration of active directory and e-directory.
- Project Team Leader to monitor Network performance and Anti Virus upgrade in Army network.
- Team leader in providing technical support with critical issues, such as virus attacks, network outages, and in configuring and troubleshooting for groups issues.
- Team leader for Army network monitoring for VOIP and date network security.
- Wireless security implementation.
- Deployed VOIP for Picatinny Arsenal using a Nortel switch solution.

- Architect, migrated, and implemented Picatinny Arsenal to 1GB for all data center servers.
- Architected and implemented Catalyst 6500 LAN switches in four data centers. The magnitude of this project directly imclientcted the network infrastructure throughout the Army Network.
- Proactively involved in creating strategic and tactical designs to provide network connectivity infrastructure for data centers, Army Base Headquarter locations and Distributed Server Farms.
- Interfaced with senior level Management for high level network architecture plans.
- Responsible for lab simulations of all new network infrastructures prior to actual deployment.
- Responsible for running network management Software Comclientny wide, such as TACACS+, CRM 2000, NetCelera and Concord network health.
- Designed and Testing IPv6 in the Army network for IPv6 deployment.

Computer Service Center Inc, 05/1994 – 04/2004

Director of IT Services

- Designed network infrastructure for many clients, like NYPD, Hudson United Bank, ABHCT, Ferrari, Midland Clientrk Boarder of Education, Cliffside Clientrk Board of Education ,B&L.....
- Network security implementation for many clients.
- Redundant service design for clients.
- Installed Cisco Catalyst 6500, 4500, 3750, 3550 and 2950 Switches for many clients.
- Implemented a considerable amount of VPN connections between client sites on 7500/3640/2640 Routers and Microsoft VPN client PPTP.
- Configured and performed troubleshooting for all Internet Security, for Gov. and enterprise comclientnies.
- Implemented the Ferrari North America network, including installation of Cisco 6513 switch, PIX Firewalls, VPN Concentrators and URL Filtering devices.
- Consolidated the Pepsi Corporation network from four buildings to two buildings and relocated their Data Center.
- Designed a network architecture upgrade for Hudson United Bank after the acquisition of 95 branches from First Union in 1998. This involved the redesign all VLANs and the installation of all Internet security, as well as the training of their security administrators.
- Implemented and maintained NYPD network and Internet security from 1994 to 1999.
- Implemented VLAN and ATM links for Cliffside Clientrk Board of Education including six schools and the BoE. Included in this project was the install of all Internet Security mediums including PIX Firewall, URL filtering, and VPN solutions.
- Implemented inter-site links between all schools for the Midland Clientrk Board of Education. Configured internet access for all schools via a connection to the

High School which acted as a main hub. Installed network security with PIX Firewall, URL/Spyware Filter.

- Upgraded Advance Behavioral Health (CT public health agency) for GB data center and VPN for 19 hospitals
- Designed JOBSBL.com network, including Firewall, VPN and Internet Filtering, also enabling their employees to work at home.

Xincon Institute in New Jersey

CCIE Routing/Switching and Security Instructor

- Provided CCIE curriculum, lab scenarios, and consultation.
- Taught numerous CCIE classes with very positive feed back from students.

CCNP, CCSP, Wireless and IPv6 instructor

- Provided CCSP, CCNP curriculum, lab scenarios, and consultation
- Taught CCSP, CCNP, and IPv6 classes with very positive feed back from large number of students.

Hardware:

Very strong knowledge of the following:

- *Catalyst 65XX, 45XX, 55XX, 37XX, 35XX and 29XX switches.*
- *Cisco 26XX, 28XX, 36XX, 37XX, 7200VXR, and 7500 Routers.*
- *MSFC/PFC2, RSM.*
- *Strata-Comm IGX 8400 WAN switches.*
- *10/100/1000 Ethernet hardware.*
- *Frame-Relay, ATM, DWDM, ISDN, Data Compression, and MPLS.*

Software and Routing protocol

Very strong knowledge of the following routing protocols:

- BGP4, OSPF, EIGRP, RIPv2, IS-IS.
- MPLS, NLSP, Multicast.
- Quality of service, VoIP, Video over IP.
- IP/IPX tunneling, VPN.
- DLSW+, ASC+, CRM.
- CEF, DCEF, HSRP, DSCP, and traffic analyzers.
- IPV6

Reference: available upon request

2. a. **Describe HBE's methodology for administrating and maintaining the LENEL system?**

1. PES Remote System Audit and Health Check (with call)

1.1. Remote Audit and Health Check

1.1.1. Lenel PES will be provided, with a broadband link to the OnGuard Enterprise system. Lenel shall dial into the Master Server and each Region to perform the following system maintenance activities:

1.1.1.1. Server maintenance shall include the cleanup of failed transactions within a manageable amount determined by the Supplier (failed transactions not to exceed 15 per dial-in per server). If the number of failed transactions exceeds this amount, it shall be determined that the servers require a more frequent service, or the VAR shall assist in the maintenance of these transactions. Increasing the frequency of the server maintenance shall require a change order to this agreement, with additional costs. Assistance by the VAR will be billed on a Time and Materials basis

1.1.1.2. "To Do" transaction monitoring

1.1.1.3. Hardware events transaction monitoring

1.1.1.4. Verification of Lenel Replicator service and schedule

1.1.1.5. Verification of archive/purge completion per system settings

1.1.1.6. Verification that Legato functionality appears healthy through user interface

1.1.1.6.1. Verification of the Legato element in now way implies liability or support of this configuration

1.1.1.7. Review of error log and event viewer for potential issues, notification and tracking of concerns via the audit log and conference call

1.1.1.8. Verification that scheduled backup occurred

1.1.1.8.1. PES can verify that the backup occurred, but will be unable to test integrity of the backup. It is recommended that this element occur by the VAR or End User no less than once a quarter.

1.1.1.9. Database size monitoring

1.1.1.10. Database integrity check (DBCC)

1.1.1.11. Hard disk and CPU utilization

1.1.1.12. 30 minutes of event monitoring per Region to evaluate erroneous alarm concerns

1.1.2. HBE and Lenel shall perform maintenance and corrective actions, and report to client on all work performed on the schedule allocated by the service.

1.2. Audit Review and Progress Meeting

1.2.1. Following the System Audit (on the same day), Lenel will conduct a (1) hour conference call with HBE and the End User to discuss the findings of the audit. Topics of discussion that are expected, but are not limited to the following:

1.2.1.1. Review of System Audit results
1.2.1.2. Recommended corrective actions based on audit findings
1.2.1.3. Critical or Severe issue notice of items critical to system stability
1.2.1.4. Software development plans, upgrades and updates (bug fixes).
1.2.1.5. Corrective procedures and planning.
1.2.1.6. Hardware specifications and procurement instructions.
1.2.1.7. Software specifications and procurement instructions.
1.2.1.8. System network environment schemas and requirement instructions.
1.2.1.9. Database system layout.
1.2.1.10. Forms design for OnGuard Enterprise system.
1.2.1.11. Credential design for OnGuard Enterprise system based upon criteria from Purchaser conforming to system parameters.
1.2.1.12. Access level configuration for OnGuard Enterprise system.
1.2.1.13. Alarm configuration for OnGuard Enterprise system.
1.2.1.14. Other system configuration instructions, as may be required and applicable.
1.2.1.15. Field controller and/or device configuration instructions.

1.2.2. A detailed audit log and meeting notes will be distributed following the call.

1.2.3. Agenda items may be submitted to the PES Team Leader prior to the call for inclusion as requested.

1.2.4. All technical support issues will be reported to HBE, who will report the issues to Lenel through the standard Lenel Technical Support Channel.

1.2.5. Performance of System Audit activity implies no liability on the part of Lenel for system issues that may arise, in particular system issues or operator error outside of the elements Lenel is auditing.

1.2.6. This contract does not include or imply any Technical Support components outside of standard Lenel channels

1.2.7. PES does not guarantee a single PES technician will perform all audits, which will be determined by scheduling availability. Please see scheduling section for guidelines and important information.

2. Enterprise System Administration

2.1. HBE will provide an Enterprise System Administrator for the client's OnGuard Enterprise system as required during normal business hours, three days per week. The Enterprise Administrator will be the single point of contact to HBE and will assure the continued efficiency of the system, its components, and monitoring including, but not limited to:

2.1.1. A complete survey and inventory of the existing equipment (devices, servers, software, hardware, etc). Any defective equipment, dated software and hardware – i.e. servers - should be clearly identified.

2.1.2. Generate reports to determine system deficiencies. Identify system problems and recommend technical solutions.

2.1.3. Monitor system operator actions and response times. Identify ways to enhance system operator performance, efficiency and accuracy.

2.1.4. Assure component optimization (including camera views, intrusion device locations, etc.). Train security staff to monitor camera views and maintain optimal performance.

2.1.5. Assist security personnel in electronic investigations and audits. Make sure that records retrieval and other investigative activities are being handled consistent with best known practices.

2.1.6. Coordinate system upgrades and fixes.

2.2. Weekly Activities

2.2.1. PIC Data Import. HBE will monitor the import of data from the client database to ensure that the import is successful. Any problems encountered will be reported to the Regional Administrator to be forwarded to the PIC department.

2.2.2. Replication Administration. Replication Administration provides centralized management and configuration of OnGuard Enterprise systems. It is used at facilities to manage the transport of data between the Master Server and the Regional Servers. The System Diagnostic Tool is used to check the status of all the machines involved in the OnGuard Enterprise system. Specific checks to be performed by HBE include, but are not limited to:

2.2.2.1. Replicator service is functioning normally

2.2.2.2. The number of To-do, Hardware, Event and User Transactions and their earliest timestamp

2.2.2.3. The number of Failed, Warning, and Successful Transactions

2.2.2.4. The size of the Database and the Database log file

2.2.2.5. The size of the Logs directory in the OnGuard installation directory

2.2.2.6. Repair and reinitiate failed transactions

2.2.3. Redundancy. Legato 2000 Co-Standby Server is the third party software application utilized to create a mirror image of a server onto another server and then move any and all changes made from the primary machine to the secondary machine. If the primary machine ever fails, Legato 2000 Co-Standby detects the failure and automatically designates the secondary machine as the primary machine. HBE will monitor the Legato Management console to ensure the continued operation of the server cluster.

2.2.4. Replication Administration. Older successful transactions in the replication logs will begin to occupy valuable space on the hard drives. These transactions are a record of the data being replicated between servers, and are not the actual events themselves. HBE will purge older successful transactions from the Replication logs.

2.2.5. Disaster Recovery. Back-ups are often the last defense in recovering lost data or recovery from a failed machine. Backup media must also be verified. SQL may show a successful backup but if the tape is flawed the backup will have no value in disaster recovery. HBE will back up and verify the SQL Server database on all Master and Regional servers according to the schedule recommended by Lenel.

2.2.6. Hard Drive Verification. A full disk can mean a loss of sensitive data and may indicate that back ups need to take place more often. Lenel will monitor the size of the databases as part of the Remote Maintenance agreement and HBE will perform the corrective action as required. HBE will verify that the log files are being archived and purged as intended.

2.2.7. Archive / Purge. This function is considered house-keeping, but if not followed can result in unwanted data taking space within the systems and is normally performed at the master server and regional servers. This is important because these transactions are stored in the database and will occupy hard drive space that is needed for other functions. HBE will perform routine event archive and backup of events to off-line media.

3. Consulting

3.1. Because HBE will be on-site while performing Enterprise Administration, we will also be available to assist the client by performing the role of Security Consultant. The duties of Security Consultant will evolve to meet the changing requirements of the client. These duties are likely to include, but are in no way limited to:

3.1.1. Identify access control areas by category and level of security. Specific concerns relates to the current level of security in the garage.
3.1.2. Assure appropriate electronics and personnel are in place to control & monitor such areas.
3.1.3. Create and implement procedures for authorizing, monitoring and auditing access privileges.
3.1.4. Identify appropriate department personnel to authorize access privileges.
3.1.5. Design and coordinate the routine collection, implementation and reconciliation of access privilege information.
3.1.6. Create appropriate photo identification credential design (with unique identifiers and validation).
3.1.7. Confirm that the existing procedures for authorizing issuance of photo ID reflect best security practices.
3.1.8. Identify appropriate department personnel to authorize photo ID issuance.
3.1.9. Confirm that the existing routine for issuance of photo IDs reflect the best industry practices.
3.1.10. Confirm that existing training of appropriate security personnel in policy and procedure for creating and issuing photo ID is adequate and sufficiently detailed.
3.1.11. Work with Security personnel to create and administer procedures to monitor and respond to electronic security information, notifications and alarms.
3.1.12. Organize appropriate locations, equipment and personnel for monitoring of ACAM systems.
3.1.13. Organize a response plan for each type of notification and alarm that may occur.
3.1.14. Design a communication scheme for the dispatch of personnel.
3.1.15. Design a routine for the timely report generation and notification of appropriate authorities.
3.1.16. Coordinate training for all appropriate security personnel, including other System Administrators.
3.1.17. Work with internal and external maintenance staff to assure the continued operation of the system.
3.1.18. Design and implement periodic testing procedures and documentation. This exercise would prioritize cameras and card readers.
3.1.19. Coordinate periodic maintenance schedules and documentation.
3.1.20. Develop a response plan for failures of field devices and head-end equipment.
3.1.21. Develop a routine for security and non-security personnel to report problems.
3.1.22. Interface with network departments and providers to resolve network problems.
3.1.23. Develop a catastrophic disaster recovery plan in conjunction with some of the client's existing efforts.
3.1.24. Assist in selection of contractors.
3.1.25. Investigate addition of features and components

3.1.26. Oversee project work as appropriate.
3.1.27. Assure integration of new components to existing system.
3.1.28. Update policy and procedure to incorporate expansion.
3.1.29. Evaluate and prioritize expansion projects and areas.
3.1.30. Collect budgetary information for procurement of funding for future projects.
3.1.31. Generate specifications for projects.

2. b. **Describe what industry best practices you will be applying?**

i. See following procedures:
Information Technology Change Management Policy & Procedure
Information Technology Security Policy
Logical System Access Policy
Operations Management Policy

HENRY BROS. ELECTRONICS, INC.
17-01 Pollitt Drive Fair Lawn, NJ 07410
Phone: 201.794.6500 www.hbe-inc.com Fax: 201.794.8341

Information Technology Change Management Policy & Procedure

Title	**Change Management Policy & Procedure**		
Author	Michael Babcock	**Date**	03/16/07
		Revision	1.0
Reviewed	Emil Marone	**Date**	03/23/07

Version Control

Version	Date	Comments
0.1	03/13/07	Initial Draft
1.0	03/23/07	Final Copy

This document to be reviewed and updated as required. At a minimum an annual review will be performed.

Introduction

The purpose of change management is to ensure that standardized methods and procedures are used to alter the production environment while minimizing the risk for negative impact. The specific objectives of applying a change management procedure are to:

- Implement changes on schedule.
- Eliminate or reduce the number of changes that are regressed due to issues without change planning and implementation.
- Provide a back out plan for all changes.

The benefits gained from implementation of a change management procedure are improved system reliability and availability due to control, planning, and testing prior to installation of changes.

Henry Bros. Electronics, Inc.'s changes are mainly focused on infrastructure systems and software that is Commercial off the Shelf (COTS); therefore, the procedures are not as complex as they would be for in-house developed software.

Scope

This policy statement provides direction on the application of change management for systems within the scope of materiality. For the purposes of this policy, change is defined as any alteration to software, database, hardware and operating system affecting data, data structures, or other aspects of the data processing environment and its attached networks.

This policy applies to all employees, temporary employees, contractors, consultants, vendors, and other workers, including workers affiliated with third parties requiring access to Henry Bros. Electronics, Inc.'s information systems at all locations.

These policies address the procedures for Change Management within the Henry Bros. Electronics, Inc. Information Technology (IT) environment (**Key Control IT.C.5.1**). Only those changes that conform to the Change Management process described in this document are authorized for implementation.

Responsibilities

Change Initiator

The Change Initiator is the individual generating the change. Generally this is an individual representing the department with the most to gain from the change.

IT Operations and Business Owners

Information Technology (IT) personnel will implement changes. If cooperation from other departments is necessary, all groups will coordinate the integration in a cooperative fashion. Under no circumstances will any entity integrate new applications into a production environment without the assistance from Information Technology personnel.

The Chief Technical Officer (CTO) assumes responsibility for scheduling and communicating the change to all appropriate work groups and for coordination and execution of changes into the production environment. This includes:

- Ensuring overall compliance with the documented change process (reviewing, modifying, and reporting as needed).
- Serving as the starting and the focal point for the change management process and procedures.
- Monitoring all change requests and plans and ensuring the flow of information.
- Keeping all interested parties informed and communicating changes to the appropriate work groups.
- Requiring proper approval for the change.
- Reviewing all change requests for accuracy and completeness.
- Scheduling and recording all changes.

Change Process

This procedure addresses Change Management within the Henry Bros. Electronics, Inc. IT environment. Only those changes that conform to the Change Management process described in this document are authorized for implementation.

Change Management consists of the following processes:

- Change Initiation.
- Monitoring and Tracking.
- IT Review of Change Request.
- Testing.
- Test Data Approval (End User Acceptance).
- Implementation.
- Controls.
- Reporting.

Change Initiation

Requests for program changes (including patches), system changes, reports, and maintenance (including changes to system software and configurations), infrastructure, and network changes are subject to change management procedures and require a change request form be completed.

The change initiator will complete a Change Control Form (CCF) to be submitted to the CTO or designated IT Manager. See Change Control Form in Attachment A.

Monitor / Track

The CTO or designated IT Manager assumes responsibility for scheduling and communicating changes to all appropriate work groups and for coordination and execution of changes into the production environment. This includes:

- Ensuring overall compliance with the documented change process (reviewing requests for accuracy and completeness, modifying, and reporting).
- Requiring proper approvals for the change.
- Scheduling and recording all changes.
- Monitoring all change requests and plans and facilitating the flow of information.
- Communicating changes, change acceptance/denial, and change schedules to the appropriate work groups.

IT Review of Change Request

- The Chief Technical Officer or designated IT Manager will review all completed control forms for completeness and signoff.

Testing

A testing strategy is developed, and followed for all significant changes in applications and infrastructure technology, which addresses system, integration, and user acceptance-level testing to help ensure that deployed systems operate as intended (**Key Control IT.C.4.1**).

Test Environment

- Testing must be performed in a test environment that is separate from the production environment.
- After successful testing, changes will be staged for user (change initiator, IT, effected department representative) acceptance within the test environment. (NOTE: In some cases, user review and acceptance of unit testing may suffice in lieu of user acceptance testing.)
- Changes will only be implemented into the production environment after user-acceptance.

Test Plans

Test plans include the following information as appropriate:

- Testing Methodology is developed based on Vendor recommendation and documentation.
- Test Data to be used.
- Expected outcomes.
- Task dependencies (cable moves, ID assignment, files relocated, etc.).
- Impact of the change on other scheduled/pending changes.
- Impact of the change on Information Security.

Test Data Approval

End users do not request system changes (hardware, infrastructure, patches) or software changes (upgrades, patches). Upgrades and/or patches affecting financially significant software applications are provided by the software vendor (COTS) and typically are tested by IT based on vendor recommendations (README files) (**Key Control IT.C.4.3, IT.C.4.4**). IT management sign off on test results is required prior to submission for user acceptance testing (UAT), where applicable. In some cases, user review and acceptance of unit testing (IT) may suffice in lieu of user acceptance testing.

End user requests for new/change reports follow the change management process.

Implementation

CTO or designated IT Manager will track and document the implementation process and communicate the results via with stakeholders. Any problems associated with the implementation of changes will be discussed with the appropriate associated users associated with the change.

CTO or designated IT Manager will ensure that:

- Program / application code is backed up prior to change.
- Changes are scheduled.
- Patch maintenance is timely and does not affect normal processing.
- Only authorized/ approved changes are moved into production.
- There is appropriate segregation of duties between the staff responsible for moving a program into production and program development (**Key Control IT.C.5.3**).

Controls

- **Documentation Maintained**

  The CTO will ensure that documents related to the change, including Change Control Forms, test plans, test results, and signoffs are retained.

Version Control

For vendor provided software (COTS) version control is maintained and readily available from the vendor.

The CTO or designated IT Manager ensures that test versions located in the test environment are deleted. This will help ensure that prior versions are not used when future changes are required.

Back Out / Recovery

Back out / Recovery procedures are included in the change request documentation (Change Control Form).

Documentation Updates

Based on change, appropriate documentation for system, application, user, network, and/or configuration settings is updated and retained.

Change Types

All changes fall into one of two types and must follow the change management process:

- Routine.
- Emergency.

Routine Changes

Routine Changes include planned updates and or enhancements to existing hardware or software. These changes follow the change management process and a Change Control Form is completed.

Emergency Changes

Emergency changes may be necessary to recover from system failures, hardware problems, or application problems. Emergency changes provide the flexibility required for the timely response to immediate, critical problems. These problems include fixes to prevent recurring/imminent system failure, negative impact on business, or production problems.

This category has been developed to facilitate unscheduled changes when extenuating circumstances occur and changes need to be made. These circumstances must be documented and follow the Change Management Policy. Signatures at management level will be required (**Key Control IT.C.5.2**).

Emergency changes are made by IT Staff. The IT staff member must document thoroughly the reason for the emergency change, the IT staff member's name, and the date and time of the change.

Emergency changes must be tested and are subject to standard approval procedures after they have been made. Approval must occur within forty-eight (48) hours.

Prior to implementation, back out procedures must be submitted on the Change Control form.

When appropriate, the CTO and business owner should meet to discuss the emergency change. They should analyze why the emergency occurred, how such events can be avoided in the future, and whether the action taken was appropriate.

Any temporary access that was granted to facilitate the change must be terminated.

HENRY BROS. ELECTRONICS, INC.
17-01 Pollitt Drive Fair Lawn, NJ 07410
Phone: 201.794.6500 www.hbe-inc.com Fax: 201.794.8341

Information Technology Security Policy

Title	**IT Security Policy**		
Author	Michael Babcock	**Date**	03/08/2007
		Revision	1.1
Reviewed	Emil Marone, CTO	**Date**	03/16/07

Version Control

Version	Date	Comments
0.1	03/12/07	Initial Draft
1.0	03/16/07	Final Copy
1.1	03/22/07	Updated to include version control table.

This document to be reviewed and updated as required. At a minimum an annual review will be performed.

Introduction

SECURITY OF INFORMATION SYSTEMS

Computer systems are powerful tools that touch upon many aspects of life in modern society. They can be used to enhance quality of life or degrade it. The impact of this effect may range from negligible to the dramatic.

Security of information systems means the protection of the availability, integrity, and confidentiality of information systems. While the growing use of information systems has generated many benefits, it has also shown a widening gap between the need to protect systems and the degree of protection currently in place. All individuals and organizations have a need for proper information system operations. Users must have confidence that information systems will be available and operate as expected without unanticipated failures or problems. Otherwise, the systems and their underlying technologies may not be used to their full potential and further growth and innovation may be prohibited.

PURPOSE

This document contains senior management policy directives for the security of information throughout Henry Bros. Electronics, Inc (**Key Control IT.B.1**). These directives apply to all Henry Bros. Electronics, Inc. sites, regardless of division, geographical region or computing platform. Individual divisions may have more stringent management requirements.

RESPONSIBILITY

All personnel who access or make decisions affecting Henry Bros. Electronics, Inc. information play a role in protecting that information. Accordingly, it is expected that all Henry Bros. Electronics, Inc. employees and agents, including but not limited to full-time employees, part-time employees, temporary employees, contractors, vendors and customers that access Henry Bros. Electronics, Inc. systems, will be held personally accountable for protecting Henry Bros. Electronics, Inc.'s information.

It is the responsibility of every employee who has knowledge of infringement of these policies to notify his or her department director.

COMPLIANCE

Security is very important to the continued health of the business and the maintenance of public trust. While the needs of the business in a particular situation will always determine the appropriateness of any security standard in that situation, non-compliance without valid justification will not be tolerated. All personnel who use, have access to, or are responsible for Henry Bros. Electronics, Inc. information assets must comply with these policies and standards. Violators are subject to disciplinary action, up to and including termination of employment, and legal action.

Security Compliance Review

To ensure observance of the Henry Bros. Electronics, Inc. Information Security Policies, compliance reviews are to be conducted annually. These reviews determine whether The Henry Bros. Electronics, Inc. information assets are satisfactorily protected. They test the effectiveness of business practice, the safeguards implemented for computer systems, and the security features included in application design plans.

Such an audit may be conducted using in-house resources or external parties. The audits may include active attacks against servers, user workstations or other network elements. These attacks may include interception of user communication or feigned communication with users ("social engineering") to trick users into divulging confidential information (passwords).

Security penetration studies involving active attacks or social engineering may only be conducted with the authorization of the Chief Technical Officer. Prior communication of the penetration study to end-users of Information System staff will be at the discretion of the Chief Technical Officer, since prior knowledge may skew the results

Compliance Exceptions

While the needs of the business may determine the appropriateness of a particular information security policy and/or standard, non-compliance without valid justification is unacceptable. Henry Bros. Electronics, Inc. management may deviate from the Henry Bros. Electronics, Inc. Information Security Policies only when:

1. It has been clearly demonstrated that a cost/benefit analysis of the available compliance options and risk of not complying has been performed by the business entity with non compliance.

2. Analysis results indicate that compliance will have a significant and unacceptable business impact.

3. Risk acceptance has been formally approved by the Chief Technical Officer.

Risk Acceptance

Henry Bros. Electronics, Inc. management must formally accept responsibility for all identified risks when deviating from the Henry Bros. Electronics, Inc. Information Security Policies. Risk acceptances must be:

1. Documented by the Business Unit most senior management personnel
2. Approved by Henry Bros. Electronics, Inc. Chief Technical Officer.
3. Maintained on file with the Henry Bros. Electronics, Inc. Chief Technical Officer.

Risk acceptance documentation must include the following information:

- The classification of the information asset(s) at risk.

- A discussion of the compliance options considered and the reason for not complying.
- The risks identified as a result of not complying.
- The estimated cost or operational impact to Henry Bros. Electronics, Inc. if each risk were realized.
- A statement of acknowledgment and acceptance of the identified risks.
- A time period set for periodic review.

General

The Relationship Between Policies and Standards

Having security is a business decision. Attached to any good business decision should be a policy. Security is no different. An information security policy is itself a part of the overall enterprise solution to the security dilemma.

Company Policy communicates management directives which are elaborated more fully in specialised documents such as the IS security policy. A policy is a high level statement of company beliefs, goals, and objectives and the general means for their attainment for a specified subject area.

Information Security Policy contains policies and practices that govern the planning, organization and control of information security. They are management directives that apply to all locations, geographical region or computing platform.

Information Security Standards are a set of best practice criteria for non-specific platforms, applications, technologies and functions. A standard is a mandatory statement of design or implementation. It is also a norm for measurement and, as such, should be restricted to situations where performance to a specific measurement is required.

Specific Implementations includes a set of specific process summaries for general IT process areas.

SECURITY POLICY STATEMENTS

Information Asset Security

Information is a vital business asset of Henry Bros. Electronics, Inc. Information, documents, systems, networks, and applications are considered to be information assets. Inadequate protection or misuse of Company information could give competitors an unfair advantage, lessen the quality of Henry Bros. Electronics, Inc. services, instigate legal conflicts, or otherwise harm Henry Bros. Electronics, Inc.

Policy Statement

It is Henry Bros. Electronics, Inc. policy that all information created, stored, processed, transmitted or printed by or on behalf of Henry Bros. Electronics, Inc. is the property of the Company. This information is an asset of Henry Bros. Electronics, Inc. and all personnel are personally responsible for safeguarding the value, integrity, and confidentiality of Company information assets. All personnel are expected to protect the information assets with which they have been entrusted from unauthorized, deliberate, or accidental:

- Access
- Modification
- Destruction
- Disclosure
- Possession

Access Control

Policy Statement

It is Henry Bros. Electronics, Inc. policy that access to all information assets must be based strictly on business need (i.e., user access must be restricted to those resources required to perform an authorized job function). Applications, networks, systems, and practices must be designed, developed, configured, and maintained so that users have access to sensitive information and tools only as needed in order to perform their jobs. Henry Bros. Electronics, Inc. services that offer customers or vendors' access to Henry Bros. Electronics, Inc. networks, computer systems, and applications must be designed to maintain the availability, confidentiality and integrity of Henry Bros. Electronics, Inc. information assets.

In order to help achieve this objective, *all new systems* and where deemed necessary, Legacy systems must provide an authenticated user ID, access control lists must protect all resources, audit trails must be provided (and themselves protected), and access rights must not be passed to other users to reuse the same items.

Physical access security measures are required to protect against the intentional or accidental intrusion of unauthorized individuals into any area where information assets may be readily accessible.

User Identification and Authentication

User identification and authentication is a process to help ensure security of system resources. Identification is determined through the use of a unique user ID. Authentication is the capability to distinguish and verify the identity of an individual.

Policy Statement

It is Henry Bros. Electronics, Inc. policy that all users must be uniquely identified and authenticated before being granted access to information assets. **(Key Control IT.B.2.1)** Processes must be established for granting, changing and revoking access to information assets on a timely basis. **(Key Control IT.B.2.3)** Such access must be authorized, logged and periodically reviewed **(Key Control IT.B.2.6)**. Procedures must specify the process and approvals needed to obtain initial access to information assets, as well as specific actions to be taken when a user leaves the company, changes status or becomes a suspected security risk.

Each User of multi-user Systems must be assigned a unique User ID. All Information processing and transmittal actions must be traceable to an individual User's System profile and authorized application access privileges.

Assignment of multiple User IDs to a single User for any multi-user System must be authorized and justified in writing by the requester's manager.

All User IDs and passwords must be distributed in a secure manner.

Secret passwords are the minimum approved authentication mechanism that must be used to validate the User's identification.
The following rules apply to *platform* passwords or for applications that do not require authorization through a platform. Exceptions to these rules include legacy systems or platforms that may not allow all of the characteristics required below (Note: a Compliance Exception must be documented and approved).

Required:

-
- (Ex. 4)
-
-
-

Strongly Recommended:

-

(Ex. 4)

(Ex. 4)

Ownership Responsibilities

All personnel who access or make decisions affecting Henry Bros. Electronics, Inc. information assets play a role in protecting those assets. Business organizations use the concept of ownership to designate decision-making authority for specific information. The owner is that individual business unit director or representative of management who has the responsibility for making and communicating judgments and decisions on behalf of the organization with regard to the use, identification, classification, and protection of a specific information asset. (Note: The ownership role should not be confused with legal ownership. All Henry Bros. Electronics, Inc. information assets are the property of the Company.)

Policy Statement

It is Henry Bros. Electronics, Inc. policy that information asset ownership roles and responsibilities be defined and documented. An owner must be designated for each business critical information asset. For purposes of this statement, the information asset is the logical information/data (e.g., Vendor Master, Customer Master, Payroll etc.) that is the intellectual property of Henry Bros. Electronics, Inc.

Management and employee roles with information security responsibilities include, but are not limited to:

- Local IT personnel will have overall custodial responsibility to protect data stored on local computer hardware, responsibility for conformance to all elements of the Henry Bros. Electronics, Inc. Information Technology Security Policy. The Chief Technical Officer will specify who has ultimate authority to grant access and use corporate computing hardware.

- Managers of departments using PCs and other computers in their possession will have direct custodial responsibility for that equipment and data, and will be responsible for conformance to all elements of the Henry Bros. Electronics, Inc. Information Technology Security Policy.

- The local IT personnel are responsible for overseeing the administration and distribution of the Henry Bros. Electronics, Inc. Information Technology Security Policy. The Director will insure that; the local computer system security adheres to the Henry Bros. Electronics, Inc. Security Policy, that reviews are performed as specified, and that only authorized individuals will be allowed access to systems. The Chief Technical Officer will also work with the appropriate personnel to review access controls and act as the focal point for interfacing with external auditors.

- The local IT personnel is responsible for physical security of computer hardware and for availability of computing services as defined in the agreed upon Service Level Agreement Statement. **(Key Control IT.E.1.6)** The computer system will be kept within a physically secure area. Only individuals on computer room access list will be given authority and capability to enter the secure area. The Chief Technical Officer will maintain the computer rooms' access list. An authorized individual must escort all other individuals entering the computer room.

- The local IT Manager is responsible for integrity of databases that they own, and for defining who shall have read and write access to those databases.

Software Distribution and Licensing

Policy Statement

It is a policy of Henry Bros. Electronics, Inc. that all third-party software used will be properly licensed and terms of the license will be complied with. When at work, or when Henry Bros. Electronics, Inc. computing or networking assets are used, copying of software in a manner not consistent with the vendor's license is strictly forbidden. Any unlicensed software must be immediately removed from Henry Bros. Electronics, Inc. computers. All software and documentation owned by Henry Bros. Electronics, Inc. must include appropriate copyright notices.

Backup and Recovery

Back up of data must be accomplished to protect against loss or corruption of operating systems, systems and application. Critical data/systems must be backed up daily. Backups must be sent to an offsite storage facility in the event that they are required for disaster recovery.

Policy Statement

It is Henry Bros. Electronics, Inc. policy that all CONFIDENTIAL, ORGANIZATIONAL, and UNRESTRICTED information resident on computer systems must be periodically backed-up (business critical files must be backed-up daily) to protect the Company from loss of data due to system failures or file corruption. Managers are responsible for establishing organizational requirements for backups (a backup plan) and for monitoring compliance with their requirements. IT Department will provide assistance in planning backup schedules and methods (**Key Control IT.D.2.4**).

Henry Bros. Electronics, Inc. also requires secure on site backup for routine recovery and an archival backup for disaster or long-term recovery. A copy of critical backups must be securely stored offsite.

Certain types of data will need to be backed up more frequently; these decisions must be made on a data-type-by-data-type basis. The specific method to employ for back-ups (grandfather, father, and son rotation for instance) will also be circumstance-dependent.

Physical Security of Computer and Network Resources

Policy Statement

It is Henry Bros. Electronics, Inc. policy that all computer and network resources must be physically and environmentally protected. Access to, computer rooms, and work areas containing critical computer and network resources must be physically restricted. Management responsible for the staff working in these areas must consult the Chief Technical Officer to determine the appropriate access control method (receptionists, metal key locks, magnetic or smart card door locks, etc.).

Minimum Security Standards

The following security standards are a set of best practice information asset protection criteria for non-specific platforms, applications, technologies and functions. Standards and guidelines are rules that must be followed. The topic areas are:

Personnel

Only authorized staff is permitted to use company software and hardware.

Physical Security

Physical access control mechanisms must ensure that access to Henry Bros. Electronics, Inc. areas not intended for public entry is limited to individuals who can demonstrate their authority to enter. Additionally, physical access authority must be revoked immediately if the employee's termination is a result of a conflict between the employee and Henry Bros. Electronics, Inc.

End-User Computing

End Users are responsible for storing critical desk top applications/data and spreadsheets on the File Servers (**Key Control IT. D.4.3**). Information Technology is responsible for the daily back-ups of these files. (**Key Control IT.D.4.2**)

System Integrity and Access Control

IT must implement a system design that provides for prevention, detection, and recovery from security breaches. Management must provide for recovery in the event that physical destruction, logical destruction, or the corruption of operating systems, software or data occurs. Management must ensure that supporting procedures are in place. (**Key Control IT.B.2.4**)

Every financially significant computer/application system must have a designated system administrator. The security administrator must develop and administer forms and procedures to ensure that access is provided according to Henry Bros. Electronics, Inc. policy and standards. The security administrator must also maintain records of access authorization.

Computer Operations

Operations and technical support staff must not have access to data, programs, or operating system information beyond that required to perform their jobs.

Network Security

Network documentation will be developed and kept current. The documentation should include schematics of networks and connections, user documentation, system documentation and configuration, problem reporting procedures and contingency plans, and operations documentation.
Access control mechanisms must be able to create an audit trail, where applicable and feasible, of accesses to objects (e.g.: programs, devices, queries, files, etc.) protected by the mechanism. At a minimum, the audit trail will contain all information necessary to trace an individual event back to the point of entry to the local network serving the protected resource.
Special controls (e.g., firewalls) must be established to safeguard systems connected to public (or shared) networks (e.g., the Internet); especially those extending across organizational boundaries to ensure that computer connections and information flow do not breach the access policy of the business applications.

Internet usage

Non-Henry Bros. Electronics, Inc. External clients or "outsiders" (non-Henry Bros. Electronics, Inc. users) are not permitted access to Henry Bros. Electronics, Inc.'s internal networks unless specifically approved. Under no circumstances should Henry Bros. Electronics, Inc. users establish Internet or other external connections that could allow outsiders to gain access to Henry Bros. Electronics, Inc.'s systems and information. These connections include, but are not limited to, multi-computer file systems, Internet home pages and FTP servers.

Mobile computing

Employees using mobile computing systems, such as laptop computing, will be responsible for taking all possible measures to protect them when they are not secured.

Virus Controls

Window computer systems must be equipped with virus protection. Virus detection software must be installed on each microcomputer (PC), workstation or local area network (LAN), and gateways that processes critical or sensitive information. Virus detection software must be run at regular time intervals to scan files for the possible existence of computer viruses. Employees must not attempt to eradicate computer viruses. If they suspect a virus they must immediately stop using the compute and notify the appropriate personnel.

Third Party Access

Access to Henry Bros. Electronics, Inc. information by third parties must be controlled. Where there is a business need for such third party access, a security risk analysis must be carried out to determine the security implications and control requirements. The controls must be agreed and defined in a contract with the third party.

Service Level Agreements

A Service Level Agreement (SLA) describes in detail the rights and duties of a provider towards a client in the framework of an agreement: it describes who (provider and client) has to execute what, when and where **(Key Control IT.E.1.1)**.
An SLA has to be complete, meaning that everything that is not written in the agreement cannot be claimed either. The exact content of a SLA depends on the context of the contract (internal / external). **(Key Control IT.E.1.4)**.
A SLA reflects the objective elements by which one can measure the "service level", or determine exactly how the provider and the client are (or are not) filling in their essential obligations towards each other. Continuous and detailed service monitoring is necessary. **(Key Control IT.E.1.6)**.

HENRY BROS. ELECTRONICS, INC.
17-01 Pollitt Drive Fair Lawn, NJ 07410
Phone: 201.794.6500 www.hbe-inc.com Fax: 201.794.8341

Logical System Access Policy

Title	**Change Management Policy & Procedure**		
Author	Michael Babcock	**Date**	03/16/07
		Revision	1.0
Reviewed	Emil Marone	**Date**	03/30/07

Version Control

Version	Date	Comments
0.1	03/16/07	Initial Draft
1.0	03/30/07	Final Copy

This document to be reviewed and updated as required. At a minimum an annual review will be performed.

Overview

Approved users (**Key Control IT.B.2.3**) are required to use valid login ids and passwords to access financial reporting systems. (**Key Control IT.B.2.1**) Users must logout of or lock their workstations when they leave their workstation for any length of time. The screen saver wait time is administered through Active Directory. All unused workstations must be logged off outside working hours.

Scope

This procedure covers all Company employees, consultants, agents, and others (collectively, employees) working on any Henry Bros. Electronics, Inc. premises. Logical system access is critical to the security of Henry Bros. Electronics, Inc. systems.

Roles and Responsibilities

The Chief Technology Officer (CTO) has oversight responsibility for the development, administration, and communication of this procedure as it currently exists or any modifications that are made to it. This procedure will be reviewed annually and modifications will be made as required.

General

All employees and subcontractors are to follow Henry Bros. Electronics, Inc.'s *Information Technology Security Policy* when carrying out activities covered in this procedure.

User IDs used in the processing of financial information are unique and enable users to be accountable for transactions. Generic user accounts (including system, shared and / or default accounts) are removed / disabled as appropriate. Where they are required (e.g., system limitations) the use of these accounts is documented and approved by management.

Access Requests (Key Control IT.B.2.3).

New User Requests

New user requests must be made from the appropriate business department. The request contains the Name and role of the new employee. It also contains an existing user to be used as a basis for initial access.

1. A request is made of IT.
2. A request is generated for Tech Support.
3. Tech Support creates the Active Directory User account and adds the user to the appropriate groups (**Key Control IT.B.2.5**).
4. User are assigned a unique User ID (**Key Control IT.B.2.1**) and a temporary password (**Key Control IT.B.2.2**)
5. Tech Support creates the base access rights for production and email accounts. (**Key Control IT.B.2.5**).

Additional Access Requests

Requests for access to additional resources are made to IT. The classification of the data should be used to determine the appropriate approval level for the requests.

1. A request is made of IT.
2. A request is generated for Tech Support.
3. If the appropriate manager responsible for the resources makes the request, access is granted.

4. If another party makes the request, an e-mail request to the responsible manager is sent to verify access.
5. If the request is related to financial data, the vice-presidential level within Finance must approve the request.

System/Interface Access Requests

Requests for system and interface access (applications) are made via requests to the Corporate Finance Group. IT has no role in system and interface user administration. The classification of the data should be used to determine the appropriate approval level for the requests.

1. An email is sent to Corporate Finance Group.
2. The manager responsible for the application must approve the request.
3. A unique username and password are created for each application. **(Key Control IT.B.2.1)**.

Access Removal Requests

Requests for the removal of access are made of IT.

1. A request is made of IT.
2. A request is generated for Tech Support.
3. Removal of access to particular resources needs to be approved by the appropriate manager level.

Termination Requests

Employee Access Termination requests are made to IT.

1. When an employee is removed from the HR System, an request is generated and sent to IT.
2. A request is generated for Tech Support.
3. The employee's Active Directory account is disabled upon notification, for a period of one week when the business identifies where the email is to be forwarded, and then it is deleted.
4. Tech Support notifies the System Administration for removal of other logins and accounts.

Periodic Review of High Privileged Access

IT Management reviews and certifies high privileged and administrator access quarterly **(Key Control IT.B.2.6)**.

For financial significant applications (Timberline), the Corporate Finance Group is responsible for periodic review of user access.

User Authentication

Passwords are used for various purposes at Henry Bros. Electronics, Inc. Some of the more common uses include: user level accounts, financial applications, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Strong passwords should be employed on an enterprise-wide basis.

Strong passwords are required to have the following attributes:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- Are at least eight alphanumeric characters in length.

- Are not a word in any language or slang, and should not appear in a dictionary
- Are not based on personal information, names of family, pets, etc.
- Passwords should never be written down or stored on-line.

Within the Microsoft Active Directory, complex password checking is active. It requires passwords be at least eight characters in length and has three of the following four types of characters:

- Lower case letters
- Upper case letters
- Numbers
- Special Characters

Users are forced to change their first-time passwords, or reset passwords upon initial use.
Users are forced to change their passwords at least every 180 days.

HENRY BROS. ELECTRONICS, INC.
17-01 Pollitt Drive Fair Lawn, NJ 07410
Phone: 201.794.6500 www.hbe-inc.com Fax: 201.794.8341

Operations Management Policy

Title	**Operations Management Policy**		
Author	Michael Babcock	**Date**	03/16/07
		Revision	1.0
Reviewed	Emil Marone	**Date**	04/10/07

Version Control

Version	Date	Comments
0.1	03/27/07	Initial Draft
1.0	04/10/07	Final Copy

This document to be reviewed and updated as required. At a minimum an annual review will be performed.

Problem Management

Overview

Requests for Information Technology (IT) assistance and reports of service problems or interruptions are handled routinely by IT through associated workflow. It is appropriate that standards are set for allocation of priorities to these requests and service problems, and that all problems reported to IT are managed and escalated effectively. This includes critical incidents affecting significant Henry Bros. Electronics, Inc. business functions. This procedure covers problem and critical incident management at all locations.

Purpose

This procedure prescribes how service problems and requests for assistance are managed by IT. It includes guidance for allocating priorities to problems, handling routine problems and requests, and for managing critical incidents.

Scope

This procedure covers all service problems and requests for assistance received by IT staff from all locations. This may include service interruptions notified by system monitoring alerts, and those notified by users of IT facilities. All high, medium, and low service problems will be recorded into the IT problem management tracking system. The goal of problem management is to maintain the highest standard of reliability and availability possible and provide a means to perform statistical trend analysis.

Procedures

General

In the event of an unscheduled problem or outage in the Henry Bros. Electronics, Inc. environment, IT will follow a set of procedures to facilitate quick resolution. These are problem alert, tracking, problem identification and isolation, troubleshooting, notification, escalation, and problem resolution. If timely action or resolution is not found problem escalation will be enforced to ensure that all available resources are utilized in the effort to resolve the problem.

Infrastructure and application system requests for assistance and service problems which are recorded into the problem management system are to include the following information: name of requestor, name of person recording the problem, date and time, problem priority, person assigned to address the problem, responsible manager, description of the problem, and the current status of the problem. There should also be a detailed chronology of the problem resolution from start to finish captured into the Issues List record.

All problem calls will be channeled to the IT person assigned with this responsibility. Calls will be entered into the Issues List record.

A generic email address (MIS Tech Support) is provided to help ensure that requestors may be able to submit requests at any time. In the event that the problem resolution will involve unexpected budget, the Chief Technical Officer (CTO) or appointed designee is to be consulted for approval.

If problem resolution could potentially impact current contract compliance, executive management should be notified so that appropriate action, if required, may be taken.

If any reported incident or problem results in a change to application or infrastructure resources that are required are to be made in accordance with change management policies and procedures.

Quarterly, IT management will review problems for resolution, similarity and reoccurrence. Lessons learned and trends should be noted. Where problems are found to be of a repetitive nature, management will develop an action plan to address the issues found to help minimize problem reoccurrence.

Executive management may determine that, due to the nature of a problem, it may not be responded to in the way that the requestor expects due to events such as system retirement, contractual obligations, legal concerns, customers who have archaic systems or that continue to use releases of the product which are no longer supported, or cost involved.

All trouble reports should be retained to enable root cause analysis.

Configuration Management

System infrastructure, including firewalls, routers, switches, network operating systems, servers, and other related services are properly configured. Configuration standards and settings are documented. Semi-annually, IT reviews configurations of critical systems to ensure compliance to standards.

Changes to configuration settings follow the change management policy and procedure.

Data Backup Procedure

Overview

Henry Bros. Electronics, Inc. recognizes that there is a heavy reliance on the information contained in the Henry Bros. Electronics, Inc. infrastructure and application systems.

Purpose

This document details the procedures followed by the IT staff in executing the data backup of Henry Bros. Electronics, Inc.

Scope

This document applies to the procedures for data backup of all infrastructure and application servers. Files on desktops and laptops will only be backed up if they are copied to an infrastructure or application server.

Types of Backups

DAILY

- Incremental backup - only the files that were changed since the previous backup
- Operated automatically with backup running on Monday - Thursday
- A round of 5 generations is saved (about two weeks)

WEEKLY

- Full backup – All files on the system
- Operated automatically with backup running on Friday
- A round of 8 generations is saved (about two months)

MONTHLY

- Full backup- All files on the system
- Operated automatically with backup running on the last Friday of the month
- Saved for seven years

Backup Tape Handling

Rotation

Backup tapes will be rotated using the table below. D(aily), and W(eekly) are so noted below in the Table Column entitled **Tape Used**.

Week	Day	Tape Used	Storage
1	Monday	MondayD1	On-site in IT Switch/Phone room, inside a fireproof safe.
1	Tuesday	TuesdayD1	
1	Wednesday	WednesdayD1	
1	Thursday	ThursdayD1	
1	Friday	FridayW1	Off-Site
2	Monday	MondayD2	On-site in IT Switch/Phone room, inside a fireproof safe.
2	Tuesday	TuesdayD2	
2	Wednesday	WednesdayD2	
2	Thursday	ThursdayD2	
2	Friday	FridayW2	Off-Site
3	Monday	MondayD1	On-site in IT Switch/Phone room, inside a fireproof safe.
3	Tuesday	TuesdayD1	
3	Wednesday	WednesdayD1	
3	Thursday	ThursdayD1	
3	Friday	FridayW3	Off-Site
4	Monday	MondayD2	On-site in IT Switch/Phone room, inside a fireproof safe.
4	Tuesday	TuesdayD2	
4	Wednesday	WednesdayD2	
4	Thursday	ThursdayD2	
4	Friday	Month	Off-Site

When there are five weeks in the month, on the fourth Friday use Friday 4. On the fifth Friday, use the Month tape and store it off-site

Backup Monitoring

Errors notices (e.g. failed backups, incomplete backups) are auto generated from the backup management software and emailed to the IT Manager for review, logging in the problem management system, and action defined.

Tape Labeling

The backup management software provides a system generate log of tape inventory

On-site Storage

Tapes will be removed from the tape library as early as feasible Monday morning and moved to the fireproof safe, located in the IT Switch/Phone room. Access to backup tapes will be limited to the Henry Bros. Electronics, Inc. IT staff. Tapes will be available 7/24 for restore purposes

Off-Site Storage

All movement of tapes will be logged. The off-site vendor courier will log tapes in and out of the facility. The courier must sign for all tapes and a record must be kept which will include a list of all tapes located off-site. In addition, Henry Bros. Electronics, Inc. should ensure that the vehicle used by the off-site storage provider to transport tapes is locked when in the Henry Bros. Electronics, Inc. parking lot and the courier is not present at the truck. Off-site tapes will be available within a four hour notice seven days a week.

All employees who are authorized to request tapes to be returned to Henry Bros. Electronics, Inc. from the off-site storage vendor will be provided a list of authorized IT personnel who can authorize or request a tape transfer. The contract with the offsite storage vendor should explicitly state who is authorized to request tapes, how tapes will be transported to and stored at the off-site location, and the process to follow to request a tape from the offsite storage vendor.

No one is permitted to take any tapes to their place of residence or other offsite location without the express permission of executive management and a backup of the tape secured on-site.

Testing of backup media quality

HBE Inc periodically tests the integrity of the backup media. On a semi-annual basis, selected files are restored to servers to ensure that the backups are being performed correctly and on viable media. Additionally, IT will respond to ad hoc user requests, identified in the problem management system, for database or data file restores. Successful resolution of these requests ensures that the backup media is recoverable.

Data Center environmental and physical security

HBE Inc has one centralized data center. The data center is protected by the following automatic environmental controls:

HVAC – air conditioning, humidity control and ventilation is in place to ensure proper operating conditions. Temperature and humidity are monitored electronically. Error conditions/alerts are configured to alert administrators upon detection.

Fire Suppression – the fire suppression system is monitored electronically. Error conditions/alerts are configured to alert administrators upon detection. Should there be a discharge, IT Operations will be informed of the discharge as will Engineering and Maintenance.

UPS – Uninterrupted Power Supplies provide power to all servers, routers and switches in the data center in the event of a power outage, and provide for an orderly unattended shut down of all servers.

Access to the Data Center is controlled by keycard and on power failure by key lock to authorized and trusted persons either permanently (employees) or temporarily (visiting vendors/technicians). In all other cases an authorized employee will accompany visiting persons at all times while they are in the data center. Access to the data center is authorized and approved by the CTO. The CTO maintains a listing of authorized users. The CTO reviews the approved access list semi-annually to ensure accuracy.

4. **In the presentation HBE explained that each preventive maintenance routine is performed four times in a calendar year. Please confirm this in writing and please provide schedule.**

HBE will perform Preventive Maintenance (PM) for each system component once per quarter or four times per year.

5. **Does HBE understand the response and repair times for Type I (2 hours) and Type II (3 hours) failures? Are there any scenarios under which HBE may not be able to comply with these performance requirements? If so, what are they and how will they be addressed.**

As discussed during the HBE presentation on Thursday, July 12th, there are conditions that could impact HBE's ability to respond and repair in the times frames noted in the RFP. Some of the conditions that HBE has encountered in servicing the Access Control and CCTV systems at the Port Authority airports are:

Severe weather conditions

Severe weather make some areas inaccessible. In extreme cases Police may discourage any non-critical vehicle travel.

Power outages

In the past three years LaGuardia Airport has had to deal with both the large NYC Blackout and the localized Queens outage that affected half of the airport. In both of these cases HBE responded well within the two hour time frame however the resolution time frame was out of our control.

Severe traffic issues

Movement around and through NYC is subject to unexpected problems that can make crossing the Hudson River nearly impossible. HBE maintains offices and Service Technicians on both sides of the Hudson and should be able to minimize the effects of severe traffic conditions.

Third Party Actions

We have had to respond to a contractor's backhoe digging through a fiber network at one of the airports. In another instance a vehicle into an equipment cabinet. Again HBE responded quickly however there were a number of factors that had to be resolved (many outside of HBE's control) before a resolution could be deployed.

Work Stoppages/Labor Actions

Third party work actions can adversely affect movement and access.

Manufacturers Product Support

Manufacturers of security technology hardware and software can have limits to their Product Support plans or, in some cases, have changed the type of support offered. Of course, products that extend beyond the manufacturer's support time cannot be held to any repair parameters. HBE maintains a high level of support with the primary software/equipment manufacturer's applicable to these sites. We also maintain a file of direct connect phone numbers beyond the published support lines.

Other cases

There are many other instances where the resolution of a problem could extend beyond the listed time frame, however, HBE pledges to respond in the required time as long as there is access to the facility. Further, as we have demonstrated at the airports, we will work along with PA personnel to resolve the issues in the quickest time possible.

HENRY BROS. ELECTRONICS, INC.

perfecting security integration **since 1950**

A brief history of Henry Bros. 1950 to present

Founded as an Electronic Repair Shop by John Henry and his brothers Ray and Hank

Selected by Motorola as a Motorola Service Shop (MSS) based on their solid reputation for service and system integration

CGI acquires Henry Bros. for their communications expertise

Jim Henry, son of founder John Henry, leads buyback of the integration business and focuses on communications and security integration

HBE buys the assets of the old Motorola CCTV factory in Carol Stream, Illinois

HBE makes first regional acquisition with the purchase of the Dallas division of Ogden Allied

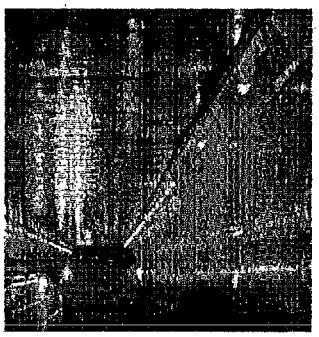
HBE issues an IPO and goes public as DSSI on AMEX

From 2002 to 2006 HBE acquires established security integrators in California, Arizona, Colorado and DC Metro to provide a national footprint

HBE acquires assets of Aerocomm (now Airorlite) and important public agency contracts from GFCI

DSSI division started to develop Emergency Action Plans and related services in NYC

our focus on vertical markets



WHO WE WORK FOR

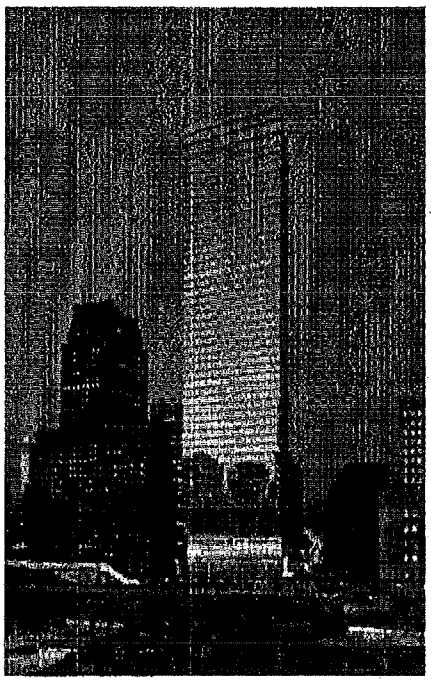
Henry Bros. counts among clients some of the most high profile real estate management, Fortune 500 companies and public transportation agencies. All come to HBE for our unique approach to integrating all facets of security into a single, comprehensive, seamless solution.

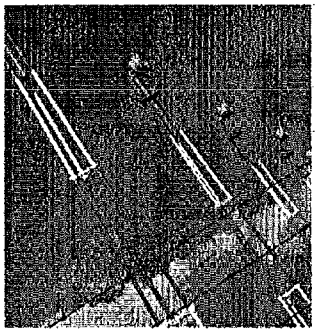
Security Consulting Firms • Engineering Firms

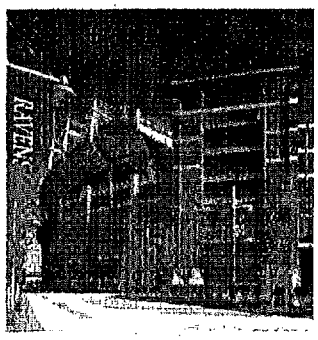
Hospitals • Transportation & Public Agencies

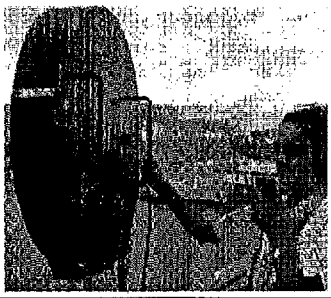
Pharmaceutical • Real Estate Management

Arenas • Education









security integration today: a technology-driven market

COMBINING TRADITIONAL SECURITY INTEGRATION WITH FAST EVOLVING TECHNOLOGIES

Henry Bros. goal is to offer the most comprehensive security integration, which includes both the tried and true 'traditional' security technologies like CCTV surveillance, access control and voice & data, but also state-of-the-art, evolving technologies like digital video recording, enterprise-level deployments, LAN/WAN convergence and wireless solutions.

range of capabilities

PROJECT MANAGEMENT

In addition to our experience installing and providing electronic security systems, we also recognize the need for a local "one point of contact" to serve the customer. Our company, unlike much of the competition, has internal policies and procedures specifically addressing the duties and responsibilities of our Project Managers/Engineers, who have overall responsibility for fulfilling the requirements of the contract. Utilizing the Frontline Project Management Program, our Project Managers/Engineers are capable of coordinating projects of any size by following the blueprint of the project. This ensures that the appropriate steps are taken on every job to guarantee a successful installation.

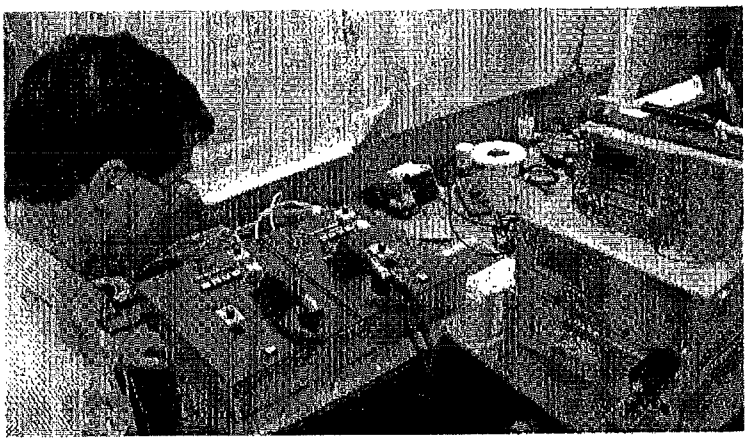
Our coordinated Project Management/Engineering Teams have completed numerous jobs utilizing a variety of technologies. Having a pool of capable Project Managers affords us a great deal of flexibility in the assignment of a Project Manager to a job, basing the decision on workload, availability, experience with specific technologies, and customer needs. Key personnel are available on a 24/7 basis.

DESIGN ENGINEERING

HBE's Design Engineering Team has completed projects ranging in size from simple Card Reader systems to complex, multi site, redundant, real time systems combining Access Control with perimeter detection, CCTV and badging, to provide the end user with the most state of the art intrusion detection system available on the market. By servicing a variety of industries including transportation, industrial, commercial, nuclear and institutional, our Project Managers/Engineers have been exposed to a wide range of industry-standard requirements and have the experience of navigating those requirements to aid the end user through the process and provide a sense of control and confidence. The end result is a quality, stress-free installation.

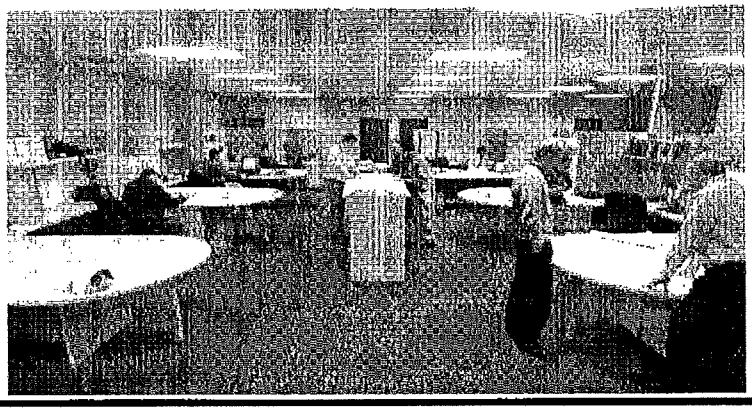
INSTALLATION, MAINTENANCE & STAFFING

HBE has the capability and bandwidth to accommodate virtually any size project - including initial installation, ongoing maintenance and upgrades and full 24/7 staffing, all adaptable to your changing security needs. Our experience with large Prime contractors as well as building trades and IT VARs give our customers scaleable and flexible solutions.

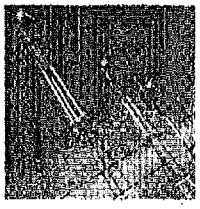


SERVICE

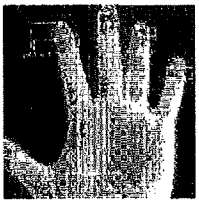
HBE recognized that the consistent delivery of superior service requires the careful design and execution of a whole system of activities that includes people, technology, and processes. HBE offers various levels of service contracts ranging from normal business hours Monday to Friday to 24/7 service with a response time of 4 hours. Our clients feel very comfortable with our service department and they have an extra level of ease knowing that they have regular access to senior level executives.



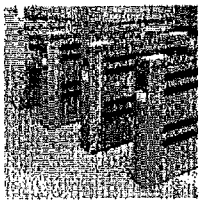
bringing it all together



Perimeter Sensors



Biometrics

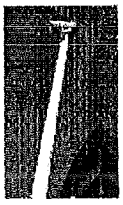


Access Control

Egress C

Radar

the Henry Bros. security matrix

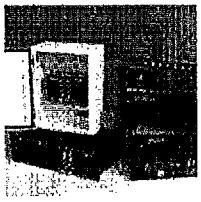


Video & Ar

Video Servers

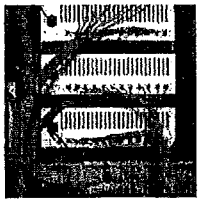
Emerge
Communic

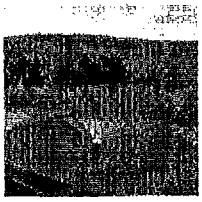
whatever you need, wherever you need it



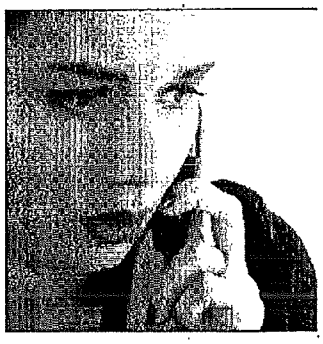
Wireless
Communications

Comma
Contr





the broadest scope of security enabling services



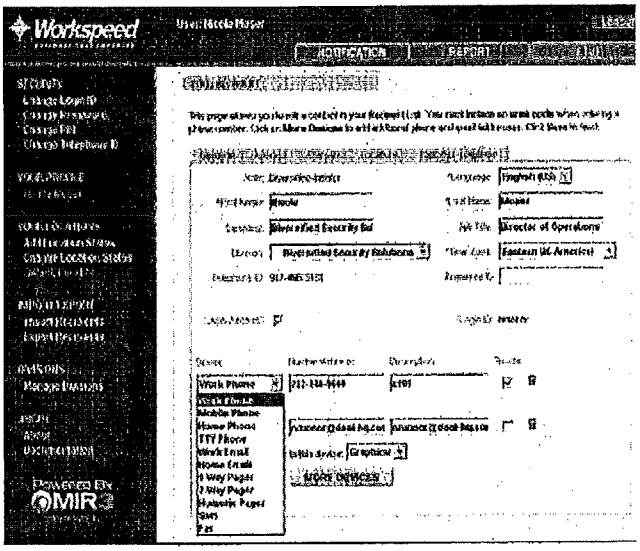
From developing tactical-level first response solutions to facilitating strategic emergency preparedness policies, HBE subsidiary Diversified Security Solutions, Inc. (DSSI) tailors workable products to clients' needs. Our team of experienced public and private consultants has years of expertise in providing objective, realistic security and emergency action plans to our growing clientele. Our exceptional dedication, expertise, and attention to detail make us the preference for clients who depend on excellence.

EMERGENCY ACTION PLANS

No plan is complete without validation and practice. Our exercise programs cover the spectrum of plan coordination and training, including tabletop exercises, walk-thru rehearsals and evaluated drills.

Using development guidelines such as those found in the U.S. Office for Domestic Preparedness Homeland Security Exercise and Evaluation Program; the Federal Emergency Management Agency exercise guidelines; and local and state policies for exercise development and evaluation, we create interactive and realistic scenarios tailored to customer requirements. Emergency notification systems are also available for integration with these plans, providing a seamless interface for business continuity.

Half and Full Day Workshops are available, covering, planning principles and considerations, plan components, situational awareness, risk and hazard assessment, agency interaction, exercise development/delivery and strategic preparedness development.



EMERGENCY NOTIFICATION SYSTEMS

Workspeed Notify from DSSI is the simplest, most powerful solution for instantaneous two-way emergency group communications.

Workspeed Notify is an emergency notification tool designed to deliver any message almost instantly to thousands of people via cell phones, pagers, email, sms, text messaging, Blackberries, fax machines, etc. This electronic system also allows recipients to respond using any of these devices and then automatically generates a report of responses. And because it is web-based, there is no need for hardware infrastructure or software installation on your end. This unique ability to broadcast an alert via a number of delivery methods provides far reaching applicability whether for corporations, universities or hi-rise building emergency action plans.

total security integration: the HBE family of companies

HBE
Henry Bros. Electronics, Inc.

HBE designs, deploys, commissions and maintains technology based electronic security and control systems for a wide range of public agencies and commercial enterprises.

Within HBE, there are three specialized divisions that enable us to address evolving systems integration needs of our customers. We provide action plans and notification programs through DSSI; mobile digital recording solutions through Viscom and specialized radio frequency communication equipment through Airorlite. Together, all of HBE's divisions work to enhance, broaden and differentiate our systems integration expertise and customer experience.

security integration

DSSI
Diversified Security Solutions, Inc.

HBE subsidiary Diversified Security Solutions, Inc. has emerged as a leader in all-hazard emergency preparedness planning for hi-rise buildings. While many companies are capable of developing building emergency response plans, Diversified Security Solutions offers a unique process which involves building staff, tenants, and external agencies in the planning process itself.

Designed specifically for each building, our facilitated program of planned meetings and exercises produce understandable and executable response plans. Once the process is complete, building staffs "own" their plan.

emergency preparedness planning

VISCOM
Viscom Products Inc.

HBE subsidiary Viscom Products Inc. provides ruggedized mobile digital video recording and wireless downloading capabilities for transit authorities across the country. Viscom has a Mobile DVR installed base of over 1000 systems, with over 30% having wireless capabilities.

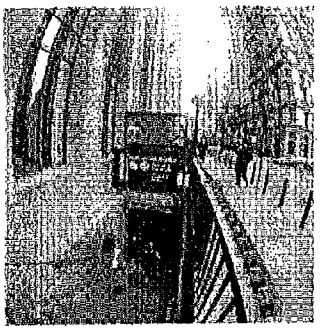
Viscom's clients include such transit authorities as Denver RTD, San Francisco Municipal Railway (Light Rail Fleet) and Santa Clara Valley Transit Authority.

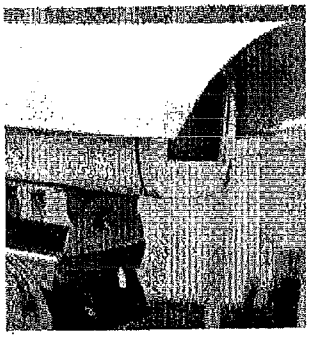
AIRORLITE
Airorlite Communications Inc.

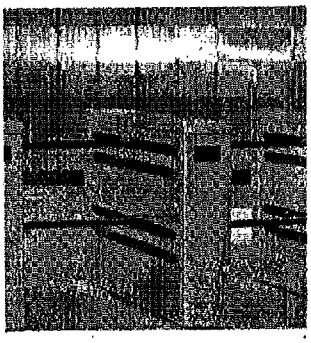
Need Emergency Communications in hard to reach locations? HBE subsidiary Airorlite Communications, Inc. designs and manufactures products to improve the quality, reliability and performance of wireless networks. Airorlite's engineers have been recruited from leading radio, fiber-optic, security and wireless product companies and provide expertise in all aspects of radio frequency systems, hardware and integrated software.

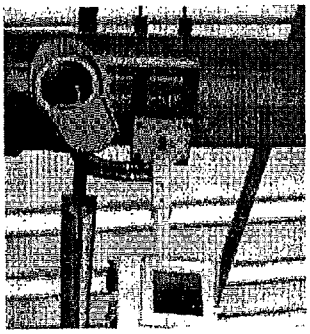
Airorlite has designed and installed communication systems for NYC's Queens, Midtown, Brooklyn Battery, Lincoln and Holland Tunnels; World Trade Center; PATH trains; LaGuardia Airport; Boston's Ted Williams Tunnel; Mercer & Mt. Baker Tunnels in Seattle, WA; and Virginia's Hampton Tunnel.

established security industry relationships









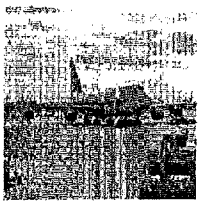
In a business climate that demands flexibility, coordination and customization, companies are finding their partner and supplier networks to be critical in providing successful solutions to customers. Our established relationships with suppliers, contractors and other integrators including government prime contractors has been a critical success factor for Henry Bros.

While we have developed a national footprint to service customers nationwide we also have a well developed network of associates with similar security competencies. Henry Bros. is a founding member of the PSA Security Network, the world's largest electronic security cooperative. The PSA Network includes more than 200 electronic security systems integrators, and over 200 manufacturing vendor partners. Together, PSA members are responsible for over $1.4 billion in annual security systems design, installation, integration and maintenance of access control, video surveillance, intrusion detection, fire, and life safety systems.

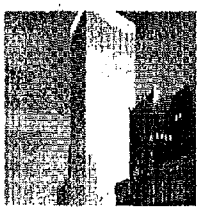
On the supplier front, Henry Bros. long standing successful relationships with Manufacturers and Business Partners include the leading innovators in today's security industry:

AD American Dynamics
cernium
group 4 Securitas
ifs International Fiber Systems Incorporated
likegami
Security and Safety
HID Corporation
LEVEL
SENTROL
SONY
TOSHIBA
RAE Systems
VICON Motion Systems
NICE
NVT
Panasonic
PELCO
VIDIENT
ULTRASCAN
INTELLIKEY Corporation
SmartSight
bioscrypt
WREN
zenitel
MARCH
BroadWare
DEDICATED MICROS
AXSYS Technologies
BARCO
Canon
DVTEL
DynaPel
GE
ioy
INTERGRAPH
MAGAL Security Systems Ltd.
PRAETORIAN
PROXIMEX
OV Object Video
VERINT
BOSCH
Cisco Systems
RSUS

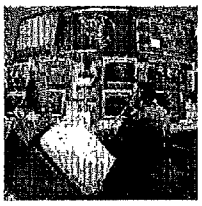
selected marquis projects



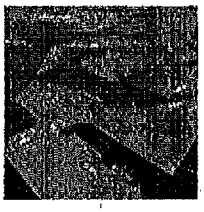
NY Metro Transportation Projects



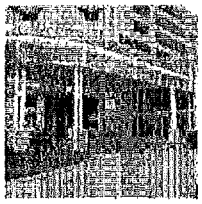
7 World Trade Center Silverstein Properties



Classified DOD Projects



Port of Long Beach

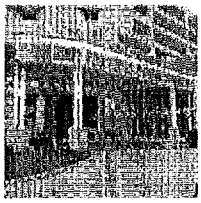


Parsons Engineering Global Deployment

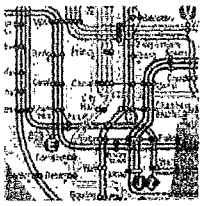
building a national footprint

HBE locations in eight states

Dept. of Homeland Security



Dallas Children's Hospital



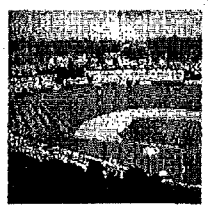
NY Metro Rail Programs

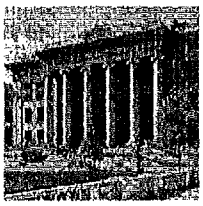
Arizona State University

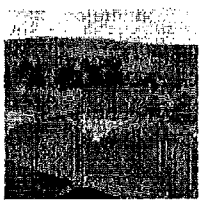
across all sectors

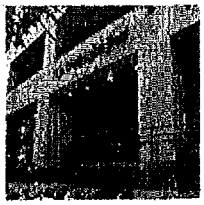
government commercial institutional public

Watson Pharmaceutical

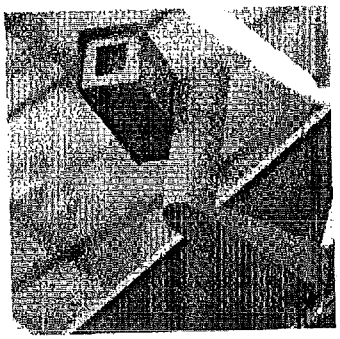






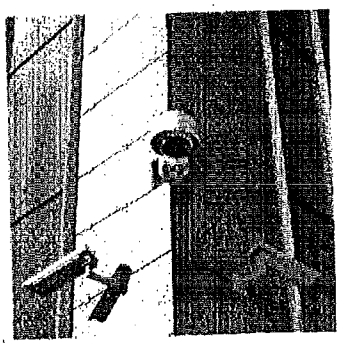


video surveillance systems



HBE provides customized video surveillance and Closed Circuit Television (CCTV) solutions so clients can monitor and record activity occurring at both local and remote facilities.

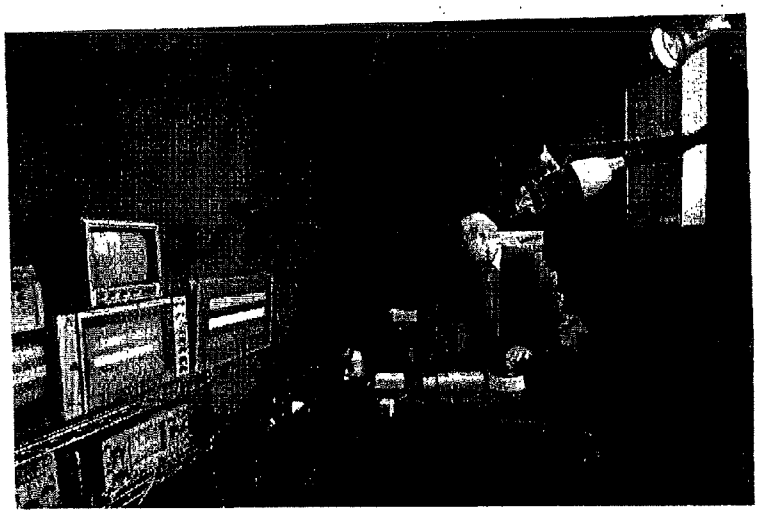
Modern camera technology now enables us to record high-quality images in virtually any type of lighting, so incidents can be monitored and accurately recorded at a facility at all hours, under all conditions.



To this end, every video camera deployed into the field is tested and calibrated in our custom-designed 'Low Light Video Lab'. This one-of-a-kind, state-of-the-art testing facility at our Fair Lawn, NJ headquarters provides us with the ability to measure the video quality and performance of cameras from many manufacturers, under many different controlled lighting conditions. For example, we can test a camera under high-pressure sodium light, halide light or fluorescent light and determine precisely which camera will function best in the type and level of light of the actual installation.

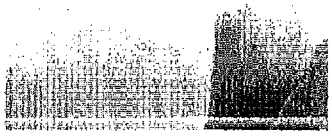
Furthermore, today's high-capacity digital video recording systems eliminate the drawbacks of previous tape-based recording systems. For example, it's now possible to view just-recorded video without interrupting the recording process, which has not been possible with non-digital VHS cassette recorders. Digital video systems also provide password-protected network access to live and recorded video for computer workstations, which allow multiple operators, even at different locations, to simultaneously view different portions of recorded video.

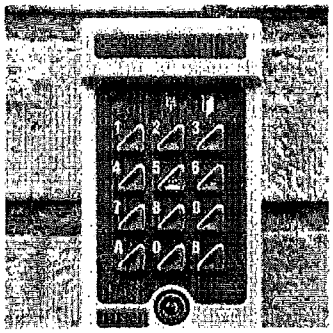
Another technology we have expertise in is 'alarm-based video recording', which begins recording when an alarm or other signal is received. This means that cameras at building entry and exit doors can be activated either by motion detectors or by smart video recording systems that can detect motion. This eliminates recording many hours of "dead time", and speeds the review of video since only actual activity is recorded.



Other advanced video technologies we employ include facial recognition, subject tracking, public area video image display ("Have you seen this person?") and transmission to printers as well as to security officer hand-held display devices. We continue to review and provide input to the video analytic suppliers. We see this as an emerging technology that when fully developed will result in outstanding ROI for our customers from both a financial and operational standpoint.

access control systems & perimeter detection



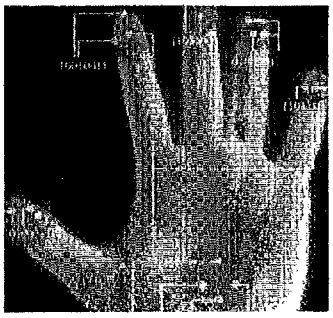


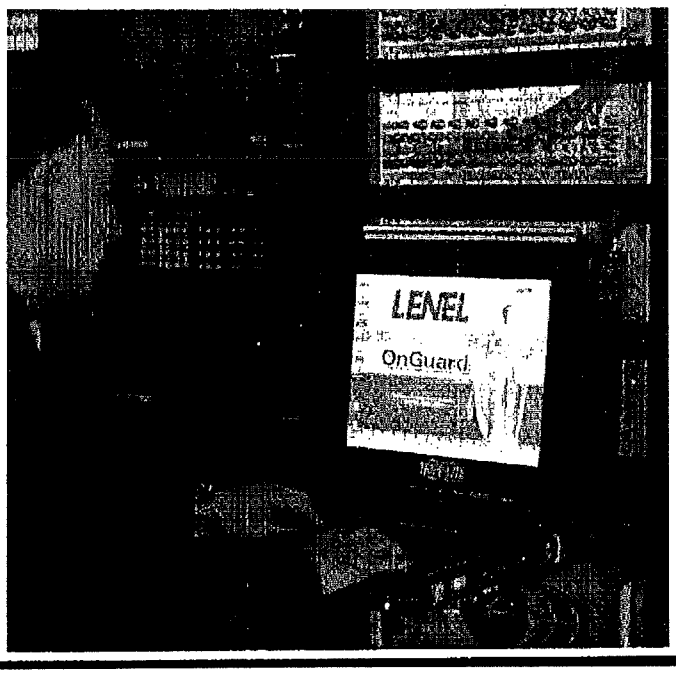
The range of access control systems starts with simple key pad and magnetic stripe locking devices progressing up to sophisticated software database-driven systems used over local and wide area networks and can incorporate biometrics, smart cards and radio frequency identification that integrate with video surveillance systems. Henry Brothers has successfully deployed this full range of access control systems, in both large and small, public and private applications.

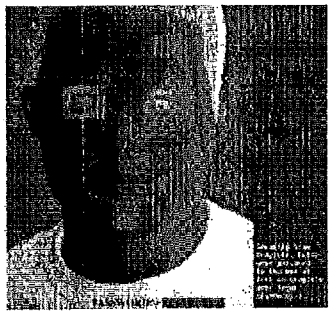
The access control systems we design are completely customizable to your needs, offering flexible control over users' access rights. For example, all staff can gain access through the main door of a building, but access to internal areas may be restricted to those who have a specific need to be there. Access may also be restricted by time, only granting access to particular users at certain times of day or night.

Henry Brothers represents the most highly regarded access control manufacturers, including:

- Lenel
- AMAG
- Cask-Rusco
- HID
- Brivo
- Kantech
- Enterprise Air

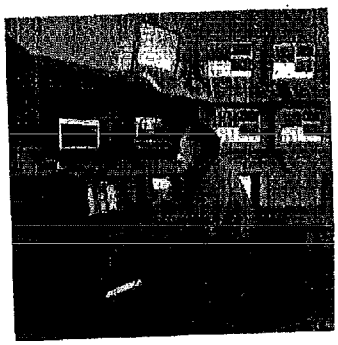




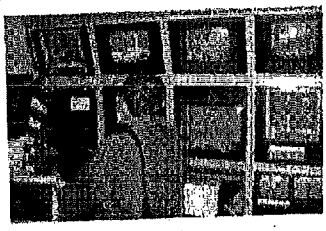


command & control centers

The visualization and access of security related information is central to an effective integrated security solution. These are not just about audio visual components being installed in a conference room or central viewing point. Command and control centers are the nerve center for providing critical information to security stakeholders and to protecting people, assets and facilities. Henry Bros. brings unique set of experience and capability to ensure that your command and control solution is integrated with the appropriate visualization and video products tied together with software and hardware for the access control, surveillance and emergency communications subsystems.

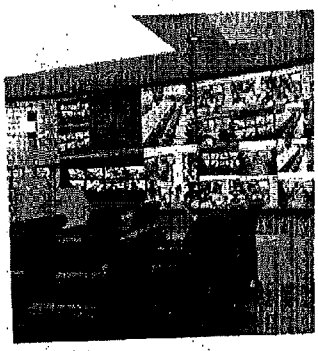


- Years of security specific experience with video and related products including single and multi-monitor systems, video walls and projection systems tailored to command and control and security applications.

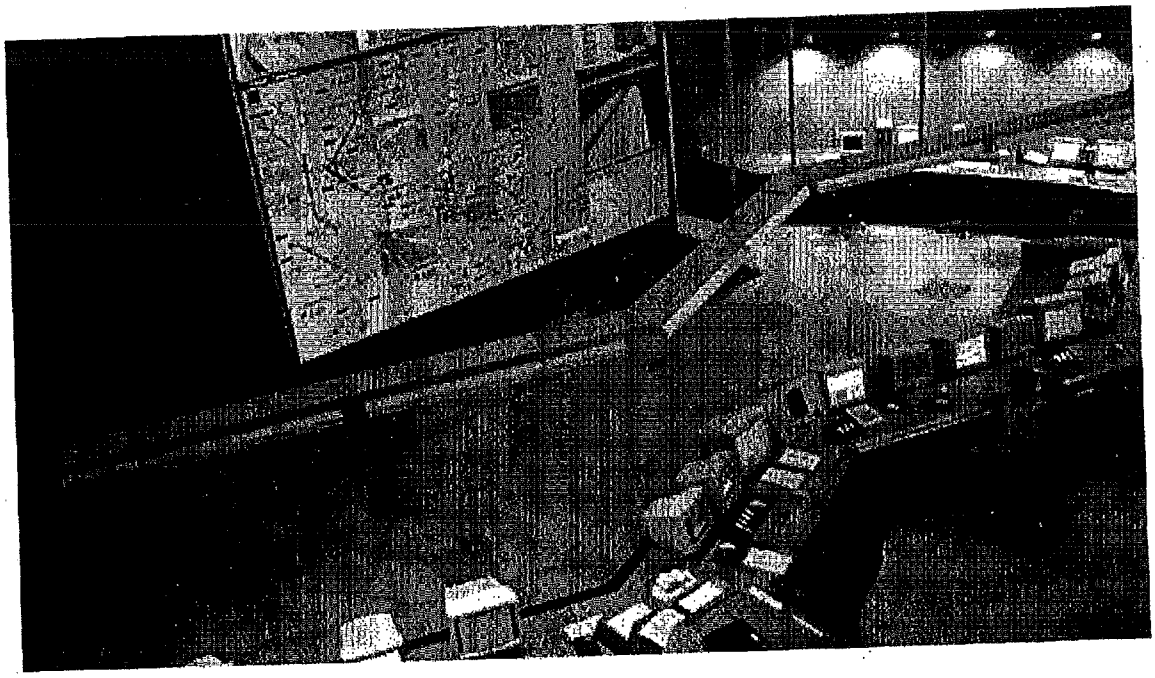


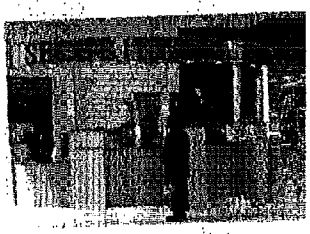
- Intimate involvement with the access and surveillance systems that will be channeled into an command center including appropriate hardware selection and installation as well unrivaled experience with the integrated and discreet software platforms that brings the information to users.

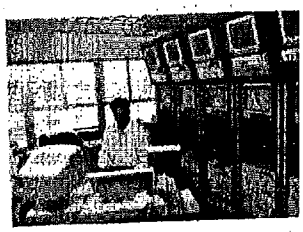
- Specialty communications products that add vital capability in supplying and monitoring emergency communications, cellular and egress control systems.



- Integration teams that have the video, access control, surveillance and emergency communications experience and training to tie all the disparate systems required into a seamless integrated visualization solution.







selected projects

COMMERCIAL

7 World Trade Center - Tishman Construction & Silverstein Properties

Description: Construction contract for the installation of a Lenel OnGuard Access Control, ID Badging System, Visitor Management, Pelco Endura Network based digital video recording system; Cisco Ethernet based Fiber Optic LAN Network, and In-Building Wireless Antenna System.

Features include:
- Installation of Lenel OnGuard Pro system with NEC Fault Tolerant Server
- 85 Bioscrypt V-Smart iClass card readers.
- Over 700 Alarm Points
- Pelco Endura Network Video System with 57.6 TB storage
- 185 Cameras with ip video encoders
- 8 custom-fabricated turnstile lanes
- 12 message boards to allow for notification signs

C

Tysons Corner Center - McLean, Virginia (Macerich Properties)

Description: Major video surveillance system add-on/installation for the T Corner Center in Mclean, Virginia. Cameras are controlled via a Pelco 97 density Matrix Switcher interfaced with a Lenel digital video recording sol new customer service and security kiosk designed and built to promote s awareness. Stentofon emergency customer call boxes have been installe the new garage areas and interface with the Lenel and Pelco systems to matically call up associated cameras and archive any events upon activa

- Total of 105 cameras and digital recorders were added the existing Lenel and Pelco video management system for a total of 260 cameras
- Video is transmitted via fiber optic backbone throughout the 2.2 million square foot property

COMMERCIAL

Beaver Creek Ski Resort - Beaver Creek, CO

Description: Exclusive ski resort and gated community in the Colorado mountains. Controlled access for residents and ski buses through six gates, including Transcore long-range transponders, using windshield tags and access cards, connected to an AMAG access control system. Some gates were configured to stand alone, while
others are connected to the central AMAG system over the customer's LAN. An example of reliable, high-speed access in an extremely harsh environment.

Features:
- AMAG Access Control System
- Six remote controlled gates, including Transcore long-range transponders, using windshield tags and access cards

Colonial Williamsburg

Description: design and install a rebroadcast system for the 38 building complex at Colonial Williamsburg Foundation (CWF). CWF needed better coverage to attract high profile events such as Congressional meetings a stay competitive with other area attractions. Airorlite utilized its modular Building-Linc system providing in-building coverage for:

Features:
- UHF channelized (4channels) full duplex
- Communications for emergency services plus maintenance channels
- Cellular wireless service for all cellular carriers in the area (5)
- SMR service which covers Nextel and the Fire Department's trunked 800 MHz system
- PCS services providing 3G service for Blackberries

ARENAS

Staples Center Arena - Los Angeles, CA

At the Staples Center and soon to opened LA Live, we deployed a cutting edge system for the cultural and sports center of the revitalized Downtown LA. With strategic partner AEG and our enterprise system experience from other arenas like Galen Arena, Dodger Stadium, Toyota and Home Depot Centers, we've built a strong practice around arena security. Staples and LA Live will include:

- Enterprise-wide integrated video and access with hundreds of cameras and readers tied in to 20TB of storage and an integrated visitor management system
- Design-build plans to triple sensor and server capacity facilitated by the proven architecture of the access platform selected and already deployed at sister locations
- System flexibility suits the multi use character of one of the largest urban development sites in the US.

H

St. Joseph Hospital - Orange, CA

Description: Lenel Fully Integrated Access Control and Video running on Hospital Wan and Detected Security Lan. System is deployed on a 14 bui campus with an additional 3 buildings by Spring 2009. Video Recording I Encoders on a 40TB Storage System.

Installation included 221 cameras Indoor/outdoor, 441 HID Prox Readers 35,000 Card Holders.

Features:
- Infant Tagging System
- Wireless Alarms
- Radionics Receiver with off-site Mounting
- Photo ID Badging

selected projects

EDUCATION

Arizona State University - all campuses

Description: Named the ISAAC (Integrated System for ASU Access Control) this system controls more than 1500 doors and alarm points and has over 300 security cameras on a secure VLAN server system supported as an enterprise system.

This system is used in all new or remodeled buildings as the standard system in Capital Projects and the design specifications are supported by our ASU Facilities, UTO, DataComm, University Business Services, Residential Life, Engineering, WP Carey, CLAS, and many others who run this in a distributed management system on 1 secure network.

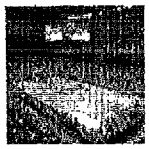
This system uses the iCLASS chip on the card and has capabilities for 2 or 3 factor authentication, biometrics, intelligent video analytics and alarm monitoring both internally by ASU or to outsourced vendors.

EDUCATIC

University of Southern California (USC)

Description : Multiple construction projects over three years including parking structures, sporting arena, lecture halls, student dormitories, computer Building. Systems include of Lenel Onguard Pro Access Control with Integrated LNVR Digital Video with Storage on a distributed Network.

Features include:
- Lenel Onguard Pro on NEC Fault Tolerant Server
- 550 Card Readers
- 2000+ Alarm Points
- 250 Cameras on IP Encoders including Pan/Tilt/Zoom Units
- 100+ Custom AV Integrated Lecture Halls
- IP Emergency Phones Integrated with Lenel systems

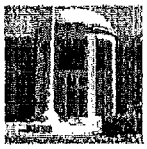


GOVERNMENT

US Post Office - Arlington, VA

Description: renovation and redevelopment of a US Post Office with underground parking. A total video solution utilizing Vicom Matrix Switchers, DVRjs and 64 cameras were installed. Access control and ID badging is via a Lenel ADV series system. The main garage entry includes a Long Range card reader and active cards enabling the USPS vehicles to be automatically recognized and the gate raised.

The other side of the property is a mixed use (High End Condos and Retail Condos) with underground parking. Video cameras provide entrance protection, telephone entry systems cover 3 entrances, plus access control, badging and video recording.



Features:
- 64 video cameras
- Access control & photo ID badging

GOVERNMEN

High Security Department of Defense Facilities

Based on our industry experience, local presence and our ability to maintain clearances, HBE's Securus Division has supported Strategic Department of Defense sites with access and surveillance solutions including:

- Access control systems
- Alarm monitoring systems
- Badging systems
- CCTV systems
- Perimeter protection systems
- IR camera systems
- System design, installation, 24 X 7, 2 hour response maintenance for over 15 years

TRANSPORTATION

Metropolitan Transportation Authority - Triborough Bridge and Tunnel Authority

Technical Support and Maintenance for the Underground Wireless Telecommunications Infrastructure at both the Brooklyn Battery and Queens Midtown Tunnels. Emergency communications are provided in both tunnels for the following agencies: Triborough Bridge and Tunnel Authority (TBTA); NY City Police Department (NYPD); Fire Department of NY (FDNY) and the city's Emergency Services Department (EMS).

- System also provides extended coverage throughout both tunnels for the commercial carriers Cingular, Nextel/Sprint, T-Mobile and Verizon
- System provides AM/FM Rebroadcast System, with over 30 channels of radio communications as well as emergency communications capabilities

TRANSPORTATI

Public Agencies

The transportation and public agency security contracts secured and completed by Henry Bros. across the country are the hallmark of our success. High profile, rigorous schedules and challenging environments have made these projects something that sets us apart. From perimeter intrusion systems at airports, bridges and tunnels to access control and surveillance in fast changing transportation venues, Henry Bros. has stepped up to the challenge deploying systems that include:

- Perimeter sensors including fence, radar and microwave systems
- Access control design, install and administration, both fixed and mobile
- Surveillance using advanced traditional, IR, Thermal and long distance cameras
- LRAD acoustical warning and defense systems

You're in good company with Henry Bros. Electronics — call us at any of our offices or email sales@hbe-inc.com to discuss your specific needs for Security Integration, Wireless Emergency Communications and expert assistance with Emergency Action Planning.

We have been perfecting security integration for over 50 years in some of the most demanding environments. Feel free to leverage our experience — now more than ever.

HBE HENRY BROS. ELECTRONICS, INC.

NEW JERSEY
Henry Bros. Electronics, Inc.
17-01 Pollitt Drive
Fairlawn, NJ 07410
201-794-6500

NEW YORK
Henry Bros. Electronics, Inc.
17 Battery Place, Suite 701
New York, NY 10004
212-240-9500

WASHINGTON, DC METRO
CIS Security Systems Corp.
A Henry Bros. Company
8350-0 Terminal Road
Newington, VA 22122
703-313-0070

MARYLAND
CIS Security Systems Corp.
A Henry Bros. Company
1500 Caton Center Drive, Suite C
Baltimore, MD 21227
410-247-9517

TEXAS
Henry Bros. Electronics, Inc.
2100 Highway 360, Suite 2101
Grand Prairie, TX 75050
972-988-8887

COLORADOSecurus Inc.
A Henry Bros. Company
12411 E. 37th Avenue
Denver, CO 80239-3404
303-373-5535

Securus Inc.
A Henry Bros. Company
3328 Adobe Court
Colorado Springs, CO 80907
719-227-1123

ARIZONA
Henry Bros. Electronics, Inc.
4710 E. Elwood Street
Phoenix, AZ 85040
480-894-2826

CALIFORNIA
Henry Bros. Electronics, Inc.
1511 E. Orangethorpe Ave, Suite A
Fullerton, CA 92831
714-525-4360

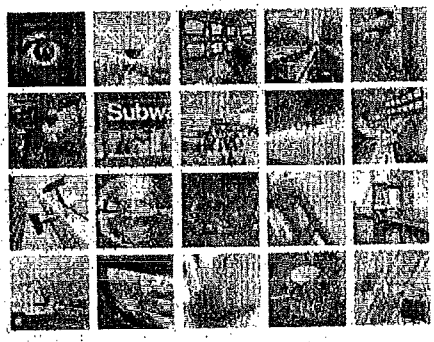
SUBSIDIARIES

Diversified Security Solutions, Inc.
Emergency Action Planning
17 Battery Place, Suite 701
New York, NY 10004
212-240-9500

Viscom Products, Inc.
Mobile Video
17-01 Pollitt Drive
Fairlawn, NJ 07410
201-794-6500

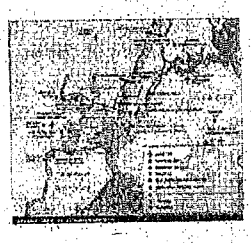
Airorlite Communications, Inc.
Wireless Emergency
Communications
17-01 Pollitt Drive
Fairlawn, NJ 07410
201-794-6500

HENRY BROTHERS ELECTRONICS, INC



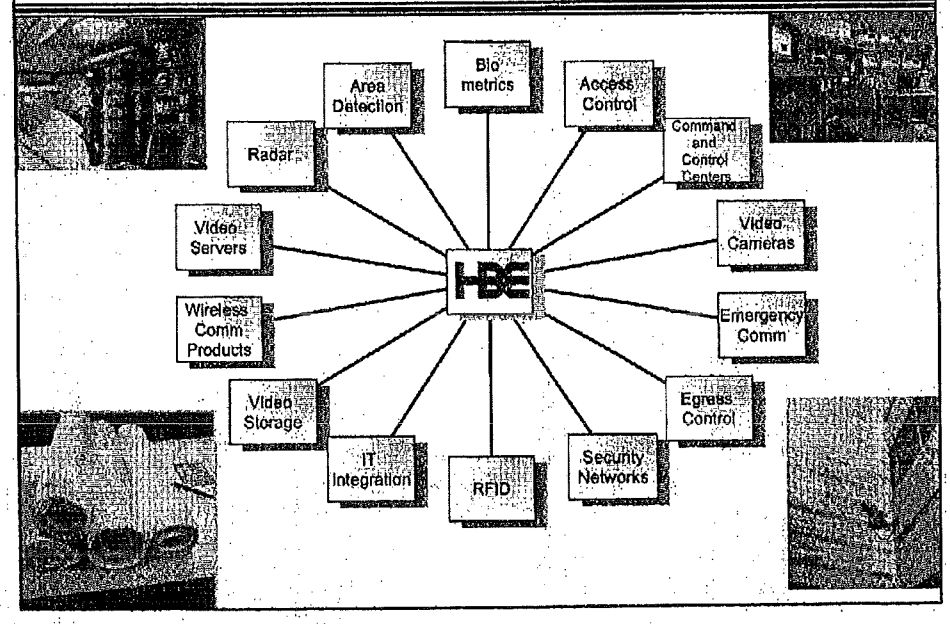
perfecting security integration since 1950

Service Contract Proposal Review for



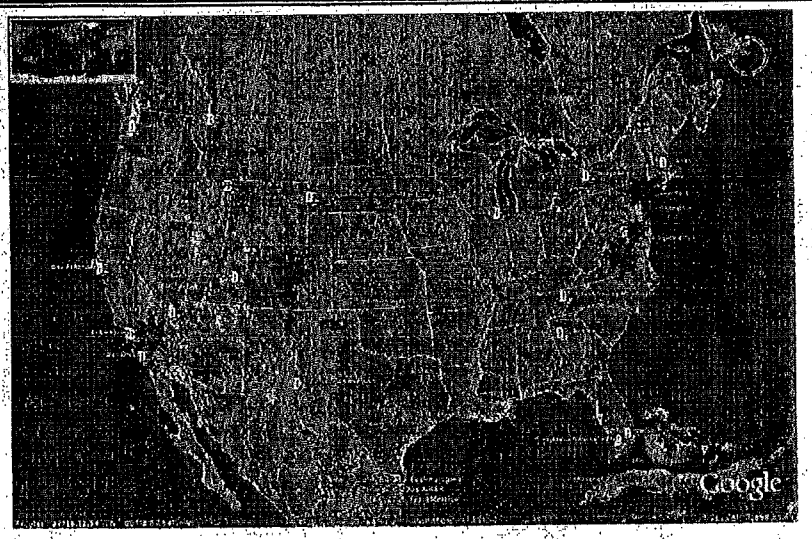
HENRY BROS. ELECTRONICS, INC.

Bringing it all together



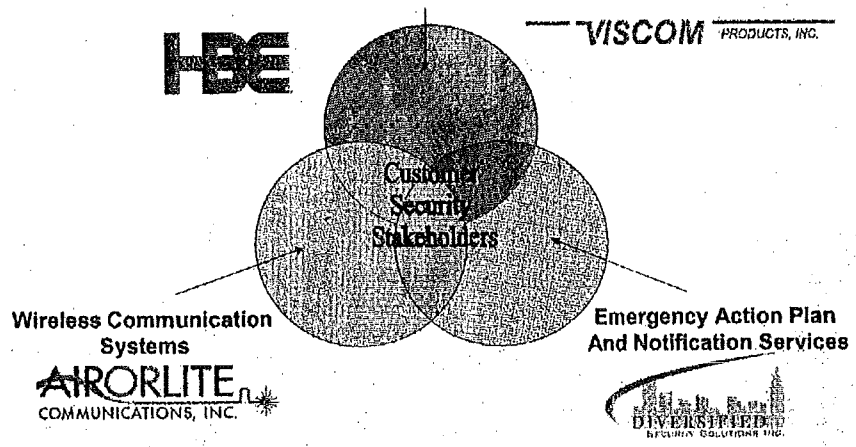
HENRY BROS. ELECTRONICS, INC.

Building A National Footprint



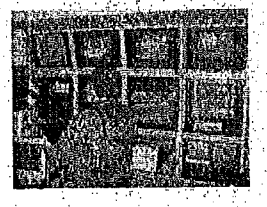
Acquisition and Expansion Strategy Supports Emerging Customer Needs

Nationwide Physical Security Design, Integration and Support



Service capability and plans

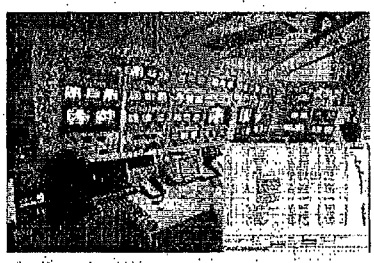
- Some examples of agreements that lock in pricing and level of service priority for specific time periods.
  - Service Maintenance Agreements as part of Open Task Order contracts
  - Service Maintenance agreements
  - Block of time agreements to guarantee pricing on Labor and Material for specific periods
- These agreements can be structured to support all of the HBE Subsidiaries and Products
- All Service Contracts will be supported by automated service call and asset tracking software (Maximo)

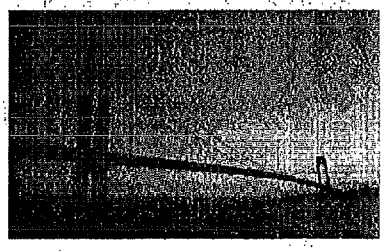


HENRY BROS. ELECTRONICS, INC.

Program Management

- Coordinated Project Management Programs
- Server Based remote Program Management SW
- Engineering Drawing Packages
- Program Status and Management Review Meetings
- Client Updates and Status Reports
- 24/7 availability of key personnel
- Remote access for field personnel to safeguarded material





HENRY BROS. ELECTRONICS, INC.

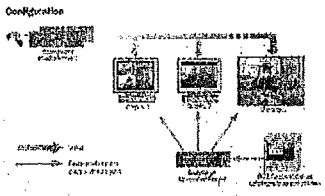
Design Engineering Capabilities

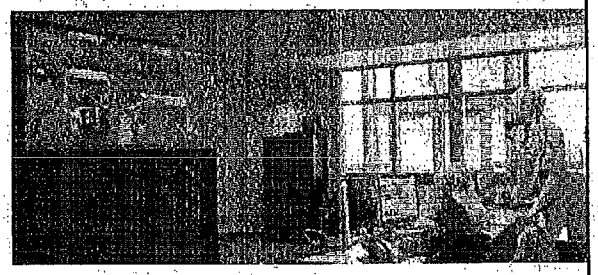
- Enterprise Class Security System Design
  - Access Control
  - Video,
  - TWIC compliant Biometrics
- Radio Communications design/build for enhanced coverage and emergency service through Airorlite
- Full Drawing Packages and Document Control with AutoCAD
- Communications Engineering
  - CCIE and CCNA on Staff
- Full Range of Engineering disciplines on Staff including BSEE, BSCS and BSME
- Software Tolls AutoCAD MS Project and Visio
- Over 40 years of Video Engineering and test experience including:
  - Test and Evaluation of new technologies
  - IP and Analog expertise
  - Thermal imaging design, test and evaluation
- Fiber optic design, install and test capabilities

HENRY BROS. ELECTRONICS, INC.
Protecting Security Integration

Command and Control Centers

- Experience with all critical elements of the C&C Environment
  - Access Control
  - Video Cameras
  - Video Walls and monitor clusters
  - IT Integration
  - Emergency Communications
- Currently under contract for the Brooklyn Battery Tunnel Command Center using Barco Video Wall

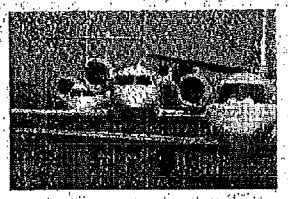




HENRY BROS. ELECTRONICS, INC.
Protecting Security Integration

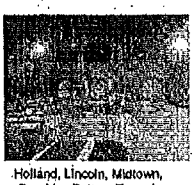
Airport Experience

- Service Agreements 24/7/365 2 hr response commitments
- On site PM and technical resources
- Port Authority Open Task Order for all NY Metro Airports
- Implementation of emerging video analytics capability
- Design, Build, Ops, Maintenance and Support (DBOM) for
  - Access Control with Lenel Systems
  - Video Surveillance and analytics
  - Radar Integration with long-range Video Surveillance
- Designed and built state of the art General Aviation Facility security network

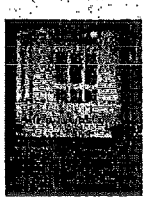


HENRY BROS. ELECTRONICS, INC.
Perfecting Security Integration

Bridge and Tunnel Expertise



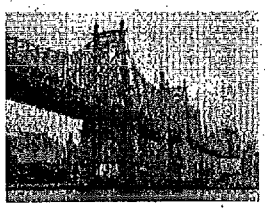
Holland, Lincoln, Midtown, Brooklyn Battery Tunnels



- Command and Control Centers
- Design challenges in video applications
- Access Control
- Communication systems
- Cabling challenges
- Safety considerations

Verrazano Narrows Bridge

Hackensack River Bridge

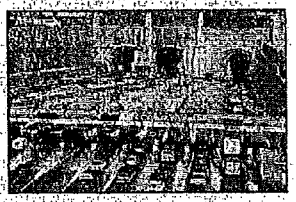


Queensboro 59th Street Bridge

HENRY BROS. ELECTRONICS, INC.
Perfecting Security Integration

Marquee Service Contracts

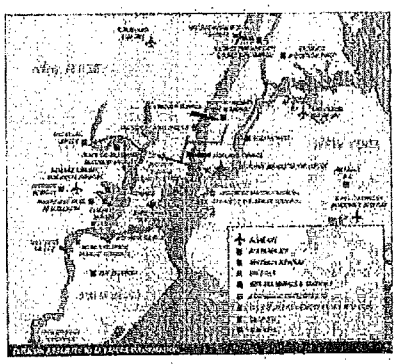
- Port Authority of NY & NJ Airports
- 7 World Trade Center - Silverstein Properties
- North American Air Defense
- Port of Long Beach
- Parsons Engineering Global Deployment
- Raytheon Perimeter Intrusion Detection System
- USC Galen Center
- Dodger Stadium
- MTA - 2 Broadway



HENRY BROS. ELECTRONICS, INC.
Perfecting Security Integration

Port Authority Experience

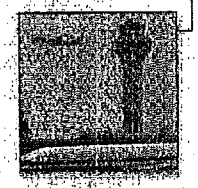
- Maintain all Access Control, Alarm Monitoring & Dedicated Security Networks at JFK, LGA and EWR.
- PATH Head End Video Storage – Replacement & upgrade
- Temporary Path Station at WTC (video recording and storage)
- Teterboro Airport First Aviation
- Perimeter Intrusion Detection System (PIDS)
- 7 World Trade Center
- Heliport Access Control & CCTV
- Staten Island Bridges Access Control & Digital Video Systems



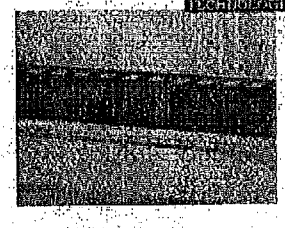
HENRY BROS. ELECTRONICS, INC.
Perfecting Security Integration

Advanced Technology support PANYNJ

- L3 Praetorian Video Flashlight (EWR)
- Microwave Perimeter Protection
- L-RAD Acoustic Device
- Radar Integration Support
- Thermal Imaging and IR Cameras
- Video Wall Support Capability
- Technologies to support post 9-11 directives
  - Advanced emergency wireless communications
  - Emergency egress
  - Redundant servers and repeaters
  - Self Healing Networks for Communications, Access & Video



Raytheon



HENRY BROS. ELECTRONICS, INC.
Performing Security Integration

Maximo Mobile Suite

Maximo Mobile for Work Management
- Eliminates redundant tasks, reduces paperwork and overall task time.
- Increases first-time fix rates and asset availability.
- Records work status, labor, materials, time and attendance, failure codes, tools, comments, etc

Maximo Asset Management
- Manages inventory
- Manages spare parts
- Manages asset allocation
- Controls purchase order/delivery status

Service/Maintenance Management
- Creates service requests
- Monitors status (open, resolved, cancelled, etc)
- Manages resource allocation

HENRY BROS. ELECTRONICS, INC.
Performing Security Integration

Management Approach

- **Transition Plan**
  - a) **Initial actions**
  - b) **Use of site experienced consultants**
- **Staffing**
  - a) **Maintenance**
    - i) **George Washington Bridge**
    - ii) **Holland Tunnel**
    - iii) **Lincoln Tunnel**
    - iv) **Staten Island Teleport**
  - b) **System Administration**
- **Implementation**
  - a) **Creation of baseline**
- **Operational Plan**
  - a) **Change Control Process**
  - b) **Incident Management Process**

HENRY BROS. ELECTRONICS, INC.
Partnering Security Integration

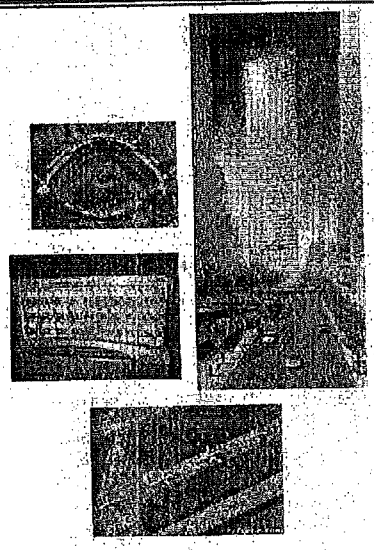
Technical Approach

- Experience with Providing Preventative and Remedial Maintenance for PANYNJ
- Experience with Equipment & Software
  - a) Lenel
  - b) Verint
  - c) Legato
- System Enhancements
  - a) Database Backups
  - b) Audit Tool Replacement
- Experience with System Upgrades
  - a) Lenel Upgrades
  - b) Verint Upgrades
  - c) Legato Replacement

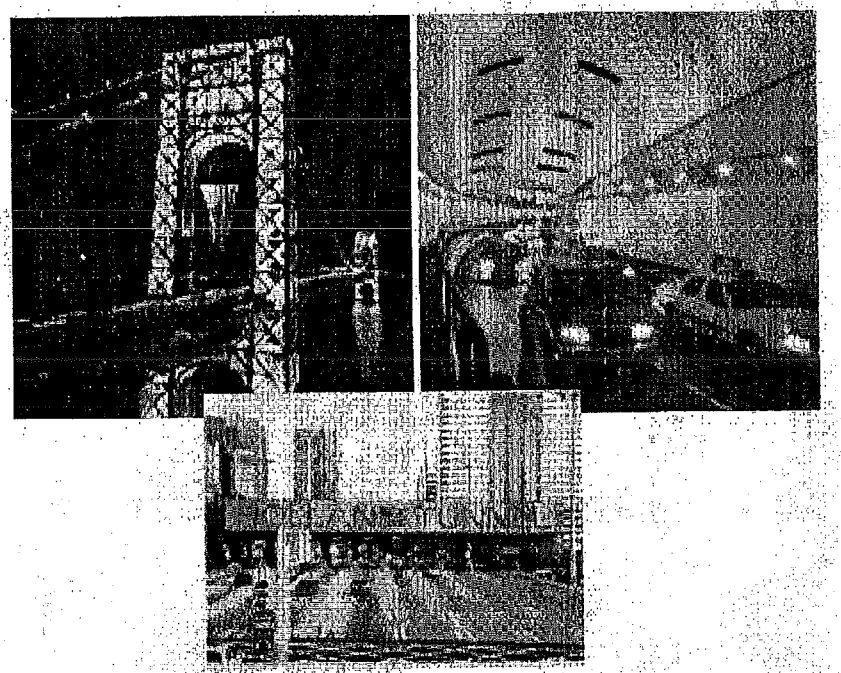
HENRY BROS. ELECTRONICS, INC.
Partnering Security Integration

Service Summary

- Henry Bros. can provide the best service solution for Advanced Physical Security, Wireless Infrastructure Installations
  - Flexibility in service offerings to maximize uptime and maintain your capital investments
  - National resources with strong local presence
  - Access to the most capable suppliers in the Physical Security Industry
  - Years of engineering experience with the special needs of the Security and Specialty Wireless Applications
  - Proven track record with IP security hardware and the staff to integrate seamlessly with IT and the technologies continue to converge
  - Experience with large multi year service contracts and Program Management



Maintenance of Access Control System
and
System Administration Services



Response to Request for Clarification

Submitted by:

HBE HENRY BROS. ELECTRONICS, INC.
17-01 Pollitt Drive Fair Lawn, NJ 07410
Phone: 201.794.6500 www.hbe-inc.com Fax: 201.794.8341

Bernie Drury (201) 794-6500 ext. 3037

July 6, 2007

HENRY BROS. ELECTRONICS, INC.
17-01 Pollitt Drive Fair Lawn, NJ 07410
Phone: 201.794.6500 www.hbe-inc.com Fax: 201.794.8341

July 5, 2007

Ms Jeanette Santos
Senior Purchasing Manager
Purchasing Services Division
The Port Authority of NY/NJ
1 Madison Avenue
Seventh floor
New York, NY 10010

Re: Maintenance of Access Control System and System Administration Services for the George Washington Bridge (GWB), Lincoln Tunnel (LT), Holland Tunnel (HT) and Staten Island Teleport.

Responses to PANYNJ questions dated June 28, 2007

Dear Ms. Santos:

Attached please find the responses to the Port Authority questions and comments posed in the letter dated June 28th.

We look forward to our presentation slot next Thursday, July 12th at 1:30PM when we can discuss these issues, and the entire HBE proposal package in greater detail.

Very truly yours,

Bernard J. Drury Jr.
VP Marketing & Sales, Aviation
Henry Bros. Electronics, Inc.

Appendix A
ACS Components

THE PORT AUTHORITY OF NY & NJ

June 28, 2007

DHL Overnight Mail – 201 794-6500

Henry Bros. Electronics, Inc.
17-01 Pollitt Drive
Fair Lawn, NJ 07410

Attn: Bernard J. Drury Jr., VP. Sales & Marketing Aviation

RE: REQUEST FOR PROPOSALS (RFP) NO. 13071 MAINTENANCE OF ACCESS CONTROL SYSTEM AND SYSTEM ADMINISTRATION SERVICES FOR THE GEORGE WASHINGTON BRIDGE (GWB), LINCOLN TUNNEL (LT), HOLLAND TUNNEL (HT) AND STATEN ISLAND TELEPORT

Dear Mr. Drury:

Thank you for submitting your response for the above referenced proposal. As a result of our initial evaluation of the proposal submitted by your firm, you are hereby requested to submit responses to the attached questionnaire. Please furnish this information before 12:00 PM on Friday, June 6, 2007. Forward one (1) original and ten (10) copies of your response to Ms. Jeanette Santos, at the address listed below. Failure to provide the requested information may result in your proposal being deemed non-responsive.

Presentation Meeting:

As part of the evaluation process, and contingent upon your satisfactory response to the above request for additional clarifications, the Committee would like to invite you and key members of the management team for a presentation and discussion. It is scheduled for Thursday, July 12, 2007, commencing at 1:30 PM and ending no later than 3:30 PM. Please arrive 15 minutes in advance to set up.

The location of this meeting is at the office of the Port Authority of New York and New Jersey (Port Authority), located at One Madison Avenue, 5th Floor Conference Room. One of the Committee representatives will meet you in the 5th Floor reception area at the appointed time to escort you to the meeting location. Please note, photo ID is necessary to gain access into the building. In addition, please send me a list of all participants 24 hours prior to your presentation date. The list can be e-mailed to jsantos@panynj.gov.

Procurement Department
One Madison Avenue, 7th Floor
New York, NY 10010
T: 212 435 7000

THE PORT AUTHORITY OF NY & NJ

Total time allocated to your firm for the presentation, including questions, answers and closing statements is no longer than **2-1/2 hours**. Generally, allow 1 hour for your presentation addressing all the important points of your proposal and responses to the attached questions. In the conclusion of your proposal presentation, the remaining time will be used for questions and answers from the Committee. Please note that the Port Authority will only provide a projector screen. You will need to provide all other equipment.

As a disclaimer, this invitation to make a presentation about your proposal to the Port Authority shall not be construed in any way whatsoever to be an acceptance of your proposal.

If you have any questions, contact Jeanette Santos at 212 435-3930.

Sincerely,

Jeanette Santos

Jeanette Santos
Principal Contracts Specialist
Priority Procurements Division
Procurement Department

Questions to Henry Brothers

Comments & Exceptions

Bullet 1
Please refer to page 87, Section O "Hardware/Software Support and Updates" The Port Authority expects all updates to be included in your cost proposal. "Software updates" is defined as maintaining all software releases for the Access Control System, for example, LENEL, LEGATO, Microsoft WINDOWS 2000, Microsoft SQL Server and Verint. The software updates shall include new releases, updates to current releases, and patches. The Contractor will be responsible for software updates within a current release. Any major releases (e.g., versions 5 to 6) would be considered extra work under the terms of this contract. Upgrades will be compensated through extra work if the Authority elects to choose the upgrade resulting an extra cost to the Contractor.

Bullet 2
The exception is rejected in its entirety. The Contractor must meet the requirements detailed in the RFP document on page 71, Section D, second and third paragraph.

Bullet 3
Except for when the Annual Period to be adjusted is an Option Period, such a fraction shall not exceed three percent (3%) per annum.
Page 24 and 25 entitled Section 2, "Duration of Contract". Refer to attached Addendum 6.

Executive Summary

1. Explain the connectivity of CMMS product proposed. Will the CMMS product be hosted off-site or on-site. Please refer to Attachment I "The Port Authority of NY & NJ Guide to System Administration" and Attachment L "Port Authority Technology Standards and Guidelines."

Technical Approach

1. You did not provide a Technical Approach in your proposal. Please identify your technical ability to provide the required services as detailed on pages 8 and pages 11 and 12 of the RFP.

2. Please provide a detailed approach to each heading included in the SOW, Attachment C; please refer to page 8 section 4 evaluation criteria and ranking Subsection A. "Technical Approach".

3. You did not outline a detailed approach for System Administration Services for ACS and maintenance of the ACS equipment as described on page 12, Section 1 "Technical Approach" Please submit as part of your proposal submission.

Experience and Management Approach

1. You did not provide a Management Approach in your proposal. Please identify your management approach on how you will provide the required services as detailed on pages 9 and 12 of the RFP.

2. Please provide a detailed M/WBE Plan as outlined in Section C and Section 5, Page 9 of the RFP.

Revised 6 26, 2007 at 1:54 PM.

CLARIFICATIONS TO PROPOSAL #13071

Amendment# 1
24, section titled " 2. Duration of Contract" third paragraph insert the following: Each price adjustment shall be capped at three (3) percent.

Page # 25, paragraph (a) and (b) insert at the end of each paragraph the following: The price adjustment shall be capped at three (3) percent for each option period.

Amendment # 2
Page # 81, second paragraph, titled "E. System and Application Data Back-ups and Archiving" delete clause and insert the following clause:

Maintaining off-site back-ups: The Contractor shall perform scheduled back-ups for off-site storage or rotate back-up media to and from the off-site storage location as appropriate. Ensure that viable and complete back-ups are delivered to the off-site storage location when scheduled and that media to be rotated is returned from off-site storage location and returned to usage on the system as appropriate. The Contractor shall be responsible only for handing the tapes over to the contractor providing the off-site storage facility on a monthly or quarterly basis, or as designated by the Authority. All back-up media destined for off-site storage will be picked up by the off-site storage contractor at the Staten Island Teleport. The Authority will pay for use of the off-site storage facilities for back-ups if site is not on the Authority's property.

Amendment # 3
Page # 81, section titled "E. System and Application Data Back-ups and Archiving" insert new clause at the end of this section:

Archiving data: Follow system archiving procedures to capture data to be archived to permanent storage media as required to maintain proper system functioning or as scheduled in the system operating procedures (whichever occurs first). The Contractor shall ensure that archived media is properly logged and maintained and that archived data is viable and accessible throughout the required archive retention period for the data. The off-site storage contractor's personnel will transport the archived storage media to and from the Authority-provided off-site storage location. The Authority will pay for use of the off-site storage facilities for archiving if the site is not on the Authority's property.

Amendment # 4
Page # 93, in the title, section titled "R. System Documentation Library , c) Off site Storage" Insert "- Record Management" after the word "Storage"

Amendment # 5

Page # 93, first paragraph, first line in the section titled "R. System Documentation Library , c) Off site Storage"

Insert "- record management" after t the word "storage"

Amendment # 6

Page 87, seventh paragraph, section titled "O. Hardware/Software Support and Updates"

Delete the word "upgrade and insert the word "update" everywhere that it appears in this paragraph.

Amendment # 7

Part III – Cost Proposal Sheets, Exhibit E is herby superceded in its entirety by the attached revised Exhibit E dated 6/22/07

PART III - COST PROPOSAL SHEETS

EXHIBIT E - Revised June 22, 2007

Maintenance of Traffic - Three Year Base Term

(A)	(B)	(C)	(D)	(E)
Description	**Lane Closures per Month**	**Estimated Price Per Lane Closure**	**X 12 Months**	**Estimated Total Annual Price**
George Washington Bridge	3		x 12	
Holland Tunnel	2		x 12	
Lincoln Tunnel	2		x 12	

Total Estimated Annual Maintenance of Traffic Cost $ _____
(Sum of Item in Column D)

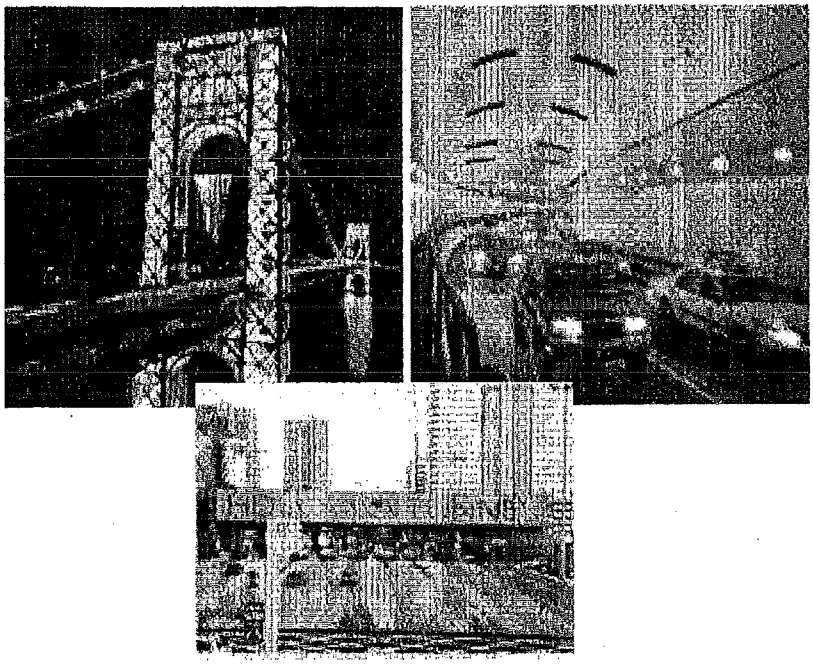
Note: Normal working hours are between the hours of 11 PM - 6 PM , unless otherwise directed by the Contract Manager or Facility Manager.

Note: The Proposer shall refer to the section titled Maintenance of Traffic Attachment C - Scope of Work.

Note: Work may be requested at the sole discretion of the Contract Manager at any time during the term of this contract. No work will be started without prior authorization. No work is guaranteed.

Original

Maintenance of Access Control System
and
System Administration Services



Submitted by:

HENRY BROS. ELECTRONICS, INC.
17-01 Pollitt Drive Fair Lawn, NJ 07410
Phone: 201.794.6500 www.hbe-inc.com Fax: 201.794.8341

Bernie Drury (201) 794-6500 ext. 3037

June 4, 2007

THE PORT AUTHORITY OF NY & NJ

THE PORT AUTHORITY OF NEW YORK & NEW JERSEY
PURCHASING SERVICES DIVISION
ONE MADISON AVENUE 7TH FL.
NEW YORK, NY 10010

Date April 25, 2007

ADDENDUM #1

To prospective bidders/proposers on bid/RFP # 13071 for MAINTENANCE OF ACCESS CONTROL SYSTEM AND SYSTEM ADMINISTRATION SERVICES FOR THE GEORGE WASHINGTON BRIDGE (GWB), LINCOLN TUNNEL (LT), HOLLAND TUNNEL (HT) AND STATEN ISLAND TELEPORT RFP

☒ Due back on MAY 23, 2007, no later than 2:00PM

☐ Originally due on , no later than 11:00AM/2:00PM

The following changes are hereby made in the documents:

1. **Site Visit has been rescheduled to May 4, 2007, at 10:00 AM**

This communication should be initialed by you and annexed to your bid/proposal upon submission.

In case any bidder/proposer fails to conform to these instructions, its bid/proposal will nevertheless be construed as though this communication had been so physically annexed and initialed.

THE PORT AUTHORITY OF NY & NJ

JANE CETERKO, MANAGER
PURCHASING SERVICES DIVISION

BIDDER'S/PROPOSER'S FIRM NAME: _____

INITIALED: _____

DATE: _____

PS11All

QUESTIONS CONCERNING THIS ADDENDUM MAY BE ADDRESSED TO Jeanette Santos, WHO CAN BE REACHED AT (212) 435-3930.

THE PORT AUTHORITY OF NY & NJ

THE PORT AUTHORITY OF NEW YORK & NEW JERSEY
PURCHASING SERVICES DIVISION
ONE MADISON AVENUE 7TH FL.
NEW YORK, NY 10010

Date May 9, 2007

ADDENDUM #2

To prospective bidders/proposers on bid/RFP # 13071 for MAINTENANCE OF ACCESS CONTROL SYSTEM AND SYSTEM ADMINISTRATION SERVICES FOR THE GEORGE WASHINGTON BRIDGE (GWB), LINCOLN TUNNEL (LT), HOLLAND TUNNEL (HT) AND STATEN ISLAND TELEPORT RFP

☒ Due back on MAY 23, 2007, no later than 2:00PM

☐ Originally due on , no later than 11:00AM/2:00PM

The following changes are hereby made in the documents:

Amendment #1
Page 65, insert new clause after 1. B, Performance Requirements, the new clause shall state:

1.C. Staten Island Bridges
It is anticipated that at some point during the term of this Contract, the Staten Island Bridges shall require similar preventive and corrective maintenance and system administration services. The Staten Island Bridges (SIB) Access Control System is similar in scope to the Holland Tunnel and Lincoln Tunnel Access Control System, which include LENEL and VERINT/LORONIX digital video recording system , two redundant servers, and security field devices. The SIB Access Control System provides coverage for the Goethals Bridge, Bayonne Bridge, and Outerbridge Crossing Bridge. The Port Authority will have the option to add the Staten Island Bridges to the Contract at any time during its term or extended term by thirty (30) days written notice to the Contractor, at the prices agreed upon by the parties as set forth in the Cost Proposal Sheet relating thereto which are annexed to the Contract.

For the purposes of providing a cost estimate, assume that SIB will be similar in scope to the Lincoln Tunnel and Holland Tunnel.

Amendment # 2
Part III – Cost Proposal Sheets, Exhibit E is herby superceded in its entirety by the attached revised Exhibit E dated 5/7/07.

Amendment # 3
Part III – Cost Proposal Sheets, insert attached Exhibit G after Exhibit F

Amendment # 4
A second site visit will be conducted based on interest expressed by Proposers on the site visit scheduled on May 4, 2007 at the George Washington Bridge. All Proposers will meet for the second site visit on Wednesday May 16, 2007 at the George Washington Bridge Administration Building , 2nd Floor Conference Room located at 220 Bridge Plaza South, Fort Lee, New Jersey.

The site inspection will be conducted according to the following schedule:

8:30 AM - George Washington Bridge - Proposers will meet at the 2nd Floor Conference Room and will be escorted to the Security Desk to receive a temporary visitor pass.

9:00 AM - George Washington Bridge - Proposers will be shown to two locations representative of a " typical" maintenance room.

Approximately 12: 00 PM - Holland Tunnel - Proposers will be shown to two locations representative of a " typical" maintenance room.

Approximately 2: 00 PM - Lincoln Tunnel - Proposers will be shown to two locations representative of a " typical" maintenance room.

For security reason, attendance will be limited to two representatives per Proposer on the day of the site visit. Two forms of photographic identification will be required for attendance at each of the sites visited. No one will be admitted without appropriate identification. No exceptions.

Attendees interested in attending shall RSVP to Barbara Abal, Supervisor, Policy and Business Planning, at 212-435-4827 or babal@panynj.gov no later than 12 noon Eastern Daylight Time on May 15, 2007 to confirm their attendance.

Amendment # 5
Please refer to attached Reading Room Guidelines

This communication should be initialed by you and annexed to your bid/proposal upon submission.

In case any bidder/proposer fails to conform to these instructions, its bid/proposal will nevertheless be construed as though this communication had been so physically annexed and initialed.

THE PORT AUTHORITY OF NY & NJ

JANE CETERKO, MANAGER
PURCHASING SERVICES DIVISION

BIDDER'S/PROPOSER'S FIRM NAME: _____

INITIALED: _____

DATE: _____

QUESTIONS CONCERNING THIS ADDENDUM MAY BE ADDRESSED TO Jeanette Santos, WHO CAN BE REACHED AT (212) 435-3930.

Reading Room Guidelines

RFP # 13071

MAINTENANCE OF ACCESS CONTROL SYSTEM AND SYSTEM ADMINSTRATION SERVICES FOR THE GEORGE WASHINGTON BRIDGE (GWB), LINCOLN TUNNEL (LT), HOLLAND TUNNEL (HT) AND STATEN ISLAND TELEPORT

To all Proposers:

Welcome to the Reading Room.

The documents provided in this Reading room have been made available for your examination. The Port Authority makes no representation or guarantee, and shall not be responsible for their accuracy, completeness or pertinence, and, in addition, shall not be responsible for the conclusions drawn therefrom. These documents are made available merely for the purpose of making available such information as is in the possession of the Port Authority and which it is able to make available, whether or not such information may be accurate, complete or pertinent or of any value to prospective Proposers.

Please take a moment to read and become familiar with the guidelines that are to be followed while using the Reading Room.

1. Documentation provided cannot be removed from the Reading room.

2. When handling the documentation, take the following precautions:

- Do not make any marks on the pages.
- Do not spindle, fold or mutilate any pages.
- Do not trace, alter, tear or bend or handle the pages in such a way as to cause damage to any pages.
- Do not tear out any pages.
- Do not refold pages in a new or different way.
- Use only Post-It notes or slips of paper for marking your place. Remove all page markers before leaving the Reading Room.

3. Duplication of documentation by camera, scanner, photocopier or other means is prohibited.

4. Laptop or other device for taking notes is permitted but the Proposers must supply their own electrical (110v-120v) connections. Internet connection is prohibited.

5. The Port Authority shall not be held responsible for the loss, damage or theft of any Proposer's electronic equipment or personal items brought into the Reading Room.

6. Access to the documents is by appointment only. If you require further examination of the documents provided, kindly schedule another appointment by contacting Barbara Abal, Supervisor, Policy and Business Planning, TB&T during the hours of 10:00 AM through 4:00 PM, Monday through Friday at 212-435-4827 or babal@panynj.gov.

****

The terms of the confidentiality agreement also pertains to the materials available in the Reading Room.

If you have read and accept the guidelines, please fill out the information requested below. Failure to sign this statement and agree to all the above conditions shall preclude you from having access to the available documents.

Name :_____

Title :_____

Company :_____

Address :_____

Phone/email :_____

Date and Time:_____

THE PORT AUTHORITY OF NY & NJ

THE PORT AUTHORITY OF NEW YORK & NEW JERSEY
PURCHASING SERVICES DIVISION
ONE MADISON AVENUE 7TH FL.
NEW YORK, NY 10010

Date May 17, 2007

ADDENDUM #3

To prospective bidders/proposers on bid/RFP # 13071 for MAINTENANCE OF ACCESS CONTROL SYSTEM AND SYSTEM ADMINISTRATION SERVICES FOR THE GEORGE WASHINGTON BRIDGE (GWB), LINCOLN TUNNEL (LT), HOLLAND TUNNEL (HT) AND STATEN ISLAND TELEPORT RFP

☐ Due back on , no later than

☒ Originally due on May 23, 2007, no later than 2:00PM

The following changes are hereby made in the documents:

- Proposal Due Date is extended to Thursday, May 30, 2007 no later than 2:00 PM
- See attached Questions and Responses from prospective proposers.

This communication should be initialed by you and annexed to your bid/proposal upon submission.

In case any bidder/proposer fails to conform to these instructions, its bid/proposal will nevertheless be construed as though this communication had been so physically annexed and initialed.

THE PORT AUTHORITY OF NY & NJ

JANE CETERKO, MANAGER
PURCHASING SERVICES DIVISION

BIDDER'S/PROPOSER'S FIRM NAME: _____

INITIALED: _____

PS11All

DATE: _____

QUESTIONS CONCERNING THIS ADDENDUM MAY BE ADDRESSED TO Jeanette Santos, WHO CAN BE REACHED AT (212) 435-3930.

THE PORT AUTHORITY OF NY & NJ

THE PORT AUTHORITY OF NEW YORK & NEW JERSEY
PURCHASING SERVICES DIVISION
ONE MADISON AVENUE 7TH FL.
NEW YORK, NY 10010

Date May 25, 2007

ADDENDUM #4

To prospective bidders/proposers on bid/RFP # 13071 for MAINTENANCE OF ACCESS CONTROL SYSTEM AND SYSTEM ADMINISTRATION SERVICES FOR THE GEORGE WASHINGTON BRIDGE (GWB), LINCOLN TUNNEL (LT), HOLLAND TUNNEL (HT) AND STATEN ISLAND TELEPORT RFP

☒ Due back on May 30, 2007, no later than 2:00 PM

☐ Originally due on , no later than

The following changes are hereby made in the documents:

Amendment 1
Between the time period of May 24, 2007 – May 30, 2007, Proposers interested in reviewing documents in the Reading Room need to RSVP John Garbarini , Contract Manager at 201-346-6061 or jgarbarini@panynj.gov between the hours of 8:00 AM and 1 PM.

Amendment 2
Cover Page, Title, insert ", Port Authority Bus Terminal (PABT)" after "Holland Tunnel (HT)"

Amendment 3
Page 3, second and fourth paragraphs, insert "Port Authority Bus Terminal (PABT)"after "Holland Tunnel (HT)"

Amendment 4
Page 33, Section 11, Support Services Payments under listing of sites, insert " / PABT" after "Lincoln Tunnel"

Amendment 5
Page 33, Section 11, Support Services Payments 2nd paragraph, replace "(GWB, HT, and LT)" with "(GWB, HT, LT/ PABT, and Staten Island Teleport)"

Amendment 6
Page 66, Section 2.A. General Requirements, fourth paragraph, insert ", Port Authority Bus Terminal (PABT)" after "LT"

Amendment 7
Page 75, Operational Availability, first paragraph, insert ", Port Authority Bus Terminal (PABT)" after "HT"

Amendment 8
Page 76, Performance Measure, first paragraph, insert ", Port Authority Bus Terminal (PABT)" after "HT"

Amendment 9
Page 78, Section 3.A., General Information, second paragraph, second line, insert ", Port Authority Bus Terminal (PABT)" after "LT"

Amendment 10
Part III – Cost Proposal Sheets, Exhibit A is hereby superceded in its entirety by the attached revised Exhibit A

Amendment 11
Part III – Cost Proposal Sheets, Exhibit C is hereby superceded in its entirety by the attached revised Exhibit C dated May 18, 2007

Amendment 12
Attachment B, Non-Disclosure and Confidentiality Agreement (NDA) is hereby superceded by the attached revised NDA dated May 18, 2007

This communication should be initialed by you and annexed to your bid/proposal upon submission.

In case any bidder/proposer fails to conform to these instructions, its bid/proposal will nevertheless be construed as though this communication had been so physically annexed and initialed.

THE PORT AUTHORITY OF NY & NJ

JANE CETERKO, MANAGER
PURCHASING SERVICES DIVISION

BIDDER'S/PROPOSER'S FIRM NAME: _____

INITIALED: _____

DATE: _____

QUESTIONS CONCERNING THIS ADDENDUM MAY BE ADDRESSED TO
Jeanette Santos, WHO CAN BE REACHED AT (212) 435-3930.

THE PORT AUTHORITY OF NY & NJ

THE PORT AUTHORITY OF NEW YORK & NEW JERSEY
PURCHASING SERVICES DIVISION
ONE MADISON AVENUE 7TH FL.
NEW YORK, NY 10010

Date May 29, 2007

ADDENDUM #5

To prospective bidders/proposers on bid/RFP # 13071 for MAINTENANCE OF ACCESS CONTROL SYSTEM AND SYSTEM ADMINISTRATION SERVICES FOR THE GEORGE WASHINGTON BRIDGE (GWB), LINCOLN TUNNEL (LT), HOLLAND TUNNEL (HT) AND STATEN ISLAND TELEPORT RFP

☐ Due back on , no later than

☒ Originally due on May 30, 2007, no later than 2:00 PM

The following changes are hereby made in the documents:

- Proposal Due Date is extended to Monday, June 4, 2007 no later than 2:00 PM
- See attached Questions and Responses from prospective proposers.

Amendment 1
Between the time period of May 24, 2007 – June 4, 2007, Proposers interested in reviewing documents in the Reading Room need to RSVP John Garbarini , Contract Manager at 201-346-6061 or jgarbarini@panynj.gov between the hours of 8:00 AM and 1 PM.

This communication should be initialed by you and annexed to your bid/proposal upon submission.

In case any bidder/proposer fails to conform to these instructions, its bid/proposal will nevertheless be construed as though this communication had been so physically annexed and initialed.

THE PORT AUTHORITY OF NY & NJ

JANE CETERKO, MANAGER
PURCHASING SERVICES DIVISION

BIDDER'S/PROPOSER'S FIRM NAME: _____

INITIALED: _____

DATE: _____

QUESTIONS CONCERNING THIS ADDENDUM MAY BE ADDRESSED TO
Jeanette Santos, WHO CAN BE REACHED AT (212) 435-3930.

THE PORT AUTHORITY OF NY & NJ

PURCHASING SERVICES DIVISION
ONE MADISON AVENUE, 7TH FL.
NEW YORK, NY 10010

REQUEST FOR PROPOSALS

TITLE: MAINTENANCE OF ACCESS CONTROL SYSTEM AND SYSTEM ADMINISTRATION SERVICES FOR THE GEORGE WASHINGTON BRIDGE (GWB), LINCOLN TUNNEL (LT), HOLLAND TUNNEL (HT) AND STATEN ISLAND TELEPORT

NUMBER: *13071*

SUBMIT PROPOSALS BEFORE THE DUE DATE AND TIME TO THE ABOVE ADDRESS

PROPOSAL DUE DATE: May 23, 2007 **TIME:** 2:00 PM

QUESTIONS SHOULD BE SUBMITTED BY: May 3, 2007 **TIME:** 2:00 PM

SITE VISIT: April 30, 2007 **TIME:** 10:00 AM

BUYER NAME: Jeanette Santos **PHONE#:** (212) 435-3930
FAX#: (212) 435-3959

PART I - PROPOSAL REQUIREMENTS:

1. INFORMATION FOR PROPOSERS ON THIS REQUEST FOR PROPOSALS (RFP)

A. General Information: The Port Authority of New York and New Jersey 3
B. Deadline for Receipt of Proposals 4
C. Submission for Receipt of Proposals 4
D. Communications Regarding this RFP 4
E. Proposal Acceptance or Rejection 5
F. Pre-Proposal Meeting(s)/Site Inspection(s) 5
G. Available Documents 5
H. Union Jurisdiction 6
I. City Payroll Tax 6

2. PROPOSER PREREQUISITES 7

3. FINANCIAL INFORMATION 7

4 EVALUATION CRITERIA AND RANKING 8

5 M/WBE SUBCONTRACTING PROVISIONS 9

6 PROPOSAL SUBMISSION REQUIREMENTS 10

A. Letter of Transmittal 10-11
B. Executive Summary 11
C. Agreement on Terms of Discussion 11
D. Certifications with Respect to the Contractor's Integrity Provisions 11
E. Documentation of Proposer Prerequisites 11
F. Proposal 11-12
G. Acknowledgment of Addenda 13
H. Acceptance of Standard Contract Terms and Conditions (or Form of Contract) 14
I. M/WBE Plan 14

7. CONDITIONS FOR THE SUBMISSION OF A PROPOSAL 14

A. Changes to this RFP 14
B. Proposal Preparation Costs 14
C. Disclosure of Proposal Contents/Use of Ideas and Materials 14
D. Ownership of Submitted Materials 14
E. Subcontractors 15
F. Conflict of Interest 15
G. Authorized Signature 15
H. References 15
I. Evaluation Procedures and Negotiation 15
J. Taxes and Costs 15
K. Most Advantageous Proposal/No Obligation to Award 15
L. Right to Extend Contract 16
M. Rights of the Port Authority 16
N. No Personal Liability 17

PART II –GENERAL CONTRACT TERMS AND CONDITIONS

PART III – COST PROPOSAL FORMS

PART IV- ATTACHMENTS:

Attachment A – Agreement on Terms and Discussion

Attachment B - Non-Disclosure and Confidentiality Agreement (NDA)

Attachment C - Scope of Work

Attachment D – 2006 Web-based Application Checklist

Attachment E – Port Authority Control Security Requirements

Attachment F – Security Administration Function

Attachment G – Security Discussion

Attachment H – System Administration and Operation Manual Requirements

Attachment I – The Port Authority Of New York and New Jersey Guide to System Administration

Attachment J – Disaster Recovery Checklist

Attachment K - Handbook for Protecting Security Information

Attachment L - Port Authority Technology Standards and Guidelines

1. INFORMATION FOR PROPOSERS

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

The Port Authority of New York and New Jersey ("Port Authority" or "the Authority") is a body corporate and politic created by Compact between the States of New York and New Jersey with the consent of the Congress of the United States. The Port Authority, together with its wholly-owned subsidiaries, provides the region with integrated transportation and trade services and operates facilities in connection therewith, including, but not limited to, three major regional airports, interstate traffic through four bridges and two tunnels, a bus terminal, a bus station, the PATH rapid transit system, the Hoboken-lower Manhattan ferry service, and certain New York-New Jersey port facilities.

The Port Authority is hereby seeking proposals from qualified firms to provide Maintenance of Access Control System and System Administration Services for the George Washington Bridge, Lincoln Tunnel, Holland Tunnel and Staten Island Teleport Access Control System referred to hereunder as "ACS", as more fully described herein.

Brief Summary of Scope of Work

The Port Authority is seeking to retain a single firm to provide the Port Authority with Maintenance and System Administration services for the ACS, which is an efficient means by which to monitor and control access of critical and/or sensitive locations at the George Washington Bridge (GWB), Lincoln Tunnel (LT), Holland Tunnel (HT) and Staten Island Teleport. The Access Control System (ACS)is a fully integrated access control and intrusion detection system, including security field equipment, Video Badging, Digital Video Storage and Retrieval – Verint/Loronix Digital Video systems and Stetofon Public Address and Intercom Systems.

The heart of the system are the LENEL host computer systems (Master Servers) and software, which form the basis of the integrated system. The system employs two computer systems(servers) at each location and other related equipment and computer support systems, which are logically configured as Primary and Stand-by (redundant) with automatic fail over in event of a computer system failure. No operator intervention is required to implement the switch from Primary to Stand-by.

The Port Authority has made every reasonable effort to identify all ACS equipment, ACS systems, and related components, as described in this Request for Proposals . However, it is the Contractor's responsibility to identify, inventory and maintain the entire ACS system,which includes prior engineering project installations, updates, enhancements and subsequent engineering/maintenance changes.

Functions to be performed by the successful Proposer for these systems include but are not limited to the following:

- Preventative Maintenance
- Corrective Maintenance

- Web-enabled Computerized Maintenance Management System
- System Administration Services
- Maintenance Reporting
- Hardware/Software Support and Updates

The full Scope of Work is set forth in detail in Attachment C "Scope of Work"

The Contract will be for a three (3) year period. The Port Authority shall have at its sole option the right to extend the Contract for up to two (2) additional two year periods. In addition, the Port Authority will have sole right to extend the Contract for one 120-days period.

B. 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).

The Port Authority assumes no responsibility for delays caused by any delivery service. Post marking by the due date will not substitute for the actual proposal receipt.

C. Submission of Proposals

One reproducible original (containing original signatures and clearly designated as such) and ten (10) copies of the proposal must be submitted on or before the due date and time in accordance with the information on the cover page of this RFP and sent or delivered to the 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 along with the title of this RFP, this RFP number and the Proposal Due Date.

The original and each copy of the submission should include, in a separate envelope marked "Proposer Prerequisites", all documentation necessary to demonstrate that the Proposer meets the prerequisites set forth in Part I, Section 3 entitled "Proposer Prerequisites".

The Proposer should submit one (1) CD copy in Microsoft Word format of their proposal to assist in the review. If there is any difference between the CD and paper copy, the paper copy takes precedence.

D. Communications Regarding this RFP

All communications concerning this RFP should be directed to the Buyer listed on the cover page. All questions regarding this RFP should be submitted in writing to the Buyer at the address or facsimile number listed on the cover page, no later than 3:00 PM on the date listed on the cover page.

The 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 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.

E. 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.

F. Pre-Proposal Meeting(s)/Site Inspection(s)

A site inspection is scheduled for 10:00 AM on Monday, April 30 , 2007 at the George Washington Bridge Administration building, 2ND Floor Conference Room located in Fort Lee, New Jersey. As the largest of the three facilities, the George Washington Bridget is a representative site of a "typical" facility with similar field devices, computer systems and maintenance requirements.

Any questions concerning this RFP should be submitted in writing prior to the meeting so that the Port Authority may prepare responses in advance of the meeting. Additional questions may be permitted at the meeting; however, responses may be deferred and provided at a later date by written addenda.

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 a site inspection.

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 Barbara Abal, Supervisor, Policy and Business Planning, TB&T, Tel. No. 212-435-4827 or babal@panyni.gov no later than 12 noon (EST) of the business day preceding the scheduled date(s) to confirm their attendance and/or receive traveling directions.

***G.* Available Documents**

Certain documents, specified below, will be made available for examination by Proposers by contacting Barbara Abal, Supervisor, Policy and Business Planning, TB&T, Tel. No. 212-435-4827 or babal@panynj.gov Monday through Friday between the hours of 9:00 A.M. and 5:00 P.M.

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, pertinent or of any value to Proposers.

Documents for Reading Room:

-
-
- (Ex. 4)
-
-
-
-
-
-

H. Union Jurisdiction

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

I. City Payroll Tax

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

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

These taxes, if applicable, are the sole responsibility of the Proposer. Proposers should consult their tax advisors as to the effect, if any, of these taxes. The Port Authority provides this notice for informational purposes only and is not responsible for either the

imposition or administration of such taxes. The Port Authority exemption set forth in the Paragraph entitled "Sales or Compensating Use Taxes", in the "Standard Contract Terms and Conditions" included herein, does not apply to these taxes.

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. Proof of meeting the following prerequisites must be submitted with the Proposal. It should be noted that a determination that a Proposal meets the prerequisites is no assurance that the Proposer will be deemed qualified in connection with other proposal requirements included herein. At a minimum, Proposers must meet all of the following qualification requirements:

The Proposer shall be pre-qualified to perform under Collective #8253 - Prequalification of Security System Technology Design, Integration, Installation, and Maintenance System Integrators, dated November 30, 2005. Proposers must submit documentation showing that their firm is prequalified.

Joint Ventures of two or more prequalified entitities, containing firms certified by Lenel and Verint/Loronix as follows, are eligible to submit a bid. One firm may be certified by Lenel and a different firm may be certified by Verint/Loronix. Certification requires: Technicians shall have manufacturers certification for maintaining and servicing Lenel Access Control Systems and
Verint/Loronix systems.

Refer to Port Authority Web Site for a list of prequalified vendors: www.panynj.gov

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 reviewed statements from an independent accountant setting forth the aforementioned information shall be provided.

Where the statements submitted pursuant to subparagraphs (1) and (2) aforementioned do not cover a period which includes a date not more than forty-five 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 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

Proposals will be reviewed and evaluated on the following criteria listed in order of importance:

A. Technical Approach

The extent to which the Proposer demonstrates their ability to execute the required services, including, but not limited to:

- Demonstrated technical ability to provide required services including maintenance and system administration for the same or similar access control and intrusion detection technology based upon prior experience.

Evaluation of:

- Staffing plans.
- Standard operating procedures.
- Approach to System Administration and Maintenance Management Reporting
- Quality of start-up approach and business transition plan for start of contract and termination of contract.
- Provision and features of the on-line Maintenance Management System.
- Approach to each heading included in the Scope of Work, Attachment C.
- Describe background screening method conducted on employees, subcontractors, principals and concerned parties.

B. Financial Approach

The degree and extent to which the Proposal is cost effective to the Port Authority and the overall cost of the service. The Contractor's methods, practices, tools and techniques that will result in cost containment, and the likelihood of those methods, practices, tools and techniques being successfully deployed.

Describe the extent and quality of relevant experience of the Proposer, including similar services provided and the Proposer's financial capability.

C. Experience and Management Approach

The experience, qualifications and availability of the management and staff proposed to be assigned to provide the services (including subcontractors, if any) and, if applicable, a wage and supplemental benefits plan for key personnel and a self-assessment plan . The nature and quality of the Proposer's Quality Assurance/Quality Control Program. The Proposer's maintenance and system administration methodology. The quality of the on-site management plans for this Proposal.

The quality and extent of financial, reconciliation and auditing procedures. Prior experience between firms proposing a joint venture and prime subcontractor relationship will also be evaluated in this category; the quality and effectiveness of the Proposer's M/WBE plan and the extent to which it meets or exceeds Port Authority Standards; and the Proposer's ability to mitigate and eliminate business risk.

5. M/WBE SUBCONTRACTING PROVISIONS

The Port Authority of NY & NJ has a long-standing practice of making its business opportunities available to Minority Business Enterprises (MBEs) and Women-owned Businesses (WBEs) and has taken affirmative steps to encourage such firms to seek business opportunities with the Port Authority. The successful Proposer will use every good faith effort to provide for meaningful participation by Port Authority certified M/WBEs as defined in this document, in all purchasing, subcontracting and ancillary service opportunities associated with this contract, including purchase of equipment, supplies and labor services. Good faith efforts include 1) dividing the services and materials to be procured into small portions where feasible, 2) giving reasonable advance notice of specific subcontracting and purchasing opportunities to such firms as may be appropriate, 3) soliciting services and materials from M/WBEs, which may be certified by the Port Authority and 4) insuring that provision is made for timely progress payments to the M/WBEs.

The Port Authority has a list of certified M/WBE firms, which are available to Proposers at their request. The Port Authority makes no representation as to the qualifications and ability of these firms to perform under this contract. The Proposer may use firms which are not on the list but will be required to submit, to the Port Authority's Small Business Programs (SBP) for certification, the names of M/WBE firms it proposes to use. Only Port Authority certified M/WBE firms may be considered to meet the goals. For inquiries and assistance, please contact SBP at (212) 435-7819.

To the maximum extent feasible and consistent with the Proposer's exercise of good business judgment, the Proposer shall make a good faith effort to include 12% participation by MBE's and 5% participation by WBE's in all procurement, subcontracting and ancillary service opportunities associated with this contract. The Proposer shall submit an M/WBE Participation Plan, (Plan) which shall be evaluated and rated for this procurement. The Plan shall consist of the following:

Previous M/WBE Participation: Describe any previous or current M/WBE participation which the Proposer has sponsored.

Scope of Work: Describe the specific scope of work the M/WBE's will perform.

Identification of M/WBE's: Provide the name and address of any M/WBE included in the Plan. If none are identified, describe the process for selecting participant firms.

Level of Participation: Indicate the percentage of M/WBE participation expected to be achieved with the arrangement described in the Plan.

6. 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 or a joint venture . In all cases, information required for a single entity is required for each participant in a joint venture. Explain all prime subcontractor relationships.

The Letter of Transmittal shall contain:

(1) Name and address of the Proposer and an original signature on the Letter of Transmittal by an authorized representative on behalf of the Proposer;

(2) Name(s), title(s) and telephone number(s) of the individual(s) who are authorized to negotiate and execute the Contract;

(3) Name, title and telephone number of a contact person to which the Port Authority can address questions or issues related to this RFP;

(4) Name and address of proposed subcontractors, if any;

(5) If a corporation: (a) a statement of the names and residences of its officers, and (b) a copy of its Certificate of Incorporation, with a written declaration signed by the secretary of the corporation, with the corporate seal affixed thereto, that the copy furnished is a true copy of the Certificate of Incorporation as of the date of the opening of the Proposals;

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

If an individual: a statement of residence;

If a joint venture: information on each of the parties consistent with the information requested above;

If a joint venture which has not been established as a distinct legal entity submits a proposal, it and all participants in the joint venture shall be bound jointly and severally and each such participant in the joint venture shall execute the proposal and do each act and thing required by this RFP. On the Letter of Transmittal and wherever else the Contractor's name would appear, the name of the joint venture proposer should appear if the joint venture is a distinct legal entity. If the proposer is a common law joint venture, the names of all participants should be listed followed by the words "acting jointly and severally". All joint venture proposers must provide documentation of their legal status.

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 Contractor, by signing the Letter of Transmittal, makes the certifications in the "Contractor's Integrity Provisions," and agrees to all provisions stated in the "General Contract Provisions" included in PART II of this RFP. If the Contractor cannot make any such certifications, or has any specific exceptions, it shall enclose an explanation of that inability or exception in a separate letter included with its response to this RFP.

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 which details and clearly describes its capability to perform the work described in this RFP, its approach to such work and the cost of such work to the Port Authority. The Scope of Work (see Attachment C) is intended to outline the Port Authority's basic requirements for system administration services and access control system maintenance. At a minimum, the Proposal shall address the following:

(1)**Technical** The Proposer shall describe in detail its' technical approach to the Scope of Work as defined in Attachment C of this document, including performance standards, scheduling and milestones and a quality control/assurance plan, safety and work plans

including an overall description of its' employee safety training programs. Attach supporting documentation where applicable.

The Proposer shall respond to each heading included in the Scope of Work, Attachment C describe in detail ed in the The Proposer shall describe its approach to each heading included in the Scope of Work, Attachment C describe its methodology and approach to the Systems Administration Services for ACS, maintenance of the ACS equipment including but not limited to the Access Control System, CCTV cameras, servers and workstations, equipment and all Subsystems for each heading in the Scope of Work, Attachment C.

For the maintenance of the ACS equipment, the Proposer shall include a six month comprehensive preventive maintenance plan in its Proposal which will also include a plan for actively monitoring and reporting on system performance especially as it pertains to key points of failure. Scheduled preventive maintenance shall consist of, but not be limited to, inspection, testing, cleaning, lubricating, adjustment, repairs, the replacement of field installable parts that are approaching unserviceable status, and all actions necessary to prevent Access Control and Intrusion Detection System failures and extend the Access Control and Intrusion Detection System's useful life. Such maintenance shall be performed in accordance with the component manufacturers' recommendations.

The Proposer must propose a Computerized Maintenance Management Software package that will allow the Port Authority to track work performed by the successful Proposer (refer to Attachment C, Scope of Work "Computerized Maintenance Management System").

(2) **Management** – The Proposer shall describe in detail its' experience, including relevant contracts performed during the last three (3) years, its financial capability, management structure and proposed staffing, detailing technical training, certifications, applicable licenses (i.e., electrical), skills and experiences and capability of proposed staff and other supporting documentation demonstrating its ability to perform the work.

The Proposer shall provide detailed descriptions of its pre-employment screening procedures; safety and emergency procedures including, but not limited to, disaster recovery plans. The Proposer shall identify and provide key management and resources for program administration.

The Proposer shall provide a staffing plan that clearly outlines staffing needed to perform each function as described in the Scope of Work and submit training requirements for all technical employees. The Proposer shall describe how availability and response time requirements will be achieved. The Proposer shall describe the anticipated location of staff as well as the planned locations of the Proposer's nearest offices.

The Proposer shall address M/WBE provision as to what efforts it has taken for subcontracting provisions.

(3)**Financial** – The Proposer shall describe in detail all financial compensation it expects to receive from Port Authority for the performance of the work described in the Scope of

Work (refer to Attachment C - Scope of Work, Part III – Cost Proposal and Part IV – Attachments)

(4)The Proposer shall provide any other financial information, which is related to the above requirements or the evaluation criteria that the Proposer believes, would be helpful to the Port Authority of New York and New Jersey in the evaluation of their Proposal. This information should be able to be validated by certified corporate financial statements or corporate viability, which can be validated by organizations such as Dun & Bradstreet.

(5)**Background and Integrity Checks** - The Proposer shall submit a Proposer 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 5 years of employment history or verification of what an employee documented they have done in the last 5 years preceding the date of the investigation, resources utilized to perform this, and the frequency at which it is performed on current employees
- The type of investigation conducted, including criminal history background investigation to the extent permitted by law, and other investigatory measures including but not limited to personal, employment and credit history from open public source documents, if any, where permitted by law
- The type of company identification issued and controls utilized to ensure only authorized personnel possess such company identification, including procedures to return identification cards; upon termination of employment
- The length of time required by the Proposer to perform the identity check/background screening and to issue an identification card
- Details on what constitutes an exception to the identity check/background screening and actions taken as a result thereof;

Proposer employees, subcontractors, principles and concerned related parties may also be subjected to a Criminal History Background check completed by law enforcement in the Port Authority Police Department at the request of the Port Authority.

(6) **Business Risk**

The Proposer shall describe its policies, procedures, and strategies to review and address financial and technical business risks.

G. Acknowledgment of Addenda

If any Addenda are 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.

H. Acceptance of Standard Contract Terms and Conditions

The Port Authority has attached to this RFP as Part II, General Standard Contract Terms and Conditions governing the Contract. The Proposer is expected to agree with these General Standard Contract Terms and Conditions . However, if the Proposer has any specific exceptions, such exceptions should be set forth in a separate letter included with its response to this RFP.

The Proposer will be precluded from raising any exceptions not set forth in such a letter unless they are justified by changes in the scope of work or other requirements that are agreed to by the Proposer and the Port Authority.

I. M/WBE Plan

The Proposer shall submit an M/WBE Plan in accordance with the section of this RFP entitled "M/WBE Subcontracting Provisions".

7. 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 to whom RFP's were mailed. 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, 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

Sales to the Port Authority are currently exempt from New York and New Jersey states and local sales and compensating use taxes and generally from federal taxation. 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. Right to Extend Contract

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

M. 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 therefore 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.

N. No Personal Liability

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

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, ideas, models, drawings, or other material communicated or exhibited by us or on our behalf) is not to 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 letter, either orally or in writing, is not given in confidence. Such information may be used, or disclosed to others, for any purpose at any time without obligation or compensation and without liability of any kind whatsoever. Any statement which is inconsistent with this agreement, whether made as part of or in connection with this agreement, shall be void and of no effect. This Agreement is not intended, however, to grant to the Port Authority rights to any matter which is the subject of valid existing or potential letters patent. The foregoing applies to any information, whether or not given at the invitation of the Port Authority.

Notwithstanding the above, and without assuming any legal obligation, the Port Authority will employ reasonable efforts, subject to the provisions of the Port Authority's Freedom of Information Resolution adopted by its Committee on Operations on August 13, 1992, not to disclose to any competitor of the undersigned, information submitted which are trade secrets or is maintained for the regulation or supervision of commercial enterprise which, if disclosed, would cause substantial injury to the competitive position of the enterprise, and which information is identified by the Proposer as proprietary, which may be disclosed by the undersigned to the Port Authority as part of or in connection with the submission of a proposal.

_____
(Company)

_____
(Signature)

_____
(Title)

_____
(Date)

Freedom of Information – Port Authority Policy and Procedure

In 1977, the Committee adopted a policy for access by the public to records maintained by the Port Authority. While based on the policy therefore declared by the States of New York and New Jersey, with respect to access by the public to public records, inasmuch as the respective New York and New Jersey statutes differed (and continue to differ) as to certain policy particulars and provide for different procedures for implementation of the policy, it was deemed desirable for the Committee to adopt a separate Port Authority Policy and Procedure. In light of action new being taken by the Board with respect to open public meetings, it is appropriate at this time to restate the basic principles and reflect necessary procedural changes.

Pursuant to the foregoing report, the following resolution was adopted with Commissioners Burgos, Hellmuth, Henderson and Kaltenbacher voting in favor, none against:

> **RESOLVED**, that government, including the activities and decisions of The Port Authority of New York and New Jersey (and its wholly-owned subsidiary corporations) is the public's business and therefore the public should have access to the records of the Port Authority (and its subsidiaries) as herein provided for; and it is further
>
> **RESOLVED,** that the resolution of the Committee on Operations adopted on September 28, 1977, regarding Freedom of Information (which resolution appears at pages 12 et seq. Of the Committee Minutes for that date) shall be, and it hereby is rescinded; and it is further
>
> **RESOLVED,** that all records of the Port Authority (and its subsidiaries), including records stored electronically such as on computer tapes or disks, shall be made available for public inspection and copying, except that such access may be denied as to records or portions of thereof which:

(1) are rendered confidential or privileged or are exempted from disclosure by Federal or state law or regulations or rules of the court;

(2) if disclosed, would constitute an unwarranted invasion of personal privacy (including personnel, medical, or disciplinary records, and any lists of names and address to be used for profit or financial gain);

(3) if disclosed, would impair present or future awards or negotiations, including collective bargaining or negotiations, of leases, permits, contracts, or other agreements;

(4) are trade secrets or are maintained for the regulation or supervision of commercial enterprise which, if disclosed, would cause injury to the competitive position of the enterprise;

(5) are compiled for public safety, law enforcement, or official investigative purposes (internal or external) when their disclosure may affect public safety, interfere with internal investigations, audits, law enforcement investigations, or judicial or disciplinary proceedings, or deny or prejudice a right to a fair trial or impartial adjudication, or identify a confidential source or disclose confidential information

relating to an audit or a civil, criminal, or internal or external disciplinary investigation.

(6) if disclosed, would endanger the life and safety of any person;

(7) are inter-agency or intra-agency materials other than statistical or factual tabulations of data, provided that instructions to staff that affect public or final agency policy or determinations are not exempted;

(8) are examination questions or answers which are requested prior to final administration of such questions; or

(9) could affect or impact the competitive economic position of the Port District, the Port Authority, or specific business entities with which the Port Authority deals;

and it is further

RESOLVED, that the Secretary of the Port Authority shall maintain a current list of subject nature and category of all records in the possession of the Port Authority (and its subsidiaries) whether or not they are available for public copying and inspection, and the Secretary shall, under the direction of the Executive Director, administer the following rules and regulations with respect to public inspection and copying are available records:

Procedures

Requests for inspection or copying of public records of the Port Authority shall be made to the Secretary of the Port Authority upon a form prescribed by the Port Authority and shall contain sufficient information to identify the particular record sought. Such requests shall be made either:

(1) In person during regular business hours at the Port Authority's main office or

(2) By mailing such request, postage prepaid to said Secretary, The Port Authority of New York and New Jersey, at the aforesaid address, Attention: FOI Administrator.

Upon receipt of a request, the Secretary of the Port Authority shall promptly determine whether or not the record requested can be made available and will notify the person making the request of such determination. If the request is granted, such person shall also be notified where and when the record will be made available. The Port Authority will provide an opportunity for inspection and copying of the record.

The record may be inspected only under the supervision of the Secretary of the Port Authority or such other officer or employee as may be designated by the Secretary in the Office of the Secretary during regular business hours or at such other times or places as the Secretary deems convenient.

(1) Documents which are to be copied will be copied by The Port Authority, if practicable,

and the person requesting a copy will be charged a fee equal to the Port Authority's cost but no less than 25 cents for each page of the first ten, 15 cents for each page of the second ten, and 10 cents for each

additional page. If it is not practicable for the Port Authority to copy such documents, they will be copied commercially and the person requesting the copy will be charged a fee equal to the Port Authority's cost of such commercial reproduction. Documents which have been purchased by the Port Authority commercially (such as stenographic transcripts) may be copied and the person requesting the copy will be charges a fee no less than the amount paid by the Port Authority for such documents.

(2) A fee of no less than two dollars will be charged for certification by the Secretary of the Port Authority as to authenticity of any document, or that a record of which the Port Authority is legal custodian cannot be found.

(3) In the event a search for records requested requires more than one person hour, or in the event a search of computer records requires programming which would take more than one person hour, a fee will be charged at the rate of not less than five dollars per hour, or any part thereof, per person assigned to such search or programming.

(4) All such fees shall be paid by the person making the request in cash, certified check, or cashier's check, in advance or at any time of the delivery of any record for inspection or copies of any records or certificate referred to in this procedure.

The Secretary of the Port Authority, or the Secretary's designee, shall respond to each request within ten business days of the receipt thereof. The response shall provide reasons for the denial of access or copying or a statement of the time and place when the record requested will be made available.

Appeals

A. Any person who is denied access to a public record of the Port Authority (or its subsidiaries) by the Secretary of the Port Authority may file an appeal from such denial with the Port Authority's General Counsel (who serves as Counsel to the subsidiaries).

B. Such appeal shall be accompanied by a memorandum in support thereof setting forth the reasons why the appellant is entitled to access to the record requested.

C. Appeals pursuant to this procedure shall be decided by General Counsel or his designee. If the appeal is denied, the reasons therefore shall be explained fully in writing within seven business days of the date on which such appeal is received by General Counsel.

PART II - CONTRACT TERMS AND CONDITIONS

TABLE OF CONTENTS

PART II – GENERAL CONTRACT SPECIFIC TERMS AND CONDITIONS

1. General Agreement	24
2. Duration of Contract	24
3. Prevailing Wage (Davis-Bacon-Act)	25
4. Definitions	26-28
5. General Provisions	28-29
6. Intellectual Property	29-30
7. Indemnity in Request to Infringement	30-31
8. Property Rights in Subject Matter Not Within Software License	31
9. Time	31
10. Required Service Level Liquidated Damages for Non-Performance	32-33
11. Support Services Payment	33-34
12. Extra Work	34
13. Compensation for Extra Work	34
14. Extra Work Procedures	35
15. Performance of Extra Work	35
16. Final Payments	35
17. Termination of Agreement	36-37
18. Withholding of Payments	37
19. Contractor Personnel Standards of Performance	37
20. Harmony	38-39
21. High Security Areas	39
22. Notification of Security Requirements	39-40
23. Insurance Procured By the Contractor	40-42
24. Assignments and Subcontracts	42
25. Certain Contractor's Warranties	43-44
26. Right and Remedies of the Authority	44-45
27. Right and Remedies of the Contractor	45
28. Tax Exemptions, Duties and Imposts	45-46
29. Title of Equipment	46
30. Notice Requirements	47-48
31. Services of Notices on the Contractor	48
32. No Third Party Rights	48
33. Indemnifications	48
34. Risks Assumed by the Contractor	48-50
35. Port Authority Technology Standard	50
36. Applicable Law	50
37. Authority of the Director	50-51
38. Approval by the Director	51
39. Contractor Review and Compliance Audits	52
40. Authority Access to Records	52-53

41. Claims of Third Persons 53
42. Performance of Work as Agent for Contractor 53
43. Discrimination in Employment, Equal Employment and Opportunity 53
44. Integrity 53-58
45. Confidential Information 58
46. Provision of Law Deemed Inserted 59
47. Invalid Clauses 59
48. Estoppel or Waiver 60
49. Non-Liability of the Authority Representatives 60
50. Modification of Contract 60
51. M/WBE Subcontracting Provisions 60
52. Entire Agreement 61

Part II - General Contract Provisions

1. General Agreement

The undersigned (hereinafter referred to as the "Contractor" or "you") agrees to provide, and The Port Authority of New York and New Jersey (hereinafter referred to as the "Authority") agrees to purchase Maintenance Services for the ACS system including software and hardware support management and System Administration Services as more fully set forth in the Scope of Work attached hereto and made a part hereof. The Contractor shall also furnish management maintenance support of the operating systems, databases and all software including proprietary software all as more fully set forth in the Scope of Work attached hereto and made a part hereof. The Scope of Work requires the doing of all things necessary or proper for or incidental to the requirements as set forth in the Scope of Work. All things not expressly mentioned in the Scope of Work but involved in carrying out their intent are required by the Scope of Work and the Contractor shall perform the same as though they were specifically mentioned, described and delineated.

Subject only to the provisions of the clause herein entitled: "Extra Work", the Contractor's sole compensation in full consideration for the performance of all the Contractor's obligations under this Contract shall be the amounts computed in accordance with the Pricing Sheets annexed hereto and made a part hereof.

2. Duration of Contract

This agreement shall commence upon complete execution of a Contract award letter by the Port Authority and the Contractor and shall remain in effect for a period of three (3) years (hereinafter the "Base Term") unless otherwise terminated in accordance with the provisions hereof.

The Authority shall have the right at its sole option to extend this Contract for up to two (2) additional two (2) year periods ("Option Periods") and an additional 120 day period, from the date originally fixed for expiration upon the same terms and conditions except as set forth elsewhere in this Agreement, to be effected by written notice to the Contractor received no later than thirty (30) days prior to original expiration date or the expiration date of the extended period then in effect, if applicable.

All Contract prices for services shall be applicable to the three years of the Base Term. For the first and second Option Periods that are applicable to this Contract and are exercised hereunder, (excluding the 120 day Extension Period as described in the paragraph entitled "Extension Period" in Part II, hereof) the Port Authority shall adjust the compensation due the Contractor utilizing the Consumer Price Index for all Urban Consumers; Series Id: CUURA101SA0L2; Not Seasonally Adjusted; New York-Northern New Jersey-Long Island, NY-NJ_CT-PA area; all items less shelter; 1982-1984=100, published by the Bureau of Labor Statistics of the United States Department of Labor (hereinafter called the "Price Index")_.

(a) For the first two-year option period of the Contract, the Price Index shall be determined for the fourth Quarter 2009 shall be obtained. The compensation for services payable in the third year of the Base Term of the Contract shall be multiplied by a fraction, the numerator of which shall be said Index for the fourth Quarter of 2009 and the denominator of which shall be said Index for the fourth Quarter of 2007. The resulting product shall be the compensation payable for services in the first option period.

(b) For the second two-year option period of the Contract, the Index for the fourth Quarter 2010 shall be obtained. The compensation for services payable in the second year of the first option period of the Contract shall be multiplied by a fraction, the numerator of which shall be said Index for the fourth Quarter of 2010 and the denominator of which shall be said Index for the fourth Quarter of 2008. The resulting product shall be the compensation payable for services and in second option period.

(c) In the event of a change in the basis for the computation of the said Index or the discontinuance of its publication, such other appropriate index shall be substituted as may be agreed upon by the Authority and the Contractor as properly reflecting changes in the value of the services similar to that established in the said Index.

(d) The Contractor's compensation for service costs for the 120-day extension option shall not be subject to adjustment. Labor and service costs for the 120-day extension period shall be the same as in effect during the contract year prior to the start of the 120-day option.

The provisions in the foregoing paragraphs with respect to extension of the term of the contract shall be null and void if the contract has been terminated or revoked during the initial term or any extension thereof.

3. Prevailing Wage (Davis-Bacon Act)

The Contractor shall pay of provide (and shall cause all subcontractors to pay or provide) to his or their workmen and laborers (who are employed by him or them to work on an hourly or daily basis at any trade or occupation at or about the Site of the Work) at least the prevailing rate of wage and supplements for others engaged in the same trade of occupation in the locality in which the Work is being performed as determined by the Authority.

For the purposes of this Contract, The Authority has determined that the prevailing rates of wage and supplements are those established by the Secretary of Labor of the United States pursuant to the Davis-Bacon Act (40 U.S.C.A. 276a) for the locality in which the Work is to be performed. The applicable rates shall be those which are in effect on the date of Contract execution.

The provisions of this numbered clause are inserted in this Contract for the benefit of such workmen and laborers as well as for the benefit of the Authority; and if the Contractor or any subcontractor shall pay or provide any such workman or laborer less

than the rates of wages and supplements above described, such workman or laborer shall have a direct right of action against the Contractor or such subcontractor for the difference between the wages and supplements actually paid or provided and those to which he/she is entitled under this clause. If Such workman or laborer is employed by any subcontractor whose subcontract does not contain a provision substantially similar to the provisions of this clause (requiring the payment or provision of at least the above minimum and providing for a cause of action in the event of the subcontractors failure to pay or provide such wages and supplements) such workman or laborer shall have a direct right of action against the Contractor. The Authority shall not be a necessary party to any action brought by any workman or laborer to obtain a money judgment against the Contractor or any subcontractor pursuant to this numbered clause.

Nothing herein contained shall be construed to prevent the Contractor or any subcontractor from paying higher rates or providing higher supplements that the minimum hereinbefore prescribed The Port Authority does not represent that required labor may be obtained for the specified wages/benefits.

4. Definitions

The term "**days**" or "**calendar days**" in reference to a period of time shall mean consecutive calendar days, Saturdays, Sundays and holidays, included. The term "**week**", unless otherwise specified, shall mean seven (7) consecutive calendar days, Saturdays, Sundays, and holidays included.

The term "**month**", unless otherwise specified, shall mean a calendar month.

"**Work**" shall mean all structures, equipment, plant, labor, materials (including materials and equipment, if any, furnished by the Authority) and other facilities, and all other things necessary or proper for, or incidental to the activities at the Site of the Work.

The term "**Site of the Work**", "Facility", or words of similar import shall mean:

"**Director**" shall mean the Director of Tunnels, Bridges, and Terminals Department and/or the Director of Aviation for the purpose of this Contract, acting personally or through one of his/her authorized representatives for the purpose of this Contract.

"**Facility Manager and/or Contract Manager**" shall mean the person designated by the Director to manage all aspects of this Contract or his/her successor in duties for the purpose of this Contract, acting personally or through his/her duly authorized representative.

"**Facility Manager**" shall mean the General Manager of each of the "**Work Sites**" listed above or his/ her successor in duties for the purpose of this Contract, acting personally or through his/her duly authorized representative.

No persons other than those specifically identified above shall be deemed a representative of the Director or of the Contract Manager except to the extent specifically authorized in an express written notice to the Contractor signed by the Director or the Contract Manager, as the case may be. Further, no person shall be

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

"**Subcontractor**" shall mean anyone who performs Work (other than or in addition to the furnishing of materials, plant or equipment) at or about the Site of the Work directly or indirectly for or on behalf of the Contractor (and whether or not in privity of Contract with the Contractor).. "SubContractor", however, shall exclude the Contractor or any subsidiary or parent of the Contractor or any person, firm or corporation which has a substantial interest in the Contractor or in which the Contractor or the parent or the subsidiary of the Contractor, or an officer or principal of the Contractor or of the parent or the subsidiary of the Contractor has a substantial interest, provided, however, that for the purpose of the clause hereof entitled "Assignments and SubContracts" the exclusion in this paragraph shall not apply to anyone but the Contractor.

The term "**maintenance**" or words of similar import, as used herein, shall mean the aggregate of the following: preventative and corrective maintenance, periodic inspection, testing and remedial repairs of the systems as specified herein. Such maintenance shall include the furnishing and replacing of any parts or items of equipment that may be required to keep all the system components in working order, 24 hours a day 7-days a week. However, such maintenance shall not include the furnishing and replacing of any parts of items of equipment that may be required as the result of damage caused by accident, abuse or negligence not attributable to employees of the Contractor as is demonstrated to the satisfaction of the Manager, which shall constitute Extra Work.

"**Materialmen**" shall mean anyone who furnishes materials, plant or equipment (including temporary or consumable materials) to the Contractor or any subcontractor for use at or about the work site in the performance of Work.

The term "**Authority**" refers to the Port Authority of New York and New Jersey.
"**Notice**" shall mean a written notice.

Reference to Work or its performance, "directed", "required", "permitted", "ordered", "designated", "prescribed", and words of similar import shall mean directed, required, permitted, ordered, designated, or prescribed but the Manager; and "approved", "acceptable", "satisfactory" and words of similar import shall mean approved by or acceptable or satisfactory to the Manager; and "necessary", "reasonable", "proper", "correct" and words of similar import shall mean necessary, reasonable, proper, or correct in the judgments of the Manager.

"**First in, First out (FIFO)**" – A queuing principle in which entities in a queue leave the queue in the same order in which they arrive.

"**Burn-in**" – To test for defects by operating a component, equipment or software for a continuous period of time.

"**ACS**" shall refer to the Access Control System

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

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

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

5. General Provisions

A. No certificate, payment, (final or otherwise), acceptance of any work nor any other act or omission of the Authority shall operate to release the Contractor from any obligations under or upon this agreement, or to stop the Authority from showing at any time, that such certificate, payment, acceptance, act or omission was incorrect or to preclude the Authority from recovering any monies paid in excess of that lawfully due, whether under mistake of law or fact or to prevent the recovery of any damages sustained by the Authority.

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

C. Under no circumstances shall Contractor or any subcontractors communicate in any way with any department, board, agency, commission, or other organization or any person whether governmental or private in connection with the services to be performed hereunder except upon prior written approval and instructions of the Director, provided, however, that data from manufacturers and suppliers of materials, devices and equipment shall be obtained by the Contractor when it finds such data necessary unless otherwise instructed by the Authority.

D. Any services performed for the benefit of the Authority at any time by the Contractor or on the Contractor's behalf, even if expressly and duly authorized by the Authority, shall be deemed to be rendered under and subject to this Agreement (unless referable to another expressly written, duly executed agreement by the same parties), whether such additional services are performed prior to, during or subsequent to the services described herein, and no rights or obligations shall arise out of such additional services except as provided under this Agreement.

E. The Contractor shall observe and obey (and compel its officers, employees, guests, invitees, and those doing business with it, to observe and obey) the rules and regulations of the Port Authority now in effect, and such further rules and regulations which may from time to time during the effective period of this Contract, be promulgated by the Port Authority for reasons of safety, health, preservation of property, or maintenance of a good and orderly appearance of the Facilities, or for the safe and efficient operation of the Facilities. The Port Authority agrees that, except in cases of emergency, it shall give notice to the Contractor of every rule and regulation hereafter adopted by it.

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

6. Intellectual Property

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

B. All pre-existing information or documentation including computer programs or code including source code, of the Contractor, utilized by the Contractor hereunder in the performance of his services hereunder shall be deemed perpetually licensed to the Authority for the purposes of this agreement, but shall remain the property of the Contractor.

C. Third party software not specially prepared for the purpose of this agreement but utilized by the Contractor hereunder in the performance of his services hereunder shall be licensed to the Contractor and the Authority for the term of this agreement.

D. The above-described software shall be furnished by the Contractor without additional compensation.

E. The right of the Authority as well as the Contractor to use all patented material, compositions of matter, manufactures, apparatus, appliances, processes of manufacture or types of construction as well as any copyrightable matter, trade secrets or other proprietary matters, shall be obtained by the Contractor without separate or additional compensation whether the same is patented before, during or after the performance of the Work.

7. Indemnity in Regard to Infringement- Research and Development

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

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

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

successors, immediate or otherwise, in the operations of or ownership of any facility now or hereafter operated by the Authority or the Authority but such license shall not be otherwise transferable.

8. NOT USED

9. Time

The Contractor shall not commence the performance of any work on Authority premises until the Contractor has received notice from the Authority that the insurance provided by the firm in accordance with the clause hereof entitled "Insurance to be Provided by the Contractor" is satisfactory, as evidenced by the certificate to be furnished under said clause. The Contract term shall not be extended on account of the time required to furnish the documents referred to above, but the Authority shall give notice to the Contractor within five (5) days after receipt of the certificate of insurance as to whether or not such insurance is satisfactory.

The Contractor's obligations for the performance and completion of all work within the time or times provided for in this Contract are of the essence of this Contract. The Contractor guarantees that he can and will complete performance under this Contract within the times herein stipulated.

10. Required Service Levels and Damages for Non-Performance

The Contractor's obligations for the performance of all work at the service levels specified in this Contract are of the essence. The Contractor guarantees that he can and will complete performance under this Contract at the service levels stipulated in the Scope of Work. The Authority may consider continued failure to meet performance under this Contract at the levels stipulated as a material breach of this Contract. Service level monitoring and damages assessed will begin immediately at the end of a 60-calendar day transition period beginning on the date of contract award. Inasmuch as the damage and loss to the Authority which will result from the Contractor's failure to perform at these levels will include items of loss whose amount will be incapable or very difficult to accurately estimate, the damages to the Authority for non-performance will be liquidated as follows:

SERVICE	SERVICE LEVEL	LIQUIDATED DAMAGES FOR NON-PERFORMANCE
"Operational Availability" for host services measured monthly		See Attachment C, Scope of Work
Resolution of workstation service calls measured monthly		See Attachment C, Scope of Work
Patch and updates maintenance	The Contractor shall apply by facility all critical security, operating system and database system patches within 24 hours of their approval by the Port Authority. All other patches, updates and service packs shall be deployed within 10 business days.	For critical patches, 5% of total monthly payment for system administration for the affected facility per each 24-hour period patch is not installed after the initial 24 hours. For non-critical patches, 2% of total monthly payment for system administration for the affected facility per each 24-hour period patch is not installed after the initial 10 business days.
Lost or damaged facility keys	Failure to return or return of damaged keys as specified in Attachment C, Scope of Work.	Fee as set forth in Attachment C, Scope of Work.

Credits for damages shall be applied to the previous monthly invoice for system administration services.

Additional liquidated damages for non-performance is described fully in Attachment C, Scope of Work. Credits for damages shall be applied to the previous monthly invoice for preventive and corrective maintenance services.

Computation of on-line availability and resolution of calls refers specifically to work covered in this Contract which is the Contractor's responsibilities.

The Contractor shall not be charged with delay, or assessed Liquidated Damages for delay or failure, which occurs for reasons beyond the reasonable control of the Contractor or subcontractors as determined by the Port Authority.

11. Support Services Payments

On or prior to the fifth (5th) day of each calendar month during the term of this Contract including the calendar month immediately following the expiration or termination of this Contract, the Contractor shall submit monthly invoices for the performance of services in the prior month accompanied by a complete itemization thereof and such records and other information that the Director shall require. The Contractor's invoices for payment shall bear the Contractor's Federal Identification Number. The Contractor shall submit all invoices to the following:

George Washington Bridge
Physical Plant Manager
220 Bridge Plaza South
Forth Lee, N.J. 07024

Holland Tunnel
Physical Plant Manager
13th & Provost Streets
Jersey City N.J. 07310

Lincoln Tunnel
Physical Plant Manager
500 Boulevard East
Weehawken, N.J. 07087

Staten Island Teleport
Contract Manager
220 Bridge Plaza South
Fort Lee, N.J. 07024

The Contractor shall breakout, per facility (GWB, HT and LT) separately the amount due for all equipment provided and services performed in the previous month using the price breakdown set forth in Cost Proposal.

The Port Authority shall, at the receipt of Contractor invoice and upon certification to the Port Authority and the Contractor by the Director (after receipt from the Contractor of such additional information as the Director may require including certificiation of payment of mandated wages and benefits), pay to the Contractor by check payments within 30 days after certification of the Contractor's invoices by the Director.

The Contractor shall not perform extra work or any additional services without prior written approval from the Facility Manager and/or Contract Manager.

The Contractor shall furnish to the Contractor Manager a quarterly report detailing all invoices submitted in that quarter. At a minimum, the report should include, invoice number, payment by type (i.e., monthly lump sum, extra work, etc.,). The report shall be submitted to:

George Washington Bridge
Contract Manager
220 Bridge Plaza South
Fort Lee, N.J. 07024

12. Extra Work

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

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

The Director shall have the authority to order Extra Work up to an amount equal to six percent (6%) of the total estimated Contract price unless the Contractor is advised of a greater authorization in a letter signed by the Authority's Director of Procurement. Nothing herein shall be construed as a presentation that any changes or additions will be ordered.

13. Compensation For Extra Work

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

A. the actual cost in money of the labor (including premiums for workers' compensation insurance, taxes, vacation allowances and union dues and assessments required to be paid by the employer on the basis of such labor costs) and material required for such extra work.

B. ten (10%) of the amount under (a) above,

C. in addition to the foregoing, if the extra work is performed by a subcontractor, five percent (5%) of the amounts under (a) and (b) above. No extra work shall be performed by a subcontractor without the prior written approval of the Director.

D. The Contractor shall be reimbursed for his actual costs of equipment rental if approved by the Contract Manager.

14. Extra Work Procedures

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

15. Performance of Extra Work

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

16. Final Payment

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

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

Within thirty days (30) after issuance of such certificate of total compensation earned (or within thirty days (30) after receipt of the documents provided for in the immediately preceding paragraph, if required and if such date is later), the Port Authority shall pay to the Contractor by check the amount stated in said certificate, less all other payments and advances whatsoever to or for the account of the Contractor. All prior estimates and payments shall be subject to correction in this payment, which is throughout this Agreement called the Final Payment.

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

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

The Contractor agrees that he shall not be entitled to, and hereby waives any right he might otherwise have to, and shall not seek any judgment whether under this Contract or otherwise for any such Final Payment or for an amount equivalent thereto or based thereon, or for any part thereof, if such judgment would have the effect of varying, setting aside, disregarding or making inapplicable the terms of this numbered clause or have the effect in any way of entitling the Contractor to accept such Final Payment or an amount equivalent thereto or based thereon or any part thereof other than in the same fashion as a voluntary acceptance of a Final Payment subject to all the terms of this Contract including this numbered clause, unless and until the Contractor should obtain a judgment on any claim arising out of or in connection with this Contract (including a claim based on breach of contract) for an amount not included in said Final Payment. Interest on any late payment under this Contract shall be at 6% per annum.

17. Termination of Agreement

The Authority may at any time for cause terminate this Agreement or any portion of the Agreement as to any services not yet rendered, and may terminate this Agreement or any portion thereof without cause upon thirty (30) days notice to the Contractor. Contractor shall have no right of termination as to any services under this Agreement without just cause. Termination by either party shall be by certified letter addressed to the other at its address herein after set forth. Should this Agreement be terminated by either party as

above provided, you shall receive no compensation for any services not yet performed, but if termination is without fault on your part, the Authority shall pay you as the full compensation to which you shall be entitled in connection with this Agreement for the services satisfactorily performed through the date of termination an amount which the Director determines represents the portion of Pricing Sheet and Extra Work compensation equivalent to the work satisfactorily performed less any payments previously advanced. No allowance shall be made for anticipated profits. If the Authority terminates this contract for its own convenience the Authority shall compensate the Contractor in the amount of its non-cancellable obligations.

18. Withholding of Payments

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

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

In the event payments are wrongfully withheld interest shall be paid in the amount of 6% per annum.

19. Contractor Personnel Standards of Performance

The Contractor shall furnish sufficiently trained management, supervisory, and operating personnel to perform the services required of the Contractor under this Contract. If, in

the opinion of the Director, any of the Contractor's personnel are not satisfactory in the performance of services to be furnished hereunder, the Contractor shall remove such personnel and replace them with personnel satisfactory to the Director.

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

20. Harmony

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

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

B. During the time that the Contractor is performing the contract, other persons may be engaged in other operations on or about the worksite including Facility operations,

pedestrian, bus and vehicular traffic and other Contractors performing at the worksite, all of which shall remain uninterrupted.

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

21. High Security Areas

A. Services under the Contract may be required in high security areas, as the same may be designated by the Manager from time to time. The Port Authority shall require the observance of certain security procedures with respect to the high security areas, which may include the escort to, at, and/or from said high security areas by security personnel designated by the Contractor or any subcontractor's personnel required to work herein.

B. Twenty-four hours prior to the proposed performance of any work in high security area, the Contractor shall notify the Facility Manager and/or Contract Manager. The Contractor shall conform to the procedures as may be established by the Facility and/or Contract Manager from time to time and at any time for access to high security areas and the escorting of personnel hereunder. Prior to the start of work, the Contractor shall request a description from the Facility Manager and /or Contract Manager of the high security areas, which will be in effect on the commencement date. The description of high security areas may be changed from time to time and at any time by the Facility Manager and/or Contract Manager during the term of the Contract.

22. Notification of Security Requirements

In case of conflict, the requirements set forth in the Proposal Submission Requirements and Scope of Work shall take precedence over the security requirements in this section.

The Port Authority operates facilities and systems, at which terrorism or other criminal acts may have a significant impact on life safety and key infrastructures. The Authority reserves the right to impose multiple layers of security requirements on the performance of the Contract Work, including on the Contractor, its staff and subcontractors and their staffs depending upon the level of security required, as determined by the Authority. The Contractor shall and shall instruct its subcontractors to cooperate with Authority staff in adopting security requirements. These security requirements may include but may not be limited to the following:

i. Identity Checks and Background Screening

Contractor/subcontractor identity checks and background screening shall include but shall not be limited to: (1) inspection of not less than two forms of valid/current government issued identification (at least one having an official photograph) to verify staff's name and residence; (2) screening of federal, state, and/or local criminal justice agency information databases and files; (3) screening of any terrorist identification files; (4) multi-year check of personal, employment and/or credit history; (5) access

identification to include some form of biometric security methodology such as fingerprint, facial or iris scanning.

The Contractor may be required to have its staff, and any subcontractor's staff, authorize the Authority or its designee to perform background checks. Such authorization shall be in a form acceptable to the Authority. If the Authority directs the Contractor to have identity checks and background screening performed by a particular firm designated by the Authority, the Authority will compensate the Contractor for the cost of such screening on a net cost basis.

ii. Issuance of Photo Identification cards

If the Authority requires facility-specific identification cards for the Contractor's and subcontractors' staff, the Authority will supply one card per staff member of such identification cards at no cost to the Contractor. Copies of the identification card will be issued at a cost of $25.00 each.

iii. Access Control, Inspection, and Monitoring by Security Guards

The Authority will provide for facility access control, inspection and monitoring by Authority retained security guards. Should the Authority require the Contractor to hire security guards for the purpose of facility access control and inspection in lieu of or in addition to the Authority retained facility security guards, the Contractor will be reimbursed for the cost of such security guards pursuant to the Extra Work provisions of the Contract. However, this provision shall not relieve the Contractor of its responsibility to secure its equipment and work at the facility at its own expense.

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

23. Insurance Procured By The Contractor

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

Commercial General Liability Insurance - $ 3 million combined single limit per occurrence for bodily injury and property damage liability.

Automobile Liability Insurance - $ 3 million combined single limit per accident for bodily injury and property damage liability.

In addition, the liability policy (ies) shall name The Port Authority of NY and NJ as additional insured, including but not limited to premise-operations, products-completed operations on the Commercial General Liability Policy. Moreover, the Commercial General Liability Policy shall not contain any provisions for exclusions from liability other than provisions for exclusion from liability forming part of the most up to date ISO form or its equivalent unendorsed Commercial General Liability Policy. The liability policy (ies) and certificate of insurance shall contain cross-liability language providing severability of interests so that coverage will respond as if separate policies were in force for each insured. These insurance requirements shall be in effect for the duration of the contract to include any warrantee/guarantee period.

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

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

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

Each policy above shall contain a provision that the policy may not be canceled, terminated, or modified without thirty (30) days' prior written notice to the Port Authority of NY and NJ, Att: Facility Contract Administrator, at the location where the work will take place and to the General Manager, Risk Management.

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

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

If at any time the above liability insurance should be canceled, terminated, or modified so that the insurance is not in effect as above required, then, if the Manager shall so direct, the Contractor shall suspend performance of the contract at the premises. If the contract is so suspended, no extension of time shall be due on account thereof. If the contract is

not suspended (whether or not because of omission of the Manager to order suspension), then the Authority may, at its option, obtain insurance affording coverage equal to the above required, the cost of such insurance to be payable by the Contractor to the Port Authority.

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

The requirements for insurance procured by the Contractor shall not in any way be construed as a limitation on the nature or extent of the contractual obligations assumed by the Contractor under this contract. The insurance requirements are not a representation by the Authority as to the adequacy of the insurance to protect the Contractor against the obligations imposed on them by law or by this or any other Contract **(CITS # 2887N)**.

24. Assignments and Subcontracts

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

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

25. Certain Contractor's Warranties

The Contractor represents and warrants:

A. That he is financially responsible and experienced in, and competent to perform this Contract; that no representation, promise or statement, oral or in writing, has induced him to submit his Proposal, saving only those contained in the papers expressly made part of this Contract; that the facts stated or shown in any papers submitted or referred to in connection with his Proposal are true; and, if the Contractor be a corporation, that it is authorized to perform this Contract;

B. That he has carefully examined and analyzed the provisions and requirements of this Contract, that from his own investigations he has satisfied himself as to the nature of all things needed for the performance of this Contract, the general and local conditions and all other matters which in any way affect this Contract or its performance, and that the time available to him for such examination, analysis, inspection and investigations was adequate;

C. That the Contract is feasible of performance in accordance with all its provisions and requirements and that he can and will perform it in strict accordance with such provisions and requirements;

D. That no Commissioner, officer, agent or employee of the Authority is personally interested directly or indirectly in this Contract or the compensation to be paid hereunder;

E. That, except only for those representations, statements or promises expressly contained in this Contract, no representation, statement or promise, oral or in writing, of any kind whatsoever by the Authority, its Commissioners, officers: agents: employees or consultants has induced the Contractor to enter into this Contract or has been relied upon by the Contractor, including any with reference to: (1)the meaning, correctness, suitability or completeness of any provisions or requirements of this Contract; (2) the nature, existence or location of materials, structures, obstructions, utilities or conditions, which may be encountered at the installation sites; (3) the nature, quantity, quality or size of the materials, equipment, labor and other facilities needed for the performance of this Contract; (4) the general or local conditions which may in any way affect this Contract or its performance; (5) the price of the Contract; or (6) any other matters, whether similar to or different from those referred to in (1) through (5) immediately above, affecting or having any connection with this Contract, the bidding thereon, any discussions thereof, the performance thereof or those employed therein or connected or concerned therewith.

F. That, notwithstanding any requirements of this Contract, any inspection or approval of the Contractor's services by the Authority, or the existence of any patent or trade name, the Contractor nevertheless warrants and represents that the services and any intellectual property supplied to the Authority hereunder shall be of the best quality and shall be fully fit for the purpose for which they are to be used. The Contractor unconditionally guarantees against defects or failures of any kind, including defects or failures in design, workmanship and materials, excepting solely defects or failures which the Contractor demonstrates to the satisfaction of the Authority have arisen solely from accident, abuse or fault of the Authority occurring after issuance of Final Payment hereunder and not due

to fault on the Contractor's part. In the event of defects or failures in said services, or any part thereof, then upon receipt of notice thereof from the Authority, the Contractor shall correct such defects or failures as may be necessary or desirable, in the sole opinion of the Authority, to comply with the above guaranty.

Moreover, the Contractor accepts the conditions at the sites of work as they may eventually be found to exist and warrants and represents that he can and will perform the Contract under such conditions and that all materials, equipment, labor and other facilities required because of any unforeseen conditions (physical or otherwise) shall be wholly at his own cost and expense, anything in this Contract to the contrary notwithstanding.

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

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

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

26. Rights and Remedies of The Authority

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

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

For the purpose of this Contract, breach shall include but not be limited to the following, whether or not the time has yet arrived for performance of an obligation under this Contract: a statement by the Contractor to any representative of the Authority indicating

that he cannot or will not perform any one or more of his obligations under this Contract; any act or omission of the Contractor or any other occurrence which makes it improbable at the time that he will be able to perform any one or more of his obligations under this Contract; any suspension of or failure to proceed with any part of the Work by the Contractor which makes it improbable at the time that he will be able to perform any one or more of his obligations under this Contract; any false certification at any time by the Contractor as to any material item certified pursuant to the clauses hereof entitled "Certification of No Investigation (Criminal or Civil Anti-Trust), Indictment, Conviction, Debarment, Suspension, Disqualification and Disclosure of Other Required Information" and "Non-Collusive Bidding and Code of Ethics Certification; Certification of No Solicitation Based on Commission, Percentage, Brokerage, Contingent or Other Fee", or the willful or fraudulent submission of any signed statement pursuant to such clauses which is false in any material respect; or the Contractor's incomplete or inaccurate representation of its status with respect to the circumstances provided for in such clauses.

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

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

27. Rights and Remedies Of The Contractor

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

28. Tax Exemptions, Duties and Imposts

Sales to the Authority, as the governmental instrumentality of the States of New York and New Jersey, are exempt from taxation, either state or municipal, in those two states, and also from Federal taxation, including excise taxes. Certificate of Registry for tax-free transactions under Chapter 32 of the Internal Revenue Code is No. 13-730079K. The Contractor should retain a copy of this Contract to substantiate the exempt sale. The Contractor shall pay all duties and imposts, if any, on the importation of any materials.

The Authority is an organization exempt from the New Jersey State Sales and Use Tax Act, and the New York State and New York City Sales and Compensating Use Tax Act. In view of the foregoing, the Contractor should not include in his prices any amounts for New Jersey, New York State or New York City sales and use taxes on materials supplies and services.

If (I) any claim is made against the Contractor by New Jersey, New York State or New York City for such sales or compensating use taxes, or (II) any claim is made against the Contractor by a materialmen or subcontractor on account of a claim against such materialman or subcontractor by either State or the City for such sales or compensating use taxes, then the Authority will reimburse the Contractor in an amount equal to the amount of such tax required to be paid in accordance with the requirements of law, provided that:

A. the Contractor, or the Contractor and any such subcontractor, as the case may be, have complied with such rules and regulations as may have been promulgated relating to the claiming of the exemption from such taxes and have filed all forms and certificates required by the applicable laws, rules and regulations in connection therewith; and

B. the Authority is afforded the opportunity before any payment of tax is made, to contest said claim in the manner and to the extent that the Authority may choose and to settle or satisfy said claim, and such attorney as the Authority may designate is authorized to act for the purpose of contesting, settling and satisfying said claim; and

C. the Contractor, or the Contractor and any such subcontractor, as the case may be, shall give immediate notice to the Authority and its designated attorney in contesting said claim and furnish promptly to the Authority and said attorney all information and documents necessary to contest such claim which items shall be preserved for six (6) years after the date of Final Payment or longer if such a claim is pending or threatened at the end of such six (6) years.

If the Authority elects to contest any such claim, it will bear the expense of such contest.

29. Title to Equipment

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

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

30. Notice Requirements

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

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

A. In the case of any claims for which requirements are set forth elsewhere in this Agreement as to notice and information, such requirements shall apply.

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

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

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

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

waiver of any provision of this clause or as authority or apparent authority to effect such a waiver.

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

31. Service Of Notices On The Contractor

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

32. No Third Party Rights

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

33. Indemnification

The Contractor shall indemnify and hold harmless the Authority, its Commissioners, officers, representatives and employees, from and against all claims and demands, just or unjust, of third persons arising out of or alleged to arise out of or in connection with the Contractor's acts or omissions, and those of its officers, employees, agents and subcontractors, in the performance or non-performance of its services under this Contract, and for a all expenses incurred by the Authority in the defense, settlement or satisfaction thereof. If so directed, the Contractor shall at its own expense defend any suit based upon any such claim or demand, even if such suit, claim or demand is groundless, false or fraudulent, and in handling such shall not, without obtaining express advance permission from the General Counsel of the Port Authority, raise any defense involving in any way the jurisdiction of the tribunal over the person of the Port Authority, the immunity of the Port Authority, its Commissioners, officers, agents or employees, the governmental nature of the Port Authority or the provision of any statutes respecting suits against the Port Authority.

34. Risks Assumed By The Contractor

The Contractor assumes the following risks, whether such risks arise from acts or omissions (negligent or not) of the Contractor, the Authority, or the Contractor's subcontractors responsible for any aspect of the work required hereunder, or third persons or from any other cause: excepting only risks occasioned solely by affirmative, willful acts of the Authority done subsequent to the effective date of this Contract with the intent of causing the loss or damage,

A. The risk of loss or damage to property of the Authority arising out of the acts or omissions of the Contractor. The Contractor shall forthwith repair, replace, and make good any such loss or damage without cost to the Authority.

B. The risk of loss or damage to any property of the Contractor.

C. The risk of claims, just or unjust, by third persons against the Contractor or the Authority on account of personal injuries (including wrongful death) or property damage arising or alleged to arise out of or in connection with the Contractor's performance of the Contract, (whether or not actually caused by or resulting from the performance of the Contract) or out of or in connection with Contractor's operations or presence at or in the vicinity of Authority premises including claims for workers' compensation, whether such claims are made and whether such injuries, damage, or loss are sustained at any time both before and after the completion of the work provided for herein.

D. The risk of claims made against the Contractor or the Authority for loss or damage to any property of subcontractors, materialmen, workmen and others performing the Contract, occurring at any time prior to the completion or removal of such property from the Authority premises or the vicinity thereof.

The Contractor shall indemnify the Authority against all claims described in subparagraphs B, C and D above and for all expenses incurred by it in the defense, settlement or satisfaction thereof, including expenses of attorneys, except where indemnity would be precluded by the New York State General Obligations Law, Section 5-322.1. If so directed, the Contractor shall defend against any claims described in subparagraphs B, C and D above, in which event it shall not, without obtaining express advance permission from the General Counsel of the Authority, raise any defense involving in any way jurisdiction of the tribunal, immunity of the Authority, governmental nature of the Authority or the provisions of any statute respecting suits against the Authority. Such defense shall be at the Contractor's cost.

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

Neither the Authority's acceptance of the performance by the Contractor in part or in whole, nor the making of a payment shall release the Contractor from its obligations under this numbered clause.

Moreover, neither the enumeration in this numbered clause nor the enumeration elsewhere in this Contract of particular risks assumed by the Contractor or of particular claims for which it is responsible shall be deemed (a) to limit the effect of the provisions of this numbered clause or of any other clause of this Contract relating to such risks or claims, (b) to imply that it assumes or is responsible for risks or claims only of the type enumerated in this numbered clause or in any other clause of this Contract, or (c) to limit the risks which it would assume or the claims for which it would be responsible in the absence of such enumerations.

35. Port Authority Technology Standards and Guidelines

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

36. Applicable Law

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

37. Authority Of The Director

Inasmuch as the public interest requires that the Project to which this Contract relates shall be performed in the manner which the Authority, acting through the Director deems best, the Director shall have absolute authority to determine what is or is not necessary or proper for or incidental thereto and the Specifications shall be deemed merely the Director's present determination on this point. In the exercise of this authority, the Director shall have power to alter the Specifications, to require the performance of Work not required by them in their present form, even though of a totally different character from that not required, and to vary, increase and diminish the character, quantity and quality of, or to countermand any Work now or hereafter required. If at any time it shall be, from the viewpoint of the Authority, impracticable or undesirable in the judgment of the Director to proceed with or continue the performance of the Contract or any part thereof, whether or not for reasons beyond the control of the Authority, the Director shall have authority to suspend performance of any part or all of the Contract until such time as the Director may deem it practicable or desirable to proceed. Moreover, if at any time it shall be, from the viewpoint of the Authority impracticable or undesirable in the judgment of the Director to proceed with or continue the performance of the Contract or any part thereof for reasons within or beyond the control of the Authority, the Director

shall have authority to cancel this Contract as to any or all portions not yet performed and as to any materials not yet installed even though delivered. Such cancellation shall be without prejudice to the rights and obligations of the parties arising out of portions already satisfactorily performed, but no allowance shall be made for anticipated profits. To resolve all disputes and to prevent litigation, the parties to this Contract authorize the Director to decide all questions of any nature whatsoever arising out of, under, or in connection with, or in any way related to or on account of, this Contract (including claims in the nature of breach of contract or fraud or misrepresentation before or subsequent to acceptance of the Contractor's Proposal and claims of a type which are barred by the provisions of this Contract) in the first instance. The Director's decision may be based on such assistance as he/she may find desirable. The effect of the decision shall not be impaired or waived by any negotiation or settlement offers in connection with the question decided, whether or not he/she participated therein, or by any prior decision of his/her or others, which prior decisions shall be deemed subject to review, or by any termination or cancellation of this Contract.

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

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

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

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

38. Approvals by the Director

The approval by the Director of any service required hereunder, shall be construed merely to mean that at that time the Director knows of no good reason for objecting thereto and no such approval shall release the Contractor from his full responsibility for

the satisfactory performance of the services to be supplied. "Approved equal" shall mean approved by the Director.

39. Contract Review and Compliance Audits

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

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

40. Authority Access to Records

The Authority shall have access during normal business hours to all records and documents of the Contractor relating to any amounts for which the Contractor has been compensated, or claims he should be compensated, by the Authority. All Contractor records shall be kept in the New York Port District. The Contractor shall obtain for the Authority similar access to similar records and documents of subcontractors. Such access shall be given or obtained both before and within a period of three years after Final Payment to the Contractor, provided, however, that if within the aforesaid three years period the Authority has notified the Contractor in writing of a pending claim by the Authority under or in connection with this Contract to which any of the aforesaid records and documents of the Contractor or of his subcontractors relate either directly or indirectly, then the period of such right of access shall be extended to the expiration of six years from the date of Final Payment with respect to the records and documents involved.

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

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

The Contactor will provide system access and reasonable assistance to the Authority's External and Internal Audit Staff or its consultants in the performance of financial, system, security and operational reviews including producing specific requested information, extraction of data and reports. The Contractor shall support requests related to audits of the service level agreement and administration tasks and functions covered by the contract.

Contractor shall provide continuous access to the Authority to electronic data relating to the Contractor's performance under this Agreement.

The Authority reserves the right to use and load security and system software to evaluate the level of security and vulnerabilities in all systems that control this system.

Any External Audit staff or consultants accessing Contractor records shall be required to sign individual Contractor Non-Disclosure and Confidentiality Agreements.

41. Claims of Third Persons

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

42. Performance of Work as Agent for Contractor

In the exercise of its right to take over and complete Work as agent for the Contractor, for which provision is made in the clause hereof entitled "Rights and Remedies of the Authority", the Authority shall have the right to take possession of and use or permit the use of any and all plant, materials, equipment and other facilities provided by the Contractor for the purpose of the Work and the Contractor shall not remove any of the same from the site of the Work without express permission. Unless expressly directed to discontinue the performance of all Work, the Contractor shall continue to perform the remainder thereof in such manner as in no way will hinder or interfere with the portions taken over by the Authority. The exercise by the Authority of its right to take over the Work shall not release the Contractor from any of his obligations or liabilities under this Contract.

43. No Discrimination in Employment, Equal Employment Opportunity

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

A. The Contractor is advised to ascertain and comply with all applicable Federal, State and Local statutes, ordinances, rules and regulations and Federal Executive Orders pertaining to equal employment opportunity, affirmative action and non-discrimination in employment.

B. Without limiting the generality of any other term or provision of this Contract, in the event of the Contractor's non-compliance with any such statutes, ordinances, rules, regulations or orders, this Contract may be canceled, terminated, or suspended in whole or in part.

44. Integrity

A. 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 Proposer and each person signing on behalf of any Proposer certifies, and in the case of a joint bid each party thereto certifies as to its own organization, that the Proposer and each parent and/or affiliate of the Proposer has not:

- been indicted or convicted in any jurisdiction;
- 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 Proposer;
- 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;
- ever used a name, trade name or abbreviated name, or an Employer Identification Number different from those inserted in the Bid;
- 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 $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;
- 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
- 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.

B. 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 Proposer and each person signing on behalf of any Proposer certifies, and in the case of a joint bid, each party thereto certifies as to its own organization, that
- 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 Proposer or with any competitor;
- the prices quoted in its bid have not been and will not be knowingly disclosed directly or indirectly by the Proposer prior to the official opening of such bid to any other Proposer or to any competitor;
- no attempt has been made and none will be made by the Proposer to induce any other person, partnership or corporation to submit or not to submit a bid for the purpose of restricting competition;

- this organization has not made any offers or agreements or taken any other action with respect to any Authority employee or former employee or immediate family member of either which would constitute a breach of ethical standards under the Code of Ethics dated April 11, 1996 (a copy of which is available upon request to the individual named in the clause hereof entitled "Proposer's Questions"), 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; and
- no person or selling agency other than a bona fide employee or bona fide established commercial or selling agency maintained by the Proposer for the purpose of securing business has been employed or retained by the Proposer 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.
- The Proposer 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.

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

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

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

Moreover, the foregoing certifications, if made by a corporate Proposer, shall be deemed to have been authorized by the Board of Directors of the Proposer, 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 Proposer cannot make the foregoing certifications, the Proposer shall so state and shall furnish with the signed bid a signed statement which sets forth in detail the reasons therefor. If the Proposer 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.
Notwithstanding that the Proposer may be able to make the foregoing certifications at the time the Proposal is submitted, the Proposer shall immediately notify the Authority in writing during the period in which its Proposal is under consideration of any change of circumstances which might under this clause make it unable to make the foregoing certifications or require disclosure. The foregoing certifications or signed statement shall be deemed to have been made by the Proposer with full knowledge that they would

become a part of the records of the Authority and that the Authority will rely on their truth and accuracy in awarding this Contract. In the event that the Authority should determine at any time prior or subsequent to the award of this Contract that the Proposer has falsely certified as to any material item in the foregoing certifications or has willfully or fraudulently furnished a signed statement which is false in any material respect, or has not fully and accurately represented any circumstance with respect to any item in the foregoing certifications required; to be disclosed, the Authority may determine that the Proposer is not a responsible Proposer 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, Proposers 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.). Proposers are also advised that the inability to make such certification will not in and of itself disqualify a Proposer, and that in each instance the Authority will evaluate the reasons therefor provided by the Proposer.

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

Proposers 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 Proposer is not eligible to bid on or be awarded public contracts because the Proposer has been determined to have engaged in illegal or dishonest conduct or to have violated prevailing rate of wage legislation.

The policy permits a Proposer 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 Proposer, or (ii) the state agency determination relied upon was made without affording the Proposer the notice and hearing to which the Proposer was entitled by the requirements of due process of law, or (iii) the state agency determination was clearly erroneous or (iv) the state agency determination relied upon was not based on a finding of conduct demonstrating a lack of integrity or violation of a prevailing rate of wage law.

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

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

During the term of this Contract, the Proposer 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 Proposer 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 Proposer, 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 Proposer 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 addition, during the term of this contract, the Proposer shall not make an offer of employment or use confidential information in a manner proscribed by the Code of Ethics and Financial Disclosure dated April 11, 1996 (a copy of which is available upon request to the Office of the Secretary of the Port Authority).
The Proposer shall include the provisions of this clause in each subcontract entered into under this Contract.

E. Definitions

As used in this section, the following terms shall mean:

Affiliate - Two or more firms are affiliates if a parent owns more than fifty percent of the voting stock of each of the firms, or a common shareholder or group of shareholders owns more than fifty percent of the voting stock of each of the firms, or if the firms have a common proprietor or general partner.
Agency or Governmental Agency - Any federal, state, city or other local agency, including departments, offices, public authorities and corporations, boards of education and higher education, public development corporations, local development corporations and others.
Investigation - Any inquiries made by any federal, state or local criminal prosecuting agency and any inquiries concerning civil anti-trust investigations made by any federal, state or local governmental agency. Except for inquiries concerning civil anti-trust investigations, the term does not include inquiries made by any civil government agency concerning compliance with any regulation, the nature of which does not carry criminal penalties, nor does it include any background investigations for employment, or Federal, State, and local inquiries into tax returns.
Officer - Any individual who serves as chief executive officer, chief financial officer, or chief operating officer of the Bidder by whatever titles known.
Parent - An individual, partnership, joint venture or corporation which owns more than 50% of the voting stock of the Bidder.

If the solicitation is a Request for Proposal:

Bid - shall mean Proposal;
Bidder - shall mean Proposer;
Bidding - shall mean submitting a Proposal.

In a Contract resulting from the taking of bids:

Bid - shall mean bid;
Bidder - shall mean Bidder;
Bidding - shall mean executing this Contract.

In a Contract resulting from the taking of Proposals:

Bid - shall mean Proposal;
Bidder - shall mean Proposer;
Bidding - shall mean executing this Contract.

F. Conflict Of Interest

During the term of this Agreement, you shall not participate in any way in the preparation, negotiation or award of any contract (other than a contract for your own services to the Authority) to which it is contemplated the Authority may become a party or participate in any way in the review or resolution of a claim in connection with such a contract, if you have substantial financial interest in the contractor or potential contractor of the Authority or if you have an arrangement for future employment or for any other business relationship with said contractor or potential contractor, nor shall you at any time take any other action which might be viewed as or give the appearance of a conflict of interest on your 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 you have reason to believe such an arrangement may be the subject of future discussion, or if you have any financial interest, substantial or not, in a contractor or potential contractor of the Authority, and your 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 you have reason to believe that any other situation exists which might be viewed as or give the appearance of a conflict of interest you shall immediately inform the Director in writing of such situation giving the full details thereof. Unless you receive the specific written approval of the Director, you shall not take the contemplated action which might be viewed as or give the appearance of a conflict of interest. In the event the Director shall determine that the performance by you of a portion of your services under this Agreement is precluded by the provisions of this numbered paragraph, or a portion of your said service is determined by the Director to be no longer appropriate because of such preclusion, then the Director shall have full authority on behalf of both parties to order that such portion of your services not be performed by you, reserving the right, however, to have the services performed by others and reserving the right to reduce the lump sum compensation as he/she may deem reasonable in his/her sole discretion. Your execution of this Agreement shall constitute a representation by you that at the time of such execution you know 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 your part.

45. Confidential Information

Confidential information shall mean all information disclosed to the Contractor or the personnel provided by the Contractor hereunder which relates to the Authority's past, present, and future research, development and business activities including, but not limited to, software and documentation licensed to the Authority or proprietary to the Authority and all associated software, source code procedures and documentation. Confidential information shall also mean any other tangible or intangible information or materials including but not limited to computer identification numbers, access codes, passwords, and reports obtained and/or used during the performance of the Contractor's services under this Contract. The Contractor shall hold all such confidential information in trust and confidence for the Authority, and agree that the Contractor and the personnel provided by the Contractor hereunder shall not, during or after the termination or expiration of this Contract, disclose to any person, firm or corporation, nor use for its own business or benefit, any information obtained by it under or in connection with the supplying of services contemplated by this Contract. The Contractor and the personnel provided by the Contractor hereunder shall not violate in any manner any patent, copyright, trade secret or other proprietary right of the Authority or third persons in connection with their services hereunder, either before or-after termination or expiration of this Contract. The Contractor and the personnel provided by the Contractor hereunder shall not willfully or otherwise perform any dishonest or fraudulent acts, breach any security procedures, or damage or destroy any hardware, software or documentation, proprietary or otherwise, in connection with their services hereunder. The Contractor shall promptly and fully inform the Director in writing of any patent, copyright, trade secret or other intellectual property rights or disputes, whether existing or potential, of which the Contractor has knowledge, relating to any idea, design, method, material, equipment or other matter related to this Contract or coming to the Contractor's attention in connection with this Contract.

The Contractor and all involved subcontractors shall be required to sign a Non-Disclosure and Confidentiality Agreement (NDA) included herein as Attachment B prior to being granted access to documentation for the current system.

The Contractor shall adhere to the Port Authority's information security policies and procedures as published in the Port Authority's Technology Standards and Guidelines.

46. Provisions Of Law Deemed Inserted

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

47. Invalid Clauses

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

48. No Estoppel or Waiver

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

49. Non-Liability of The Authority Representatives

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

50. Modification of Contract

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

51. M/WBE Subcontracting Provisions

The Port Authority of NY & NJ has a long-standing practice of making its business opportunities available to Minority Business Enterprises (MBEs) and Women-owned Businesses (WBEs) and has taken affirmative steps to encourage such firms to seek business opportunities with the Port Authority. The successful Proposer will use every good faith effort to provide for meaningful participation by Port Authority certified M/WBEs as defined in this document, in all purchasing, subcontracting and ancillary service opportunities associated with this contract, including purchase of equipment, supplies and labor services. Good faith efforts include 1) dividing the services and materials to be procured into small portions where feasible, 2) giving reasonable advance notice of specific subcontracting and purchasing opportunities to such firms as may be appropriate, 3) soliciting services and materials from M/WBEs, which may be certified by the Port Authority and 4) insuring that provision is made for timely progress payments to the M/WBEs.

The Port Authority has a list of certified M/WBE firms, which are available to Proposers at their request. The Port Authority makes no representation as to the qualifications and ability of these firms to perform under this contract. The Proposer may use firms which are not on the list but will be required to submit, to the Port Authority's Small Business Programs (SBP) for certification, the names of M/WBE firms it proposes to use. Only

Port Authority certified M/WBE firms may be considered to meet the goals. For inquiries and assistance, please contact SBP at (212) 435-7819.

To the maximum extent feasible and consistent with the Proposer's exercise of good business judgment, the Proposer shall make a good faith effort to include 12% participation by MBE's and 5% participation by WBE's in all procurement, subcontracting and ancillary service opportunities associated with this contract.

52. Entire Agreement

This Contract including the Request for Proposals for Agreement to Perform Maintenance and System Administration Services of the Access Control System at George Washington Bridge and Bus Station, Holland Tunnel, Lincoln Tunnel and Staten Island Teleport (including its Scope of Works and other attachments, endorsements and exhibits, if any,) as well as the Proposal submitted by the Contractor contains the entire agreement between the parties. In the event of any inconsistency between this Contract and other attachments, endorsements and exhibits, if any, including the Proposal submitted by the Contractor, this Contract shall be controlling.

PART III – COST PROPOSAL SHEETS

ENTRY OF CHARGES:

The prices quoted shall be written in black or blue ink where required in the spaces provided on the Cost Proposal Sheets attached hereto and made a part thereof.

The Contractor is asked to make sure that all charges quoted for similar operations in the Contract are consistent.

The Contractor is asked to make sure that all figures are inserted as required, and that all computations have been verified for accuracy. The Contractor is advised that the Port Authority may, in its discretion, verify only that which it determines appropriate to verify and may not check for errors in each and every price submitted. In the event that the Contractor makes errors, the Port Authority reserves the right to correct any error and to recompute the Total Estimated Contract Price, as required, based upon the applicable unit price inserted by the Contractor, which amount shall govern in all cases.

In the event that a Contractor quotes an amount in the Estimated Total Price column but omits to quote a Unit Price for that amount in the space provided, the Port Authority reserves the right to compute and insert the appropriate Unit Price.

The Total Estimated Contract Price is solely for estimating and proposal evaluation purposes. Compensation shall be in accordance with the section of the Contract entitled "Contract Terms and Conditions" (Part II).

PART III - COST PROPOSAL SHEETS

EXHIBIT A

Preventive and Corrective Maintenance of the Access Control System - Three Year Base Term

(A)	(B)	(C)	(D)
Description	**Monthly Maintenance and Corrective Repair**	**X 12 Months**	**Estimated Total Annual Price**
George Washington Bridge		x 12	0
Holland Tunnel		x 12	0
Lincoln Tunnel		x 12	0
Staten Island Teleport - Servers and Workstations		x 12	0

Total Estimated Annual Maintenance Cost $ 0
(Sum of Item in Column D)

Note: All prices will be inclusive of materials and labor including software patches and replacements parts and components if required.

Note: Software updates and new releases for which the software vendor normally charges will be compensated as Extra Work. Installation thereof will not be separately compensated.

PART III - COST PROPOSAL SHEETS

EXHIBIT B

Computerized Maintenance Management System - Three Year Base Term

(A)	(B)	(C)	(D)	(E)	(F)
Software	**Cost per Authority Licensed User**	**Estimated Required Number of Authority Licensed Users**	**Monthly Total**	**X 12 Months**	**Estimated Total Annual Price**
Software Licenses (per user)		2	$0	x 12	$0
Other		2	$0	x 12	$0
Other:		2	$0	x 12	$0.00
Other:		2	$0	x 12	$0.00
Other:		2	$0	x 12	$0.00
Other:		2	$0	x 12	$0.00
Other:		2	$0	x 12	$0.00

Total Estimated Annual Price for Computerized Maintenance Management System $ **$0.00**
(Sum of Item in Column F)

The Contractor's compensation will commence once the Authority has accepted the system.

PART III - COST PROPOSAL SHEETS

EXHIBIT C

System Adminstration Services - Three Year Base Term

(A)	(B)	(C)	(D)
Description	**Monthly System Adminstration Services**	**X 12 Months**	**Estimated Total Annual Price**
George Washington Bridge		x 12	0
Holland Tunnel		x 12	0
Lincoln Tunnel		x 12	0
Staten Island Teleport		x 12	0

Total Estimated Annual System Adminstration Cost $ 0

(Sum of Item in Column D)

PART III - COST PROPOSAL SHEETS

EXHIBIT D

Miscellaneous Costs - Three Year Base Term

(A)	Cost to add additional operator workstation to the preventive maintenance schedule	$ _____
(B)	Cost to add door security setup to the preventive maintenance schedule (for example, inside/reader, strike lock or magnetic lock, audio/visual device)	$ _____
(C)	Cost to add a camera and PTZ units to the preventive maintenance schedule	$ _____
(D)	Cost to add motion detector device to the preventive maintenance schedule	$ _____
(E)	Cost to add Access Control Panel cabinet to the preventive maintenance schedule	$ _____
**(F)	Fiber Optic Repair Cost = $_____/hr * 36 hrs * 4 times/yr	$ _____
**(G)	Repositioning of Camera during Facility Cleanup = $_____/hr * 2 hrs/unit * 25 units/yr	$ _____
(H)	Purchase of security ID cards (Quantity of 1000)	$ _____
	Total Estimated 3 Year Price	$ 0 (Sum of Items Rows A - H)

Provide rates as requested above. Work may be requested at the sole discretion of the Contract Manager at any time during the term of the Contract. No work will be started without prior authorization.

**** Note: Normal working hours are between the hours of 6 AM - 6 PM , unless otherwise directed by the Contract Manager or the Facility Manager.**

PART III - COST PROPOSAL SHEETS

EXHIBIT E

Maintenance of Traffic

(A)	(B)	(C)	(D)
Description	**Closure per Month**	**X 12 Months**	**Estimated Total Annual Price**
George Washington Bridge	4	x 12	
Holland Tunnel	4	x 12	
Lincoln Tunnel	4	x 12	

Total Estimated Annual Maintenance Cost $ 0
(Sum of Item in Column D)

Note: Normal working hours are between the hours of 11 PM - 6 PM , unless otherwise directed by the Contract Manager or Facility Manager.

Note: The Proposer shall refer to the Extra Work sections in Part II for explanation of compensation.

PART III - COST PROPOSAL SHEETS

EXHIBIT F

Price Summary

(A) Estimated Total 3 Year Price - Preventive and Corrective Maintenance of the Access Control System
(Multiply total estimated annual price from Exhibit A by 3 years) $ _____

(B) Estimated Total 3 Year Price - Computerized Maintenance Management System
(Multiply total estimated annual price from Exhibit B by 3 years) $ _____

(C) Estimated Total 3 Year Price - System Adminstration Services
(Multiply total estimated annual price from Exhibit C by 3 years) $ _____

(D) Estimated Total 3 Year Price - Miscellaneous Costs
(From Exhibit D) $ _____

(E) Estimated Total 3 Year Price - Maintenance of Traffic
(Multiply total estimated annual price from Exhibit E by 3 years) $ _____
(The Proposer shall refer to the Extra Work sections in Part II for explanation of compensation)

TOTAL ESTIMATED CONTRACT PRICE
(Total items (A), (B), (C), (D) & (E) $ 0

ATTACHMENT B
NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT

THIS NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT (the "Agreement") is made as of this ____ day of _____, 2007, by and between The Port Authority of New York and New Jersey (the "Port Authority") a body corporate and politic created by Compact between the States of New York and New Jersey, with the consent of the Congress of the United States, and having an office and place of business at 225 Park Avenue South, New York, New York, 10003, and _____("Recipient"), a

WHEREAS, the Port Authority desires, subject to the terms and conditions set forth below, to disclose to Recipient confidential and privileged information in connection with **"Maintenance of Access Control System and System Administration Services for the George Washington Bridge, Lincoln Tunnel, Holland Tunnel and Staten Island Teleport Access Control System"** (collectively, the "Project(s)) and in addition, the Port Authority may deem it necessary to disclose on a need to know basis certain security and safety information which has been designated or is deemed to be Sensitive Security Information ("SSI"), and/or (Protected) Critical Infrastructure Information ("CII/PCII", as is further referenced and defined herein); and

WHEREAS, recognizing the need to share confidential and privileged information with Recipient and in furtherance of critical governmental interests regarding public welfare, safety and security at the Project site(s), the Port Authority has collected information and undertaken the development of certain plans and recommendations regarding the security, safety and protection of the Projects, including the physical construction and current and future operations of the Projects; and

WHEREAS, the Port Authority has developed the Security Program Handbook (the "Handbook") to address standard operating procedures, including the Port Authority's plan for implementation and application of uniform security procedures regarding the identification, handling, care and storage of Confidential and Privileged, and Confidential Information, as well as SSI and/or CII/PCII; and

WHEREAS, in order to protect and preserve the privilege attaching to and the confidentiality of the aforementioned information, as hereinafter defined, as well as to limit access to SSI and CII/PCII on a strict need to know basis, the Port Authority has requested, as a condition of its sharing and/or providing access to such confidential, privileged and sensitive information, that Recipient enter into this Agreement and that its respective officers, principals, contractors, agents, employees, contractors and consultants thereafter acknowledge that each such officer, principal, agent, employee, contractor or consultant understands that it will be required to treat as strictly confidential and privileged any such information so provided, as well as the work product and conclusions of any assessments and evaluations or any recommendations relating thereto and/or relating to any construction and operational information containing Confidential and Privileged, Confidential, SSI, CII/PCII, and to also fully comply with applicable federal rules and regulations with respect thereto

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, it is agreed and expressly understood and acknowledged as follows:

1. (a) "Confidential and Privileged Information" includes, but is not limited to, any and all information, documents and materials entitled to protection pursuant to the public interest privilege under New York State law, and exempted, protected or otherwise not subject to disclosure to third parties pursuant to New York, New Jersey, federal, or common law, in any form, format or medium, whether tangible or intangible, whether oral, written, photographic, optical or any other form, it being understood and agreed that all such information shall be designated "Confidential and Privileged" by the Port Authority. Certain Confidential and Privileged Information may also be designated or include SSI or CII/PCII, as defined below.

(b) "Confidential Information" includes, but is not limited to, any proprietary, business or other financial information and/or any information that is sensitive in nature, but not otherwise privileged, in any form, format or medium, whether tangible or intangible, whether oral, written, photographic, optical or any other form, it being understood and agreed that all such information shall be designated "Confidential" by the Port Authority.

(c) Certain information provided to the Recipients may be designated and/or include SSI as defined in the Transportation Security Administrative Rules & Regulations, 49 C.F.R. 1520, (49 U.S.C. § 114), the Office of the Secretary of Transportation Rules & Regulations, 49 C.F.R. 15, (49 U.S.C. § 40119), and/or CII/PCII as defined in the Office of the Secretary, Department of Homeland Security Rules and Regulations, 6 C.F.R. Part 29 (6 U.S.C. §131-134.) SSI and CII/PCII shall also be received and handled as required by the applicable federal regulations or as provided for by the responsible Federal agency or as may be provided for by any agreement between such Federal agency and the Port Authority. Information designated or including SSI and/or CII/PCII may also be designated, or include, Confidential and Privileged Information.

2. Pursuant to the aforementioned Federal Regulations, specifically 49 C.F.R. §§15.17 and 1520.17, any such violation thereof or mishandling of SSI therein defined "is grounds for a civil penalty and other enforcement or corrective action by the [Department of Transportation] DOT [Department of Homeland Security], and appropriate personnel actions for Federal employees. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure." Under federal regulations, specifically 6 C.F.R. §29.9, any violation of, mishandling, or misuse of CII/PCII is grounds for disqualification from future receipt of CII/PCII and/or SSI.

3. The first page of any document designated "Confidential and Privileged" or "Confidential" will be plainly marked as such. All information, documents and other material provided as such and, any part thereof, shall be deemed "Confidential and Privileged" or "Confidential", notwithstanding the fact that only the first page of a document or the container is actually marked; and

4. The first page of any document designated "SSI" or any container holding information designated "SSI" will be plainly marked "SENSITIVE SECURITY INFORMATION." All information, documents and other material provided as such, and any part thereof, shall be deemed "SSI", notwithstanding the fact that only the first page of a document or the container is actually marked.

5. All information provided to Recipient in any form, format or medium containing Confidential and Privileged, and/or Confidential Information shall be handled and treated with the highest care and in a manner consistent with the Port Authority's practices and procedures as set forth in the Handbook, as may be amended from time to time, and in a manner designed to prevent their disclosure to unauthorized third parties consistent with Port Authority security policy, practices and procedures, and all such information stored in the electronic form will be password protected.

6. Confidential and Privileged and/or Confidential Information shall be used solely for the purpose of aiding the Recipients in carrying out or undertaking their duly authorized responsibilities relating to the Projects and shall not be used, quoted, cited or otherwise replicated in any way and shall not be used as part of any draft or final communication, memorandum, report and/or other written, audio or visual medium.

7. The Confidential and Privileged and/or Confidential Information shall only be used in the performance of duly authorized activities relating to the Projects and shall not be used for any other purpose, except as expressly permitted by this Agreement, or as expressly directed in writing by the Port Authority, and, until such time that the information is no longer considered Confidential and Privileged and/or Confidential Information, it will be held and treated in the strictest confidence and shall not be disclosed either directly or indirectly to any other person who has not acknowledged and agreed to be bound by this Agreement and such information shall only be provided to such persons to the extent that it is required for use on the Recipient's behalf in performing its duly authorized activities at or in connection with the Projects and shall be provided only on a need-to-know basis; nor shall any copies of documents or materials in any form, format or medium, which contain disclosures of such Confidential and Privileged and/or Confidential Information, be made without the prior written consent of the Port Authority.

8. Confidential and Privileged and/or Confidential Information shall not be disclosed to persons other than those employed by or acting on behalf of the Recipient who have a need to know and/or a need to have access to the information without the express permission of the Port Authority in its sole discretion; and if such permission is granted then such information will be provided only upon the execution of an acknowledgment (the "Acknowledgement"), the form of which is attached hereto as Exhibit A, by the person receiving the information, agreeing to be bound by this Agreement.

10. If a subpoena, discovery request, Court Order, Freedom of Information Request, or any other request or demand authorized by law seeking disclosure of any Confidential and Privileged and/or Confidential Information is received, the Port Authority will immediately be

notified of such request or demand so that it may seek to quash the subpoena, seek a protective order, or take such other action regarding the request as it deems appropriate, and the undersigned will fully cooperate in the Port Authority's efforts in this regard so as to assure that confidential treatment will be afforded the Confidential and Privileged and/or Confidential Information. In the absence of the protective order, disclosure will be made of only that part of the Confidential and Privileged and/or Confidential Information as is required to be disclosed, after advising and consulting with the Port Authority, the Recipient and their respective counsel as to such disclosure and the nature and wording of such disclosure. If at any time the Confidential and Privileged and/or Confidential Information is inappropriately disclosed, the undersigned will immediately report that fact and the circumstances regarding such disclosure to the Port Authority.

11. Upon the earlier occurrence of either the Port Authority's written request, or termination of the business relationship or of the negotiations which gave rise to this Agreement, Recipient shall promptly return to the Port Authority, or destroy, at Recipient's expense, all tangible materials describing, analyzing, containing, or referring or relating to, the Confidential and Privileged and/or Confidential Information, including, but not limited to, all originals, extracts, studies, copies, and summaries, whether received from the Port Authority or created by Recipient, or its representatives, and regardless of the medium in which the Confidential and Privileged and/or Confidential Information was provided or maintained, including any information stored in electronic form, which shall also be completely removed from any computer database; provided, however, that Recipient may retain copies of Confidential and Privileged and/or Confidential Information in accordance with the requirements of this Agreement if (a) such retention is required for professional reasons, and (b) Recipient received the express written consent of the Port Authority's authorized representative for such retention. If the Recipient elects to destroy the Confidential and Privileged and/or Confidential Information, then the Recipient shall deliver to the Port Authority a certification, in the form attached hereto as Exhibit B, signed by an authorized representative of the Recipient confirming its compliance with this requirement.

12. The obligations under this Agreement will be perpetual (unless otherwise provided in this Agreement) or until such time as the information is no longer considered Confidential and Privileged and/or Confidential.

13. If any term or provision of this Agreement shall be determined invalid or unenforceable to any extent or in any application by any court of competent jurisdiction, the validity and enforceability of the remaining provisions will not be affected thereby.

14. Recipient acknowledges and agrees that the unauthorized disclosure and handling of the Confidential and Privileged and/or Confidential Information could have an adverse and detrimental impact on public safety and security and significantly endanger the Port Authority, its facilities, its patrons and the general public.

15. Recipient hereby expressly agrees that the obligations of confidence required hereunder are extraordinary and unique and are vital to the security and well-being of the Port Authority, its customers, facilities and the general public, and that any breach by it or its

representatives of the terms hereof will result in unique and immeasurable harm to the Port Authority for which monetary damages would be inadequate. Accordingly, Recipient hereby agrees that if it breaches or threatens to breach this Agreement, the Port Authority shall be entitled, in addition to all other rights or remedies available at law or in equity, to seek temporary or permanent injunctive relief, without the necessity of proving damages or to post any bond or other security, in order to prevent further breach.

16. This Agreement shall be governed by and construed in accordance with the laws of the State of New York, without regard to the conflict of laws principle.

17. Any violation of this Agreement may result in legal and/or disciplinary action against the Recipient, and any individual violating this Agreement and the signed acknowledgment.

18. The failure of any party to enforce, at any time, or for any period of time, any provision of this Agreement shall not be construed to constitute or evidence a waiver of such provision or the right of such party to enforce each and every provision thereafter.

19. This Agreement constitutes the entire agreement between the Port Authority and Recipient on the subject matter contained herein and supersedes any and all prior negotiations, correspondence, agreements, understanding, duties or obligations between the parties hereto respecting the subject matter hereof. The provisions of this Agreement may be amended, modified or revoked, in whole or in part, only by a written instrument executed by each of the parties to this Agreement.

20. This Agreement is the joint product of the parties hereto and each provision of this Agreement has been subject to the mutual consultation, negotiation, and agreement of the parties hereto, and shall not be construed for or against any party hereto.

Dated: New York, New York
_____, 2007

By: _____

Name:
Title:

Exhibit A

ACKNOWLEDGEMENT

I, _____, am employed as a(n)_____(fill in job title) by_____ (fill in employer) located at _____. I understand that, because of my employer's relationship with _____ (fill in the other Party to the agreement with the Port Authority), both my employer and I are being, or may be, provided with access to, and/or copies of, certain sensitive security materials and information relating to the Project. I have been provided with and read _____ (fill in the Party's name) Non-Disclosure and Confidentiality Agreement with the Port Authority of New York and New Jersey, executed by _____ (fill in the Party) on _____, 2007. If it is required for me to review or receive information provided by the Port Authority that is marked "CONFIDENTIAL AND PRIVILEGED", "CONFIDENTIAL", "SENSITIVE SECURITY INFORMATION," and/or "(PROTECTED) CRITICAL INFRASTRUCTURE INFORMATION", I acknowledge that I will be bound by each and every term and provision contained therein and that failure to do so may include, but is not limited to, the imposition of disciplinary action and sanctions, and/or the institution of legal action seeking injunctive relief, monetary and/or criminal penalties for violation of law and/or Port Authority policies and procedures, as well as for violation of federal and/or state regulations.

To the extent I am currently in possession of, or have previously come in contact with, marked information as it relates the aforementioned Agreement, I agree to conform my handling procedures for "CONFIDENTIAL AND PRIVILEGED," "CONFIDENTIAL", "SENSITIVE SECURITY INFORMATION," and/or "(PROTECTED) CRITICAL INFRASTRUCTURE INFORMATION" to the practices and procedures set forth and defined herein or risk loss of access to said information, removal from said project and/or subjecting myself to the aforementioned disciplinary actions and/or civil and criminal penalties.

NAME OF RECIPIENT_____
Print Representative Name:_____
Signature:_____
Title:_____
Date:_____

Exhibit B

CERTIFICATION

To: The Port Authority of New York and New Jersey (the "Port Authority")

Reference is made to the Non-Disclosure and Confidentiality Agreement (the "Agreement") between the Port Authority and _____(the "Recipient") dated _____. Capitalized terms used and not otherwise defined herein shall have the meanings ascribed to them in the Agreement. Pursuant to the Agreement, the Recipient hereby certifies the following to be true:

> The Recipient has destroyed and has caused its agents to destroy all tangible materials describing, analyzing, containing, or referring or relating to, the Confidential and Privileged and/or Confidential Information, including, but not limited to, all originals, extracts, studies, copies, and summaries, whether received from the Port Authority or created by Recipient, or its representatives, and regardless of the medium in which the Confidential and Privileged and/or Confidential Information was provided or maintained, including any information stored in electronic form, which shall also be completely removed from any computer database, to the extent that the destruction would preclude recognition or reconstruction of the Confidential and Privileged and/or Confidential Information.

By: _____
Name:
Title:

Date: _____

Attachment F

Security Administration Function

Responsible for:

- Establishment of access rights, groups, profiles etc. for a system or application for which they are responsible and documenting their use and definitions.
- The development of security procedures which define the granting of access and the administration of security functions of their system or application. The ongoing review and update of these security procedures.
- Responsible for the development of add/change/delete access requests forms.
- The development of procedures for changing or deleting accounts or privileges when staff leave or change assignments. Execution of these procedures in a timely manner.
- Regular review of who has access to their data and determining if it is appropriate and still required.
- Ensuring that users are required to acknowledge, in writing, that they have been informed of the organization's position on security and confidentiality of information prior to access being given.
- Assigning appropriate expiration dates for accounts used by temporary/consulting staff.
- The development of procedures for responding to, documenting and escalating security incidents.
- The investigation and appropriate escalation of a security incident matter.
- Setting any global system or application controls (i.e. password controls, time out, concurrent logins) consistent with the Standards and Guidelines for Port Authority Technology.
- Restricting remote access and monitoring and reviewing the activity log. (Limit or no use of modems. Modems should be configured according to the Standards and Guidelines a certified by the Information Systems Security Officer.)
- Development and review of reports such as Kane Security Analyst, ISS or ESM to monitor areas of security exposure.
- Daily event log reviews for irregular activities and security violations.
- Keeps management and the business unit informed on security issues.

- Development of regular processing schedules for the production of security reports i.e. unsuccessful logon attempts, audit trail reports.
- Development of procedures for reviewing the reports and logs on a regular basis and taking appropriate corrective action.
- Responsible for ensuring that the system complies with the Standards and Guidelines for Port Authority Technology.
- Determining high-risk activities, establishing logs of those activities and tables and determining appropriate review cycles.
- Ensuring that operating system, database system and application security issues are coordinated.
- Keeping abreast of vulnerabilities of systems, databases, or application as they are discovered and patching them or implementing compensation controls.
- Development of procedures for the disposal of unneeded confidential data produced from the application.
- Ensure all system hardware (i.e. servers, comm. rooms, backup tapes, etc.) and software are secured from tampering or damaging.
- Ensure that operating systems at a minimum complies with the Distributed Systems Environment in the Standards and Guidelines and industry standards.
- Document a virus protection and recovery plan.
- Firewall Administration, Firewall configuration, rules, logs, and patches
- Intrusion Detection System Administration, monitoring network traffic across the firewall and in the DMZ.
- Router and Switches Administration, configuration file, backups, patches, and change controls.

13) Account Policies
   a) Concurrent log in
   b) Vendor/Consultant Account Expiration (usually the length of the contract)

Remote Access

14) Strategy/Approach
15) Approvals

Operation

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

Physical

21) Server Location
   a) Site Security
   b) Server Mounting
      i) What is the rack configuration and who has access to the keys
   c) Environmental Controls
      i) Humidity and Temperature Monitoring

Anti-Virus Management

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

Change Management

25) Testing Environment
26) Normal Procedures
27) Emergency Procedures
28) Requests are documented
29) Specific timetables/scheduling are documented

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

Patch Management

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

Reporting and Monitoring

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

Problem & Incident Management

40) Problem reporting/resolution tracking system
   a) Problems are appropriately logged and prioritized.
   b) Corrective measures are documented.

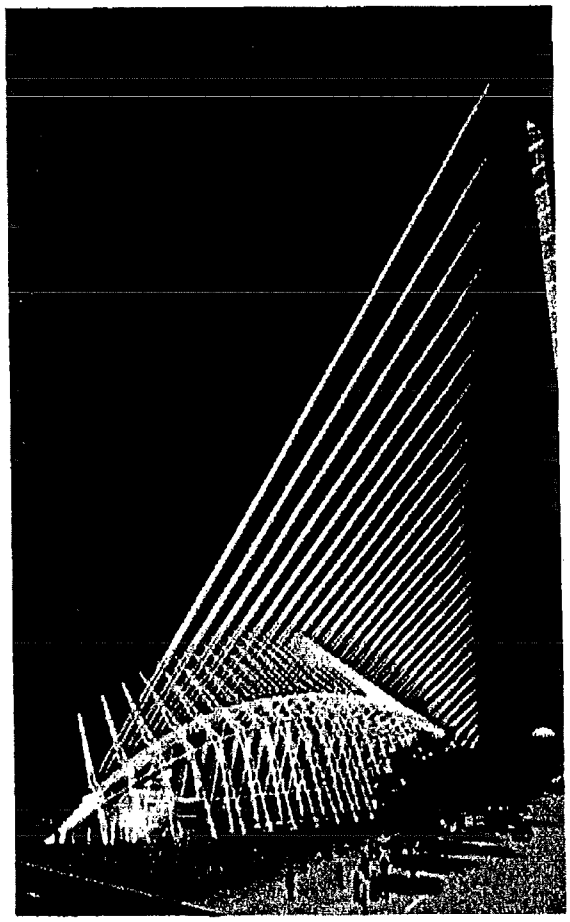
Segregation of Duties

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

ATTACHMENT K

THE PORT AUTHORITY OF NY & NJ

Handbook for Protecting Security Information



NOVEMBER 1, 2004

Revision: JULY 8, 2005

The Port Authority of New York and New Jersey
Handbook for Protecting Security Information

Summary

This Security Program Handbook describes in detail The Port Authority of New York and New Jersey's (PANYNJ) requirement for the implementation and application of uniform security procedures regarding the identification, handling, care and storage of Confidential and Privileged Security Information belonging to the PANYNJ and Sensitive Security Information as identified in 49 CFR parts 15 and 1520. Confidential and Privileged Port Authority Security Information is information that, if subject to unauthorized access, modification, loss or misuse could adversely affect the PANYNJ, public safety and homeland security. Sensitive Security Information, in accordance with 49 U.S.C. 114(s), is information obtained or developed in the conduct of security activities, including research and development, the disclosure of which TSA has determined would--

- Constitute an unwarranted invasion of privacy - including, but not limited to, information contained in any personnel, medical, or similar file)
- Reveal trade secrets or privileged or confidential information obtained from any person;
- Be detrimental to the security of transportation.

This handbook describes the requirements and other safeguards that are necessary to prevent unauthorized disclosure of both Confidential and Privileged Port Authority Security Information and Sensitive Security Information, and to control the authorized disclosure of this information for use internally within the Port Authority or when released by the Port Authority to outside entities.

The components of this Security Program Handbook are:

Security Manual - Establishes uniform procedures for identification, handling, receipt, care, and storage of Confidential and Privileged Security Information and Sensitive Security Information (SSI).

Access Control Guide - Establishes the basis for determining what type of information requires special handling and that which does not.

Non-Disclosure and Confidentiality Agreement -

Company Non-Disclosure and Confidentiality Agreement: As a condition of its providing confidential and privileged security information, the Port Authority is requiring those working on projects that require access to Port Authority Security Information / Sensitive Security Information, whether retained by it or by other contractors or consultants for its projects, to enter into this agreement, thereby acknowledging that they understand that it will be required to safeguard any such information provided, as well as its work product including conclusions of security assessments, evaluations and/or recommendations.

Individual Non-Disclosure and Confidentiality Agreement Acknowledgement: Acknowledges the agreement between the PANYNJ and those individuals provided access to Confidential and Privileged Port Authority Security Information / Sensitive Security Information, whereby the individual agrees to not disclose Confidential and Privileged Port Authority Security Information / Sensitive Security Information to any unauthorized person. . Additionally, this agreement informs the individual of (1) the trust that is placed in them by providing them access to this information; (2) their responsibility to protect this information from unauthorized disclosure. Port Authority employees with a "need to know" will be required to sign an agreement.

Security Information Practices and Procedures document (SIPP)

This supplemental document details the procedures outlined in the Security Handbook and applies them within a specific program. Users of the Security Handbook should contact the appropriate Security Information Manager to confirm that they are referencing the appropriate Security Information Practices and Procedures document.

Procedures For Handling
Confidential And Privil eged Security Information
and
Sensitive Security Info rmation

Table of Contents

Section		Page
1	Introduction	4
2	Access To Security Information	5
3	Security Training & Briefings	8
4	Safeguarding Security Information	10
5	Marking Documents	12
6	Authorized Personnel Project Lists	14
7	Document Accountability Log	15
8	Information Technology Systems	16
9	Bidding & Procurement	17
10	Security Access Control Guide	18

SECTION 1. Introduction

This document establishes uniform procedures for the identification, handling, receipt, care, and storage of Confidential and Privileged Port Authority Security Information and Sensitive Security Information (SSI). This Manual prescribes requirements and other safeguards that are necessary to prevent unauthorized disclosure of this information and to control authorized disclosure of it when released by The Port Authority of New York and New Jersey (PANYNJ) to architects, engineers, consultants, contractors, subcontractors, suppliers, and others deemed necessary in order to design, bid on and subsequently complete the work or contract.

Each organization that requires access to Confidential and Privileged Port Authority Security Information / Sensitive Security Information shall appoint a senior management level employee to be the company's Security Information Manager. The role of the Security Information Manager is an important one. This person is responsible for implementing and maintaining the firm's PANYNJ Program For Protecting Confidential and Privileged Security Information / SSI. An alternate Security Information Manager shall also be appointed. The alternate will assume the responsibilities of the Security Information Manager in their absence.

SECTION 2. Access to Confidential and Privileged Security Information

To protect Confidential and Privileged Security Information / SSI, each organization that requires access to this information shall participate in the requisite confidentiality and non-disclosure agreements and provide PANYNJ approved training to any employees requiring access to this information.

The firm shall ensure that employees: (1) are citizens of the United States of America or an alien who has been lawfully admitted for permanent residence or employment (indicated by immigration status) as evidenced by Immigration and Naturalization Service documentation or a national of the United States as defined by the Immigration and Nationality Act[1]; and (2) have the requisite need to know as defined in the Department of Transportation and the Department of Homeland Security's regulations on Protection of Sensitive Security Information[2]; and (3) have completed the PANYNJ Non-Disclosure and Confidentiality Agreement Acknowledgment. If an employee refuses to execute the acknowledgment, access to the protected information must be denied. The requirements set forth above regarding citizenship or permanent residency may be waived by the Port Authority and PATH as appropraite. This information will be reflected on the Authorized Personnel Project List, cribed below, that will be provided to the PANYNJ.

The dissemination must be included in any contract awarded that will require access to Confidential and Privileged Security Information / SSI.

The dissemination of Confidential and Privileged Security Information / SSI shall only be made upon the determination that the recipient is authorized to receive it. Authorization is based on a potential recipient's need-to-know as determined by the Security Information Manager and the proper execution of a PANYNJ Confidentiality Agreement Acknowledgement.

Confidential and Privileged Security Information / SSI includes proprietary data and/or other information that, if subject to unauthorized access, modification, loss or misuse could adversely affect the PANYNJ, public safety and homeland security.

SSI is, in accordance with 49 U.S.C. 114(s), information obtained or developed in the conduct of

[1] The term "national of the United States" means (A) a citizen of the United States, or (B) a person who, though not a citizen of the United States, owes permanent allegiance to the United States. 8 U.S.C. 1101(a)(22) (Dec 19,20 03)
[2] 49 CFR § 15.11; 49 CFR § 1520.11

security activities, including research and development, the disclosure of which TSA has determined would—

- Constitute an unwarranted invasion of privacy - including, but not limited to, information contained in any personnel, medical, or similar file
- Reveal trade secrets or privileged or confidential information obtained from any person;
- Be detrimental to the security of transportation.

The Security Information Manager from each organization that requires access to Confidential and Privileged Security Information is required to prepare an Authorized Personnel Contract Project List - a list of employees who are authorized to access Confidential and Privileged Security Information and the date they executed the Confidentiality/Non-Disclosure Agreement. A copy of this list will be provided to the PANYNJ. This list will be used as a method for authenticating that individuals have been briefed into the program and are certified for access to Confidential and Privileged Security Information.

Security requirements are a material condition of all PANYNJ contracts that will require access to Confidential and Privileged Security Information. Contracts shall be subject to termination for default, when it has been determined that a failure to comply with security requirements resulted from willful misconduct or a lack of good faith.

An individual's access to the Confidential and Privileged Security Information / SSI may be contingent upon satisfactory completion of a security background check and the imposition of satisfactory procedures and requirements for safeguarding.

Unauthorized disclosure of SSI may be grounds for a civil penalty and other enforcement or corrective action by DOT, and appropriate personnel actions for Federal employees. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure.

When a person authorized access to safeguarded information becomes aware that the information has been released to unauthorized persons, the authorized person must promptly notify the Security Information Manager. In the case of SSI, the Security Information Manager

must immediately inform TSA or the applicable DOT or DHS component or agency of the breach.

SECTION 3. Security Training & Briefings

Each organization that provides an employee with access to Confidential and Privileged Security Information shall provide training and briefings appropriate to their involvement.

Training Materials

Sample briefings and training materials may be requested from the PANYNJ.

Security Information Manager Training

The role of the Security Information Manager is critical. The Security Information Manager is responsible for implementing and maintaining the facility's PANYNJ Security Program. The Security Information Manager is responsible for educating employees on the handling of Confidential and Privileged Security Information / SSI. Security Information Managers are required to complete a half-day training session. Training requirements shall be based on the company's involvement with Confidential and Privileged Security Information and may include an orientation course. Security Information Manager training will also include a detailed explanation of the process for qualifying an individual's credentials for access. The PANYNJ is responsible for providing an initial security briefing to the Security Information Manager.

Initial Security Briefings

Prior to being granted access to Confidential and Privileged Security Information / SSI, an employee will receive an initial security briefing that includes the following:

a. An explanation of security procedures applicable to the employee's job.
b. An overview of the security categorization.

After receiving this briefing and prior to being granted access to any Confidential and Privileged Security Information the employee must execute a PANYNJ Non-Disclosure and Confidentiality Agreement Acknowledgement. If an employee refuses to execute the agreement, access to Confidential and Privileged Security Information must be denied.

Refresher Training

Employees granted access to Confidential and Privileged Security Information shall be provided with some form of PANYNJ approved security education and training annually. Refresher training shall reinforce the information provided during the initial security briefing and shall keep employees informed of any changes in security regulations.

SECTION 4. Safeguarding Confidential and Privileged Security Information

All persons granted access to Confidential and Privileged Security Information / SSI are responsible for safeguarding all such information in their possession or control. Confidential and Privileged Security Information / SSI shall be protected at all times either by appropriate storage or having it under the personal observation and control of a person authorized to receive it. Each person who works with Confidential and Privileged Security Information is personally responsible for taking proper precautions to ensure that unauthorized persons do not gain access to it.

Use and storage

During actual working hours, steps shall be taken to preclude access to Confidential and Privileged Security Information / SSI by unauthorized personnel. Before or after actual working hours, Confidential and Privileged Security Information / SSI shall be stored in an environment with password protection or in a secure container such as a safe, locked desk or file cabinet.. Only authorized individuals are permitted access to the locks combination or to the locks key. A list should be maintained as to which individuals have access to which container. It is strongly suggested that more than one employee has access to each storage container. Authorized individuals must protect combinations and keys.

Reproduction

Confidential and Privileged Security Information / SSI may be reproduced to the minimum extent necessary - consistent with the need to carry out contract performance provided that the reproduced material is marked and protected in the same manner as the original material. Authorized individuals must accomplish all reproduction. Authorized service providers may be used for this task provided that the information remains safeguarded.

Disposal of information

When Confidential and Privileged Security Information is no longer needed it shall be disposed of by any method that prevents unauthorized retrieval. All paper products will be destroyed using a crosscut shredder at a minimum. Authorized individuals must perform the destruction. Authorized service providers may be used for this task provided that the information remains safeguarded until the destruction is completed.

Transmission and Shipment of Confidential and Privileged Security Information

Confidential and Privileged Security Information may be sent via the U.S. Postal Service or express mail services (e.g. FEDEX) provided it is packaged and sealed in a way that does not disclose its contents or the fact that it is Confidential and Privileged Security Information. All packages shall be sealed in a manner that easily identifies whether the package has been opened prior to delivery to the final consignee. The use of double wrapped package or a tamper resistant envelope may be used to fulfill this requirement.

In addition, the package must be addressed to an individual whose name appears on the Authorized Personnel Contract Project List or preferably to the Security Information Manager.

Security Information Access Control Guides

The PANYNJ is responsible for providing Security Program participants with the Security Information Access Control Guides needed during the performance of the contract.

The Security Information Access Control Guide identifies the types of Security Information that will require protection. It is each organization's responsibility to understand and apply all aspects of this guide. Security information Access Control Guidance is the exclusive responsibility of the PANYNJ, and the final determination of the appropriate categorization for the information rests with the PANYNJ.

If the PANYNJ does not advise to the contrary, a firm must return all Confidential and Privileged Information in its possession to the PANYNJ upon completion of a contract. If instead, the firm chooses to dispose of the information it must follow the destruction requirements identified in this manual. The contractor shall provide a written list/certification that all Confidential and Privileged Security Information has been properly destroyed. If the PANYNJ determines that a firm has a continuing need for the Confidential and Privileged Information a letter will be issued to show the authorized retention period and to provide final disposition instructions.

SECTION 5. Markings

Marking of Confidential and Privileged Security Information:
All documents, drawings, etc. that contain Confidential and Privileged Security Information / SSI must contain protective markings. In addition, the front page (or front and back cover if appropriate) shall be marked at the top and bottom of the page. In the case of Port Authority Confidential and Privileged Security Information, the protective marking is: CONFIDENTIAL AND PRIVILEGED SECURITY INFORMATION. A 16-point font size should be used for this marking. All copies of Confidential and Privileged Security Information / SSI documents shall also bear the required markings.

Interior pages of a document shall be conspicuously marked or stamped at the top and bottom with the category of the information appearing thereon. The document may be conspicuously marked or stamped Confidential and Privileged Security Information / SSI at the top and bottom of each interior page, when the particular information to which protection is assigned is adequately identified.

Interior pages of a document shall be conspicuously marked or stamped at the top and bottom with the category of the information appearing thereon. Alternatively, the document may be conspicuously marked or stamped Confidential and Privileged Security Information / SSI at the top and bottom of each interior page, when necessary to achieve production efficiency, and the particular information to which protection is assigned is adequately identified. Portions of this document shall be marked in a manner that eliminates doubt as to which of its parts contain or reveal Confidential and Privileged Security Information or SSI.

Sets of documents large enough to be folded or rolled shall be marked so that the marking is visible on the outside of the set when it is rolled or folded. In addition, all sensitive project information shall contain the following label on the front cover, title sheet or first page (for Confidential and Privileged Security Information plans and drawings the label shall be applied to each drawing):

"WARNING": This document is the property of the PANYNJ. Further reproduction and/or distribution outside the contract team is prohibited without the express written approval of:
The Port Authority of NY & NJ

In the case of paper records containing SSI, protective markings must be conspicuously placed on the top, and the distribution limitation statement on the bottom, of the outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover; any title page; and each page of the document. The protective marking is: SENSITIVE SECURITY INFORMATION. A 16-point font size should be used for this marking.

The distribution limitation statement is:
WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this record may be disclosed to persons without a ``need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR parts 15 and 1520. . An 8-point font size should be used for this marking.

In the case of non-paper records that contain SSI, including motion picture films, videotape recordings, audio recording, and electronic and magnetic records, a covered person must clearly and conspicuously mark the records with the protective marking and the distribution limitation statement such that the viewer or listener is reasonably likely to see or hear them when obtaining access to the contents of the record.

SECTION 6. Authorized Personnel Project Lists: Team Rosters

Each organization that participates on a contract that involves Confidential and Privileged Security Information will prepare an Authorized Personnel Project List. The list will include:

- Firm's name and address
- Name and contact information for the firm's Security Information Manager and Alternate
- A list of employees authorized to access Confidential and Privileged Security Information and the date they signed the Confidentiality/Non-Disclosure Agreement Acknowledgement

A copy of this list will be provided to the PANYNJ. Additional copies of this list will be provided to other companies authorized access, which the firm will interact with during the performance of the contract. This list will be used as a method for authenticating that individuals are authorized access to Confidential and Privileged Security Information. The PANYNJ needs to be notified immediately of any/all changes to key personnel on the roster. Each organization's Security Information Manager is responsible for the accuracy of this list. If an individual's name does not appear on the list they will be denied any access to Confidential and Privileged Security Information.

SECTION 7. Document Accountability

Each organization that has Confidential and Privileged Security Information / SSI in its possession will have in place a system that will account for the material in such a manner that retrieval is easily accomplished at the contract's conclusion. The accountability log must include:

- The date that a document was received or created
- The identity of the sender or creator
- A very brief description of the document
- Number of copies
- Transmission history (sent to whom, when)
- Certification that the document has been destroyed or returned to the PANYNJ

SECTION 8. Information Technology Systems

Information systems that are used to electronically capture, create, store, process or distribute Confidential and Privileged Security Information must be managed to protect against unauthorized disclosure. Protection requires a balanced approach to include but not limited to operational (software security controls), physical and personnel controls.

The main objectives are to

- Restrict access to authorized users exclusively
- Compartmentalization of all Confidential and Privileged Security Information
- Complete removal of all Confidential and Privileged Security Information from the system when it is no longer needed

Each contractor and consultant will provide the PANYNJ with an Information Technology Systems Protection Plan for approval. The Protection Plan should describe the measures that the firm will apply to accomplish the objectives stated above.

The plan should include:

- A hardware baseline description and configuration diagram
- Software list
- Procedures for restricting access to authorized users exclusively
- Procedures used for compartmentalizing all Confidential and Privileged Security Information
- Procedures used to place system into and remove from "protected" mode
- Procedures used for removal of Confidential and Privileged Security Information

All electronic exchange of Confidential and Privileged Security Information / SSI must be accomplished using a project web site with centrally managed access control on a per individual basis with encrypted transfer.

SECTION 9. Bidding & Procurement

Confidential and Privileged Security Information that is provided under a solicitation is subject to the handling requirements for Confidential and Privileged Security Information identified in this manual.

Dissemination of Confidential and Privileged Security Information shall only be made upon the determination that the recipient is authorized to receive it. The measure for determining authorization is "need-to-know" and completion of a PANYNJ Confidentiality Agreement. This includes all persons or firms necessary to do work at the request of the PANYNJ such as architects and engineers, consultants, contractors, sub-contractors, suppliers, and others that the contractor deems necessary in order to submit an offer/bid or to complete the work or contract. It is the responsibility of the person or firm disseminating the information to assure that the recipient is an authorized user and to keep records of recipients.

The contractor shall provide a written list/certification that he and his subcontractors have properly disposed of all Confidential and Privileged Security Information after Contract award, after completion of any appeals process or completion of the work.

Section 10. Security Information Access Control Guide

The following are the basis for categorization of information and material involved in design, development, construction and/or maintenance contracts for PANYNJ projects.

Authority

The uniform procedures for categorization and/or control of Confidential and Privileged Port Authority Security Information related to architecture, engineering, construction, or rehabilitation of Port Authority facilities are issued under the authority of the Port Authority of NY&NJ.

Standards

Construction of security systems often requires that an exact standard be met or exceeded in order to insure that the security system will function properly. Drawings, details, and specification books are to indicate materials to be used, as well as any other information necessary to construct the system. They are not to indicate that the type of construction shown meets a security standard, or to contain any reference to the limits or capabilities of the type of construction/security system. This information will only be contained or referred to in the detailed Statement of Work.

Applicability

This guide applies to PANYNJ personnel, as well as to firms and individuals who are under contract, purchase order, letter contract, or who are in receipt of Confidential and Privileged Security Information through a request for quote, proposal, bid, or third party agreement.

All users of this guide are encouraged to assist in improving and maintaining its currency and accuracy.

Public Release

The fact that this section defines certain information as UNMARKED does not allow automatic public release of this information. Proposed public disclosures of UNMARKED Information regarding construction/renovation shall be processed through Port Authority's project manager or the duly designated representatives for the specific contract.

Contractual Release

Contractors are responsible to the PANYNJ for all Confidential and Privileged Security Information drawings, including shop drawings, or other documentation provided to subcontractors.

.Security Information Access Control Guide

Information constituting Confidential and Privileged Security Information and UNMARKED.

Topic	Categorization	Remarks
Any mention of information that reveals vulnerabilities, built-in or potential, relating to our critical infrastructure.	**CONFIDENTIAL & PRIVILEGED**	
That a facility is designed with extensive security features.	**UNMARKED**	
Identity of individual security systems installed at the facility.	**CONFIDENTIAL & PRIVILEGED**	
Time frame or schedules showing project progress.	**UNMARKED**	
The general areas of the project or where security systems will be installed.	**UNMARKED**	
Announcement of security subcontract awards.	**UNMARKED**	
Results of site survey documentation or review that address specific physical security vulnerabilities.	**CONFIDENTIAL & PRIVILEGED**	When referring to specific terrorist threats and/or the specific capabilities of the installation to counter the threat, or when referring to site-unique technical threat.
Design and construction information revealing details unique or essential to the	**UNMARKED**	**UNMARKED** when referring to commercially available security systems, accepted

security system(s).	**CONFIDENTIAL & PRIVILEGED**	construction techniques, information which is in the public domain and/or when security systems will be installed in area accessible to public view. **CONFIDENTIAL & PRIVILEGED** when referring to methods of defeating the security system(s) and/or covert/unexposed security systems.
Design drawings with specific forced entry ratings	**CONFIDENTIAL & PRIVILEGED**	
Shop drawings that provide specific rating Information	**CONFIDENTIAL & PRIVILEGED**	
What specific security system/ hardware model number is installed at a specific location?	**CONFIDENTIAL & PRIVILEGED**	When referring to fire safety systems, access denial systems, intrusion detection systems, core area security systems, and in-place surreptitious entry verification systems.
Details concerning overall security system(s) or individual subsystem(s), including design, engineering, construction, and fabrication. Also includes capabilities, vulnerabilities diagrams, operational	**UNMARKED** **CONFIDENTIAL & PRIVILEGED**	**UNMARKED** when data is commercially available in the public domain. **CONFIDENTIAL & PRIVILEGED** when high technology data, which was

characteristics, and support requirements.		developed by or for the PANYNJ, is revealed; or when data is site specific or concerns core area systems.
Security system effectiveness, to include range, maneuverability, resolutions, accuracy, and readiness cycle.	**UNMARKED** **CONFIDENTIAL & PRIVILEGED**	**UNMARKED** when the information is commercially available or in the public domain. **CONFIDENTIAL & PRIVILEGED** when the system was developed or modified for or by the PANYNJ; or when the information concerns a specific special application.
Information identifying critical elements of the system; such as master controls, overrides, backup power sources.	**UNMARKED** **CONFIDENTIAL & PRIVILEGED**	**UNMARKED** If equipment is readily observable to the public. **CONFIDENTIAL & PRIVILEGED** when an element has been developed and/or modified by or for the PANYNJ for a special application; or when such elements are not readily observable by the public.
Security systems command and control operating instructions and supporting	**CONFIDENTIAL & PRIVILEGED**	

countermeasures when referring to a specific site or project location.		
Blast protection design requirements for new or existing PANYNJ facilities.	**CONFIDENTIAL & PRIVILEGED**	
Blast analysis that addresses specific vulnerabilities to new or existing PANYNJ facilities.	**CONFIDENTIAL & PRIVILEGED**	If specific weaknesses are reflected or maximum tolerances are provided.
Structural plans, details, and specifications.	**UNMARKED** **CONFIDENTIAL & PRIVILEGED**	**UNMARKED** when generic criteria are used. Site-specific information generated from generic criteria is UNMARKED. **CONFIDENTIAL & PRIVILEGED** if site-specific information involves details of security system(s) or additional protection.
Design data revealing engineering, construction, or fabrication details of a Communications Center electrical system or facility support systems with signal cables (e.g., intercom, telephone). This includes grounding systems.	**UNMARKED** **CONFIDENTIAL & PRIVILEGED**	**UNMARKED** if generic design criteria/terms are used. **CONFIDENTIAL & PRIVILEGED** if data reflects calculations resulting in selection of specific items to be used inside a specific Communications Center and/or listing of those items.
Drawings and specifications for	**CONFIDENTIAL &**	**CONFIDENTIAL &**

emergency generator room or building.	**PRIVILEGED**	**PRIVILEGED** if site-specific or if any reference to control or security system.
What vulnerabilities will render the electrical and communications system(s) inoperative.	**CONFIDENTIAL & PRIVILEGED**	
Record documents identifying protective measures around Operations & Control Centers	**CONFIDENTIAL & PRIVILEGED**	
Record documents identifying the location of Police and Emergency Communication Lines	**CONFIDENTIAL & PRIVILEGED**	

INFORMATION CONSTITUTING SSI

Except as otherwise provided in writing by TSA, in the interest of public safety or in furtherance of transportation security, the following information, and records containing such information, constitute SSI:

Security Programs and Contingency Plans	**SSI**	Any security program or security contingency plan issued, established, required, received, or approved by DOT or DHS, including-- Any aircraft operator or airport operator security program or security contingency plan under this chapter; Any vessel, maritime facility, or port area security plan required or directed under Federal law; Any national or area security plan prepared under 46 U.S.C. 70103; and Any security incident response plan established under 46 U.S.C. 70104.
Security Directives	**SSI**	Any Security Directive or order-- (i) Issued by TSA under 49 CFR 1542.303, 1544.305, or other authority; (ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR part 6, or 33 U.S.C. 1221 et seq. related to maritime security; or (iii) Any comments, instructions, and implementing guidance pertaining thereto.
Information Circulars	**SSI**	Any notice issued by DHS or DOT regarding a threat to aviation or maritime transportation, including any--

		(i) Information Circular issued by TSA under 49 CFR 1542.303, 1544.305, or other authority; and (ii) Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.
Performance Specifications	**SSI**	Any performance specification and any description of a test object or test procedure, for– Any device used by the Federal government or any other person pursuant to any aviation or maritime transportation security requirements of Federal law for the detection of any weapon, explosive, incendiary, or destructive device or substance; and Any communications equipment used by the Federal government or any other person in carrying out or complying with any aviation or maritime transportation security requirements of Federal law.
Vulnerability Assessments	**SSI**	Any vulnerability assessment directed, created, held, funded, or approved by the DOT, DHS, or that will be provided to DOT or DHS in support of a Federal security program.

Security Inspection or Investigative Information.	**SSI**	Details of any security inspection or investigation of an alleged violation of aviation or maritime transportation security requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit.
	SSI	In the case of inspections or investigations performed by TSA, this includes the following information as to events that occurred within 12 months of the date of release of the information: the name of the airport where a violation occurred, the airport identifier in the case number, a description of the violation, the regulation allegedly violated, and the identity of any aircraft operator in connection with specific locations or specific security procedures. Such information will be released after the relevant 12-month period, except that TSA will not release the specific gate or other location on an airport where an event occurred, regardless of the amount of time that has passed since its occurrence. During the period within 12 months of the date of release of the information, TSA may release summaries of an aircraft operator's, but not an airport operator's, total security violations in a specified time range without identifying specific violations or locations. Summaries may include total enforcement actions, total proposed civil penalty amounts, number of cases opened, number of cases referred to TSA or FAA

		counsel for legal enforcement action, and number of cases closed.
Threat Information	**SSI**	Any information held by the Federal government concerning threats against transportation or transportation systems and sources and methods used to gather or develop threat information, including threats against cyber infrastructure.
Security Measures	**SSI**	Specific details of aviation or maritime transportation security measures, both operational and technical, whether applied directly by the Federal government or another person, including— Security measures or protocols recommended by the Federal government; Information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security duties and Federal Air Marshals, to the extent it is not classified national security information; and Information concerning the deployments and operations of Federal Flight Deck Officers, and numbers of Federal Flight Deck Officers aggregated by aircraft operator.
Security Screening Information	**SSI**	The following information regarding security screening under aviation or maritime transportation security requirements of Federal law:

		Any procedures, including selection criteria and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo, that is conducted by the Federal government or any other authorized person. Information and sources of information used by a passenger or property screening program or system, including an automated screening system. Detailed information about the locations at which particular screening methods or equipment are used, only if determined by TSA to be SSI. Any security screener test and scores of such tests. Performance or testing data from security equipment or screening systems. Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.
Security Training Materials	**SSI**	Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal government or another person to carry out any aviation or maritime transportation security measures required or recommended by DHS or DOT.

Identifying Information of Certain Transportation Security Personnel	**SSI**	Lists of the names or other identifying information that identify persons as-- Having unescorted access to a secure area of an airport or a secure or restricted area of a maritime facility, port area, or vessel or; Holding a position as a security screener employed by or under contract with the Federal government pursuant to aviation or maritime transportation security requirements of Federal law, where such lists are aggregated by airport; Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boardings, or engaged in operations to enforce maritime security requirements or conduct force protection; Holding a position as a Federal Air Marshal; or the name or other identifying information that identifies a person as a current, former, or applicant for Federal Flight Deck Officer.
Critical Aviation or Maritime Infrastructure Asset Information	**SSI**	Any list identifying systems or assets, whether physical or virtual, so vital to the aviation or maritime transportation system that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is— Prepared by DHS or DOT; or Prepared by a State or local government agency and submitted by the agency to DHS or DOT.
Systems Security Information	**SSI**	Any information involving the security of

		operational or administrative data systems operated by the Federal government that have been identified by the DOT or DHS as critical to aviation or maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.
Confidential Business Information	**SSI**	Solicited or unsolicited proposals received by DHS or DOT, and negotiations arising there from, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to aviation or maritime transportation security measures; Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities; and Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS or DOT in carrying out aviation or maritime transportation security responsibilities, but only if the source of the information does not customarily disclose it to the public.
Research and Development	**SSI**	Information obtained or developed in the conduct of research related to aviation or maritime transportation security activities, where such research is approved, accepted, funded, recommended, or directed by the DHS

		or DOT, including research results.
Other Information	**SSI**	Any information not otherwise described in this section that TSA determines is SSI under 49 U.S.C. 114(s) or that the Secretary of DOT determines is SSI under 49 U.S.C. 40119. Upon the request of another Federal agency, TSA or the Secretary of DOT may designate as SSI information not otherwise described in this section.

NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT

THIS NON-DISCLOSURE AND CONFIDENTIALITY AGREEMENT (the "Agreement") is made as of this ____ day of _____, 2007, by and between The Port Authority of New York and New Jersey (the "Port Authority") a body corporate and politic created by Compact between the States of New York and New Jersey, with the consent of the Congress of the United States, and having an office and place of business at 225 Park Avenue South, New York, New York, 10003, and _____("Recipient"), a

WHEREAS, the Port Authority desires, subject to the terms and conditions set forth below, to disclose to Recipient confidential and privileged information in connection with (insert description of project/work) (collectively, the "Project(s)) and in addition, the Port Authority may deem it necessary to disclose on a need to know basis certain security and safety information which has been designated or is deemed to be Sensitive Security Information ("SSI"), and/or (Protected) Critical Infrastructure Information ("CII/PCII", as is further referenced and defined herein); and

WHEREAS, recognizing the need to share confidential and privileged information with Recipient and in furtherance of critical governmental interests regarding public welfare, safety and security at the Project site(s), the Port Authority has collected information and undertaken the development of certain plans and recommendations regarding the security, safety and protection of the Projects, including the physical construction and current and future operations of the Projects; and

WHEREAS, the Port Authority has developed the Security Program Handbook (the "Handbook") to address standard operating procedures, including the Port Authority's plan for implementation and application of uniform security procedures regarding the identification, handling, care and storage of Confidential and Privileged, and Confidential Information, as well as SSI and/or CII/PCII; and

WHEREAS, in order to protect and preserve the privilege attaching to and the confidentiality of the aforementioned information, as hereinafter defined, as well as to limit access to SSI and CII/PCII on a strict need to know basis, the Port Authority has requested, as a condition of its sharing and/or providing access to such confidential, privileged and sensitive information, that Recipient enter into this Agreement and that its respective officers, principals, contractors, agents, employees, contractors and consultants thereafter acknowledge that each such officer, principal, agent, employee, contractor or consultant understands that it will be required to treat as strictly confidential and privileged any such information so provided, as well as the work product and conclusions of any assessments and evaluations or any recommendations relating thereto and/or relating to any construction and operational information containing Confidential and Privileged, Confidential, SSI, CII/PCII, and to also fully comply with applicable federal rules and regulations with respect thereto

NOW, THEREFORE, in consideration of the mutual promises and covenants contained herein, and for other good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, it is agreed and expressly understood and acknowledged as follows:

1. (a) "Confidential and Privileged Information" includes, but is not limited to, any and all information, documents and materials entitled to protection pursuant to the public interest privilege under New York State law, and exempted, protected or otherwise not subject to disclosure to third parties pursuant to New York, New Jersey, federal, or common law, in any form, format or medium, whether tangible or intangible, whether oral, written, photographic, optical or any other form, it being understood and agreed that all such information shall be designated "Confidential and Privileged" by the Port Authority. Certain Confidential and Privileged Information may also be designated or include SSI or CII/PCII, as defined below.

(b) "Confidential Information" includes, but is not limited to, any proprietary, business or other financial information and/or any information that is sensitive in nature, but not otherwise privileged, in any form, format or medium, whether tangible or intangible, whether oral, written, photographic, optical or any other form, it being understood and agreed that all such information shall be designated "Confidential" by the Port Authority.

(c) Certain information provided to the Recipients may be designated and/or include SSI as defined in the Transportation Security Administrative Rules & Regulations, 49 C.F.R. 1520, (49 U.S.C. § 114), the Office of the Secretary of Transportation Rules & Regulations, 49 C.F.R. 15, (49 U.S.C. § 40119), and/or CII/PCII as defined in the Office of the Secretary, Department of Homeland Security Rules and Regulations, 6 C.F.R. Part 29 (6 U.S.C. §131-134.) SSI and CII/PCII shall also be received and handled as required by the applicable federal regulations or as provided for by the responsible Federal agency or as may be provided for by any agreement between such Federal agency and the Port Authority. Information designated or including SSI and/or CII/PCII may also be designated, or include, Confidential and Privileged Information.

2. Pursuant to the aforementioned Federal Regulations, specifically 49 C.F.R. §§15.17 and 1520.17, any such violation thereof or mishandling of SSI therein defined "is grounds for a civil penalty and other enforcement or corrective action by the [Department of Transportation] DOT [Department of Homeland Security], and appropriate personnel actions for Federal employees. Corrective action may include issuance of an order requiring retrieval of SSI to remedy unauthorized disclosure or an order to cease future unauthorized disclosure." Under federal regulations, specifically 6 C.F.R. §29.9, any violation of, mishandling, or misuse of CII/PCII is grounds for disqualification from future receipt of CII/PCII and/or SSI.

3. The first page of any document designated "Confidential and Privileged" or "Confidential" will be plainly marked as such. All information, documents and other material provided as such and, any part thereof, shall be deemed "Confidential and Privileged" or "Confidential", notwithstanding the fact that only the first page of a document or the container is actually marked; and

4. The first page of any document designated "SSI" or any container holding information designated "SSI" will be plainly marked "SENSITIVE SECURITY INFORMATION." All information, documents and other material provided as such, and any part thereof, shall be deemed "SSI", notwithstanding the fact that only the first page of a document or the container is actually marked.

5. All information provided to Recipient in any form, format or medium containing Confidential and Privileged, and/or Confidential Information shall be handled and treated with the highest care and in a manner consistent with the Port Authority's practices and procedures as set forth in the Handbook, as may be amended from time to time, and in a manner designed to prevent their disclosure to unauthorized third parties consistent with Port Authority security policy, practices and procedures, and all such information stored in the electronic form will be password protected.

6. Confidential and Privileged and/or Confidential Information shall be used solely for the purpose of aiding the Recipients in carrying out or undertaking their duly authorized responsibilities relating to the Projects and shall not be used, quoted, cited or otherwise replicated in any way and shall not be used as part of any draft or final communication, memorandum, report and/or other written, audio or visual medium.

7. The Confidential and Privileged and/or Confidential Information shall only be used in the performance of duly authorized activities relating to the Projects and shall not be used for any other purpose, except as expressly permitted by this Agreement, or as expressly directed in writing by the Port Authority, and, until such time that the information is no longer considered Confidential and Privileged and/or Confidential Information, it will be held and treated in the strictest confidence and shall not be disclosed either directly or indirectly to any other person who has not acknowledged and agreed to be bound by this Agreement and such information shall only be provided to such persons to the extent that it is required for use on the Recipient's behalf in performing its duly authorized activities at or in connection with the Projects and shall be provided only on a need-to-know basis; nor shall any copies of documents or materials in any form, format or medium, which contain disclosures of such Confidential and Privileged and/or Confidential Information, be made without the prior written consent of the Port Authority.

8. Confidential and Privileged and/or Confidential Information shall not be disclosed to persons other than those employed by or acting on behalf of the Recipient who have a need to know and/or a need to have access to the information without the express permission of the Port Authority in its sole discretion; and if such permission is granted then such information will be provided only upon the execution of an acknowledgment (the "Acknowledgement"), the form of which is attached hereto as Exhibit A, by the person receiving the information, agreeing to be bound by this Agreement.

10. If a subpoena, discovery request, Court Order, Freedom of Information Request, or any other request or demand authorized by law seeking disclosure of any Confidential and Privileged and/or Confidential Information is received, the Port Authority will immediately be notified of such request or demand so that it may seek to quash the subpoena, seek a protective order, or take such other action regarding the request as it deems appropriate, and the

undersigned will fully cooperate in the Port Authority's efforts in this regard so as to assure that confidential treatment will be afforded the Confidential and Privileged and/or Confidential Information. In the absence of the protective order, disclosure will be made of only that part of the Confidential and Privileged and/or Confidential Information as is required to be disclosed, after advising and consulting with the Port Authority, the Recipient and their respective counsel as to such disclosure and the nature and wording of such disclosure. If at any time the Confidential and Privileged and/or Confidential Information is inappropriately disclosed, the undersigned will immediately report that fact and the circumstances regarding such disclosure to the Port Authority.

11. Upon the earlier occurrence of either the Port Authority's written request, or termination of the business relationship or of the negotiations which gave rise to this Agreement, Recipient shall promptly return to the Port Authority, or destroy, at Recipient's expense, all tangible materials describing, analyzing, containing, or referring or relating to, the Confidential and Privileged and/or Confidential Information, including, but not limited to, all originals, extracts, studies, copies, and summaries, whether received from the Port Authority or created by Recipient, or its representatives, and regardless of the medium in which the Confidential and Privileged and/or Confidential Information was provided or maintained, including any information stored in electronic form, which shall also be completely removed from any computer database; provided, however, that Recipient may retain copies of Confidential and Privileged and/or Confidential Information in accordance with the requirements of this Agreement if (a) such retention is required for professional reasons, and (b) Recipient received the express written consent of the Port Authority's authorized representative for such retention. If the Recipient elects to destroy the Confidential and Privileged and/or Confidential Information, then the Recipient shall deliver to the Port Authority a certification, in the form attached hereto as Exhibit B, signed by an authorized representative of the Recipient confirming its compliance with this requirement.

12. The obligations under this Agreement will be perpetual (unless otherwise provided in this Agreement) or until such time as the information is no longer considered Confidential and Privileged and/or Confidential.

13. If any term or provision of this Agreement shall be determined invalid or unenforceable to any extent or in any application by any court of competent jurisdiction, the validity and enforceability of the remaining provisions will not be affected thereby.

14. Recipient acknowledges and agrees that the unauthorized disclosure and handling of the Confidential and Privileged and/or Confidential Information could have an adverse and detrimental impact on public safety and security and significantly endanger the Port Authority, its facilities, its patrons and the general public.

15. Recipient hereby expressly agrees that the obligations of confidence required hereunder are extraordinary and unique and are vital to the security and well-being of the Port Authority, its customers, facilities and the general public, and that any breach by it or its representatives of the terms hereof will result in unique and immeasurable harm to the Port Authority for which monetary damages would be inadequate. Accordingly, Recipient hereby

agrees that if it breaches or threatens to breach this Agreement, the Port Authority shall be entitled, in addition to all other rights or remedies available at law or in equity, to seek temporary or permanent injunctive relief, without the necessity of proving damages or to post any bond or other security, in order to prevent further breach.

16. This Agreement shall be governed by and construed in accordance with the laws of the State of New York, without regard to the conflict of laws principle.

17. Any violation of this Agreement may result in legal and/or disciplinary action against the Recipient, and any individual violating this Agreement and the signed acknowledgment.

18. The failure of any party to enforce, at any time, or for any period of time, any provision of this Agreement shall not be construed to constitute or evidence a waiver of such provision or the right of such party to enforce each and every provision thereafter.

19. This Agreement constitutes the entire agreement between the Port Authority and Recipient on the subject matter contained herein and supersedes any and all prior negotiations, correspondence, agreements, understanding, duties or obligations between the parties hereto respecting the subject matter hereof. The provisions of this Agreement may be amended, modified or revoked, in whole or in part, only by a written instrument executed by each of the parties to this Agreement.

20. This Agreement is the joint product of the parties hereto and each provision of this Agreement has been subject to the mutual consultation, negotiation, and agreement of the parties hereto, and shall not be construed for or against any party hereto.

Dated: New York, New York
_____, 2007

By: _____

Name:
Title:

Exhibit A

ACKNOWLEDGEMENT

I, _____, am employed as a(n)_____(fill in job title) by_____ (fill in employer) located at _____. I understand that, because of my employer's relationship with _____ (fill in the other Party to the agreement with the Port Authority), both my employer and I are being, or may be, provided with access to, and/or copies of, certain sensitive security materials and information relating to the Project. I have been provided with and read _____ (fill in the Party's name) Non-Disclosure and Confidentiality Agreement with the Port Authority of New York and New Jersey, executed by _____ (fill in the Party) on _____, 2007. If it is required for me to review or receive information provided by the Port Authority that is marked "CONFIDENTIAL AND PRIVILEGED", "CONFIDENTIAL", "SENSITIVE SECURITY INFORMATION," and/or "(PROTECTED) CRITICAL INFRASTRUCTURE INFORMATION", I acknowledge that I will be bound by each and every term and provision contained therein and that failure to do so may include, but is not limited to, the imposition of disciplinary action and sanctions, and/or the institution of legal action seeking injunctive relief, monetary and/or criminal penalties for violation of law and/or Port Authority policies and procedures, as well as for violation of federal and/or state regulations.

To the extent I am currently in possession of, or have previously come in contact with, marked information as it relates the aforementioned Agreement, I agree to conform my handling procedures for "CONFIDENTIAL AND PRIVILEGED," "CONFIDENTIAL", "SENSITIVE SECURITY INFORMATION," and/or "(PROTECTED) CRITICAL INFRASTRUCTURE INFORMATION" to the practices and procedures set forth and defined herein or risk loss of access to said information, removal from said project and/or subjecting myself to the aforementioned disciplinary actions and/or civil and criminal penalties.

NAME OF RECIPIENT_____
Print Representative Name:_____
Signature:_____
Title:_____
Date:_____

Exhibit B

CERTIFICATION

To: The Port Authority of New York and New Jersey (the "Port Authority")

Reference is made to the Non-Disclosure and Confidentiality Agreement (the "Agreement") between the Port Authority and _____(the "Recipient") dated _____. Capitalized terms used and not otherwise defined herein shall have the meanings ascribed to them in the Agreement. Pursuant to the Agreement, the Recipient hereby certifies the following to be true:

> The Recipient has destroyed and has caused its agents to destroy all tangible materials describing, analyzing, containing, or referring or relating to, the Confidential and Privileged and/or Confidential Information, including, but not limited to, all originals, extracts, studies, copies, and summaries, whether received from the Port Authority or created by Recipient, or its representatives, and regardless of the medium in which the Confidential and Privileged and/or Confidential Information was provided or maintained, including any information stored in electronic form, which shall also be completely removed from any computer database, to the extent that the destruction would preclude recognition or reconstruction of the Confidential and Privileged and/or Confidential Information.

By: _____
Name:
Title:

Date: _____

ATTACHMENT L

THE PORT AUTHORITY OF NY & NJ

Standards & Guidelines

for Port Authority Technology

For Publication in RFPs

Technology Services Department

Version 2.9

December 31, 2003

Introduction **6**

Introduction 6

1.0 The Port Authority Wide Area Network (PAWANET) **7**

1.1 PAWANET Overview 7

1.2 Network ATM Node Assignments 7

1.3 Network Diagram 8

1.4 Inter-site Services Providers 8

1.5 PAWANET Functions 8

1.6 Features of PAWANET 8

1.7 Supported Protocols 9

1.8 PAWANET Switches and Routers 9

Cisco ISDN routers 1.9 Enterprise Addressing Scheme (including IP addressing) ←Format changed to "Heading 2" for this bullet 9

1.10 Enterprise Network Monitoring Software 10

2.0 Network Resources **11**

2.1 Network Overview 11

2.2 Enterprise Network Architecture 12

2.2.1 Operating System and Software 12

2.2.2 Configuration 13

2.2.3 Network Resources Security 14

2.2.4 Network Access and User Account Security 15

2.2.5 Remote Access System 17

2.2.6 Network Resources Hardware Standards 18

2.3 Network Naming Conventions 19

2.3.1 Server Names 19

2.4 Directory Services and Structure 19

2.5 System Management 19

2.5.1 Technology Services Department and Departmental Business System Manager Responsibilities 20

2.5.2 Change Management 22

2.5.3 Turning Over a New LAN Resource to the System Administrator 23

2.6 System Backup and Recovery 23

2.6.1 Backup Logs 24

2.6.2 Backup Scheduling 24

2.7 Business Resumption Plan 24
2.8 Telecommunications Standards for Enterprise Network Resources 25
2.8.1 Closet and Telecommunications Room Access 25
2.8.2 Telecommunications Installation Contractor's Responsibilities 26
2.8.3 Electrical Requirements 26
2.8.4 Telephone Company Interface 27
2.9 Documentation 27
3.0 Virus Scanning & Management 28
3.1 Overview 28
3.2 Standards 28
3.3 Virus Protection Stand Alone, Laptop PCs and Personal Digital Assistants (PDAs)28
3.4 Acquisition and Installation 29
3.5 Detection and Incident Response 29
4.0 Electronic Mail 30
4.1 E-Mail Overview 30
4.2 Policy on Use of E-Mail: Highlights 30
4.3 E-Mail Etiquette 31
4.4 E-Mail System Architecture 31
4.6 to E-Mail 31
5.0 Intranet 32
5.1 Intranet Overview 32
5.3 eNet Software Infrastructure Standards & Guidelines 32
5.3.1 Design Guidelines 33
6.0 Workstation and Workstation Operating System 36
6.1 Overview 36
6.3 Workstation Operating System Standard 36
6.4 Workstation Configuration 36
6.4.1 Workstation Naming Conventions 36
6.4.2 Workstation User Accounts 36
6.4.3 Remote Workstation Management 36
6.4.4 Drive Mappings 37
6.4.5 Standard Workstation Hardware Configurations 37
6.5 Standard Department Workstation Software 37

6.5.1 Standard for New Installations 37
6.5.2 Alternate Standard for Existing Installations 37
6.6 Enterprise Software 38
6.6.1 PeopleSoft 38
All access to PeopleSoft is obtained upon receipt of properly authorized access forms, signed by the requesting department, and processed through the Human Resources & Comptroller's Department.6.6.2 ..... SAP 38
All access to SAP is obtained upon receipt of properly authorized access forms, and an indication by the requesting department of the license to be assigned to the requestor.6.6.3 ..... Other Business Applications 38
6.7 Workstation Security 38
6.7.1 Physical Security 38
6.7.2 Logical Security 39
6.8 Support Desk 39
6.8.1 Functions 39
6.8.2 Hours of Staffing 40
6.9 Computing Resources Policy 40
7.0 Distributed Systems Environment 41
7.1 Overview 41
7.2 Microsoft Windows Servers 41
7.2.1 Configuration 41
7.2.3 Microsoft Windows Server Logical Security 41
7.3 Unix 42
7.3.1 Configuration 42
7.3.2 Unix Logical Security 42
7.4 OS/390 43
7.5 Databases 43
7.6 Application Security 43
7.7 Server Physical Security 43
8.0 Voice Network 44
8.1 Voice Networks (Telephone) Services 44
8.1.1 Port Authority Telephone Network 44
9.0 Vendor Provided Dedicated Systems 44
9.1 Overview 44
9.2 Physical Security Technology Standards 44

9.2.1 Agency Standard for Digital Video Recording and Access Control and Alarm Monitoring 44

10.0 Wireless Technologies 46

10.1 Wireless Guidelines 46

10.1.2 General Policy 46

10.1.3 Personal Area Networks - PAN 46

10.1.4 Wireless Local Area Networks - WLANs 46

10.1.5 Portable Electronic Devices (PEDs) – Cellphones, PDAs, messaging devices, laptops and tablets. 48

10.1.6 Cellular and Wireless Email 48

10.1.7 Synchronization 48

10.1.8 Responsibilities of Technology Services Department 49

10.1.9 Responsibilities of CTO 49

10.1.10 Responsibilities of Wireless and Handheld Device Users 50

Appendices 51

Appendix 2 – Business Resumption Plan Document Format 53

Appendix 2 – Business Resumption Plan Document Format 53

Appendix 3 – Communication Rooms/Closets Standards 55

Appendix 4 – Cabling 56

Appendix 5 – Port Authority Unified Wiring Plan 56

Appendix 6 – Telephone Closet / IDF Termination Blocks 59

Appendix 7 – Workstation Jacks 59

Appendix 8 – Standard Switches Inside the Department 59

Appendix 9 – Desktop and Lateral Cable Identification Management 59

Introduction

Introduction

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

- Implement computing and networking solutions that ensure the utmost reliability, availability and security.
- Procure hardware and software that advances current and mandated business needs and enables departments to work with other departments/offices more effectively.
- Easily and efficiently communicate and exchange information throughout the agency.
- Achieve greater systems integration through leveraging and building upon standardized infrastructure and facilitating systems management.

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

How to Use This Document

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

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

1.0 The Port Authority Wide Area Network{ XE "Wide Area Network" }{ XE "Networks" } (PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" })

1.1 PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } Overview

The Port Authority (PA) has a modern distributed computing network, called the Port Authority Wide Area Network{ XE "Wide Area Network" }{ XE "Networks" } (PAWANET{ XE "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 link s.

This network is crucial to all Port Authority businesses because it provides the connections for applications such as e-Mail, Internet and Intranet{ XE "Intranet" } access, SAP{ XE "SAP" }, PeopleSoft{ XE "PeopleSoft" }, Electronic Toll Collection, CADD, Lease Image, Closed Circuit Television (CCTV{ XE "Closed Circuit TV" }) surveillance systems, and in the future, videoconferencing, and more.

PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } consists of state-of-the art Cisco{ XE "Cisco" } Systems equipment and services provided by several other vendors. Equipment includes Asynchronous Transfer Mode (ATM{ XE "Port Authority Wide Area Network (PAWANET): ATM Node Assignments" }{ XE "ATMs" }) switches, high performance Cisco Catalyst switches, and Cisco routers. Cisco Systems maintains all network equipment. AT&T{ XE "AT&T" } provides leased high-speed data lines connecting various Agency facilities to form a Wide Area Network{ XE "Wide Area Network" }{ XE "Networks" } (WAN).

The standard for all application, database, print, file servers and personal computers is IBM. Specific models, images and part numbers will be provided to the successful proposer.

1.2 Network{ XE "Networks" } ATM{ XE "Port Authority Wide Area Network (PAWANET): ATM Node Assignments" }{ XE "ATMs" } Node{ XE "Nodes" } Assignments

The network consists of 22 ATM{ XE "Port Authority Wide Area Network (PAWANET): ATM Node Assignments" }{ XE "ATMs" } nodes, which together form a private Port Authority ATM network.

Non-ATM{ XE "Port Authority Wide Area Network (PAWANET): ATM Node Assignments" }{ XE "ATMs" } nodes are connected to the ATM core network.

1.3 *Network{ XE "Networks" } Diagram{ XE "Port Authority Wide Area Network (PAWANET): Diagram" }*

This diagram will be supplied as appropriate to the successful proposer.

1.4 *Inter-site Services Providers*

The Technology Services Department has contracted with a variety of companies to provide inter-site services. If departments have need for expanding their WAN{ XE "Wide Area Network" } services, such as a request for additional data lines, the Technology Services Department must be contacted. Companies providing communications services for the Wide Area Network{ XE "Networks" } are listed below.

- AT&T{ XE "AT&T" } Local Service{ XE "Local Service" }s
- Verizon{ XE "Verizon" }
- MCI WorldCom

1.5 *PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } Functions{ XE "Port Authority Wide Area Network (PAWANET): Functions" }*

Currently PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } provides the following functions:

Data	Supports the low and high volume transfer of data used for applications, such as SAP{ XE "SAP" } and PeopleSoft{ XE "PeopleSoft" }, and for network communications, such as e-Mail.
CCTV{ XE "Closed Circuit TV" }	The transfer of Closed Circuit TV{ XE "Closed Circuit TV" } (CCTV) data is supported across the entire network to provide security for the Port Authority's key facilities.
Voice	The network provides the hardware capabilities for voice transmission for future implementation.
Videoconferencing { XE "Videoconferencing" }	The network switches and transmission lines are capable of handling videoconferencing to support the agency's future needs.

1.6 *Features of PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" }*

PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } provides a high performance and reliable fail-safe communications network. These are its key features:

- Alternate paths of communication
- Support of high volume traffic such as CADD, CCTV{ XE "Closed Circuit TV" } and others

- Logical Permanent Virtual Circuits (PVC's) to direct traffic based on its priority level.
- ATM{ XE "Port Authority Wide Area Network (PAWANET): ATM Node Assignments" }{ XE "ATMs" } nodes have a redundant power supply and redundant cabling for alternate routing in the event of a node card failure.
- Dual ATM{ XE "Port Authority Wide Area Network (PAWANET): ATM Node Assignments" }{ XE "ATMs" } switches.
- Cisco{ XE "Cisco" } router family products with redundant power supplies.

1.7 Supported Protocols{ XE "Port Authority Wide Area Network (PAWANET): Supported Protocols" }{ XE "Protocols" }{ XE "Port Authority Wide Area Network (PAWANET): Protocols" }

The network supports the following network protocols, allowing dissimilar platforms to communicate within PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" }:

TCP/IP:{ XE "IP Addresses" }{ XE "TCP/IP" }	TCP/IP{ XE "TCP/IP" }{ XE "IP Addresses" } is the universal protocol that allows communications between all systems within the Port Authority's network, as well as other networks.
IPX/SPX:{ XE "IPX/SPX" }	This protocol allows communications between all Novell platforms.
SNA/SDLC:{ XE "SNA/SDLC" }	This protocol allows communications between all IBM systems and other systems that support SNA.

1.8 PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } Switches{ XE "Switches" }{ XE "Port Authority Wide Area Network (PAWANET): Switches and Routers" } and Routers{ XE "Routers" }

The current standard switches and routers used on PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } are:

- Cisco{ XE "Cisco" } switches
- Cisco{ XE "Cisco" } routers

Cisco{ XE "Cisco" } ISDN routers

1.9 Enterprise Addressing Scheme{ XE "IP Addresses" }

(including IP addressing) ←Format changed to "Heading 2" for this bullet

The Port Authority's Enterprise network is a TCP/IP{ XE "TCP/IP" } Class B network

1.10 Enterprise Network{ XE "Networks: Enterprise Network" }{ XE "Networks" } Monitoring Software{ XE "Port Authority Wide Area Network (PAWANET): Network Monitoring Software" }{ XE "Networks: Monitoring Software" }

- The Port Authority continually monitors its WAN{ XE "Wide Area Network" } and the availability of its links.

2.0 Network Resources{ XE "Networks" }

2.1 Network{ XE "Networks" } Overview

The Port Authority has a modern distributed computing network, which is managed as an Enterprise resource. The network connects all individual PCs{ XE "Workstations" }, 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{ XE "Networks: Enterprise Network" } consists of the PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } (see Section 1.1) and connected Local Area Networks (LAN's). The line of demarcation between the cable and wiring which is the responsibility of the carrier and the Port Authority's area of responsibility is usually a wiring closet. The Port Authority's Enterprise Network{ XE "Networks" } consists of the following components on the Port Authority side of demarcation:

- Enterprise Devices
  - Cabling{ XE "Telephone Network: Cabling" }{ XE "Cabling" }
  - Routers{ XE "Routers" }{ XE "Port Authority Wide Area Network (PAWANET): Switches and Routers" }
  - Switches{ XE "Switches" }{ XE "Port Authority Wide Area Network (PAWANET): Switches and Routers" }
  - Wiring Closets{ XE "Wiring Closets" }
  - Communications Equipment Racks
  - Server{ XE "Servers" } Racks{ XE "Servers: Racks" }
  - File and Print Servers{ XE "Servers" }
  - Application Servers{ XE "Servers: Application" }{ XE "Servers" }
  - Storage Area Networks{ XE "SANs" } (SAN)
  - Network{ XE "Networks" } Printers{ XE "Printers" }
- LAN Devices{ XE "LAN Devices" }
  - Desktop PCs{ XE "Workstations" }
  - Workstations
  - Laptops{ XE "Laptops" }
  - Local Printers{ XE "Printers" }
  - Scanners{ XE "Scanners" }
  - Copiers
  - PC Peripherals

The purpose of the following subsections is to:

- Define the policies and standards governing Enterprise and LAN resources throughout the Port Authority.
- Delineate the duties and responsibilities of the Enterprise System Administrator{ XE "System Management" }s, the Technology Services Department (TSD), and the Departmental System or Application Manager.

See the Guide to Systems Administration (this will be made available during the contract negotiation phase) for detailed information on system requirements and procedures.

2.2 *Enterprise Network{ XE "Networks: Enterprise Network" }{ XE "Networks" } 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{ XE "Wide Area Network" }{ XE "Networks" }. The flexibility provided by the use of multiple servers, server clusters and Storage Area Networks{ XE "SANs" } (SAN) offers users improved network response, greater reliability, increased data security and reduced operating cost. Adherence to the standards outlined in this section allows departments to manage their systems, applications and data in a way that best meets their business needs while maintaining interoperability and safeguarding Port Authority's information assets.

2.2.1 Operating System{ XE "Operating Systems" } and Software

All Enterprise file & print services in the Port Authority are based on the Novell Netware{ XE "Netware" } operating system. Microsoft Windows NT{ XE "Windows NT" } and Windows 2000{ XE "Windows 2000" } servers and Sun Solaris{ XE "Sun Solaris" } are supported only as application servers and only when required for functionality.

The standard for all application, database, print, file servers and personal computers is IBM.

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

- Virus Protection{ XE "Virus: Protection" }
- Network{ XE "Networks" } Security{ XE "Networks: Security" }{ XE "Security" }
- Remote Monitoring and Management
- Intrusion Detection{ XE "Intruder Detection" }
- Mainframe Systems Backup
- Uninterrupted Power Supply{ XE "Uninterrupted Power Supply" } (If central UPS is not installed at the location)
- Current Novell NetWare Support Pack

The standard for all application, database, print, file servers and personal computers is IBM. Specific models, images and part numbers will be provided to the successful proposer.

2.2.2 Configuration

All network devices--including servers, workstations, network printers, and network faxes--must contain IP{ XE "IP Addresses" } addresses which conform to the standards outlined in sections, 1.9 *Enterprise Addressing Scheme*, and 2.3.1, *Server{ XE "Servers" } Names, and which will be assigned by Technology Services Department Infrastructure staff{ XE "Servers: Names" }*. In addition, all Novell servers must include an IPX address provided by the Network{ XE "Networks" } Architecture Division.

System Administrator{ XE "System Management" }s may refer to the *Guide to System Administration* for specific instructions on how to install and configure the Novell and Windows operating systems. All Novell servers must be configured using the following parameters:

- Minimum Size of DOS Partition{ XE "Partition" }: 1GB
- Both IP{ XE "IP Addresses" } and IPX Protocol{ XE "IPX Protocol" }s{ XE "Protocols" }{ XE "Port Authority Wide Area Network (PAWANET): Protocols" }
- Frame Type for IPX protocol: IPX Ethernet_802.2
- Volume Names: SYS, DATA, APPS

2.2.2.1 Workstation{ XE "Workstations" } Drive Mapping{ XE "Workstations: Drive Mapping" }{ XE "Drive Mappings" } Conventions

Mapping of workstation drive pointers to SAN{ XE "SANs" } or server disk volumes or folders is accomplished through the Novell NetWare Login{ XE "Logins" } Script. Guidance will be provided by Infrastructure staff as needed.

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

  Example: P:\APPS

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

  Examples: P:\APPS\EXCEL
  P\APPS\LOTUS

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

Example <Server{ XE "Servers" } _name>:\DATA\SHARE on a single server

2.2.2.2 Connecting LAN Devices{ XE "Networks: Connecting LAN Devices" }{ XE "LAN Devices" } to the Enterprise Network{ XE "Networks: Enterprise Network" }{ XE "Networks" }

The Technology Services Department is responsible for connecting all LAN devices to the Enterprise Network{ XE "Networks: Enterprise Network" }{ XE "Networks" } (PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" }) provided they meet the Port Authority's standards. The following system components must meet the standards in order to connect department devices.

Type of Device or Software

- Primary Network{ XE "Networks" } Operating System{ XE "Networks: Operating Systems" } (NOS{ XE "Operating Systems" })
  - Application Server{ XE "Servers" } Operating System{ XE "Operating Systems" }
  - Network{ XE "Networks" } Interface Card{ XE "Network Interface Card" } (NIC)

The standard for all application, database, print, file servers and personal computers is IBM. Specific models, images and part numbers will be provided to the successful proposer.

2.2.3 Network Resources{ XE "Networks" } Security{ XE "Security" }

2.2.3.1 Server{ XE "Servers" } Physical Security{ XE "Servers: Physical Security" }{ XE "Workstations: Security" }{ XE "Security: Physical Security" }{ XE "Security" }

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

2.2.3.2 Server{ XE "Servers" } Logical Security{ XE "Servers: Logical Security" }{ XE "Security" }

To safeguard the Port Authority's Information Technology (IT) systems and data, TSD has implemented a number of processes and procedures, including the requirement that all users accessing the Port Authority's networks authenticate to the Novell NetWare Directory Service (e-Directory). The e-Directory Service is a database containing descriptions of all network devices including servers, printers, shared drives and user accounts.

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

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

- Guard against unauthorized access by making sure that servers cannot be booted from a floppy.
- Scan all workstations for viruses daily.
- Scan all laptops for viruses at log-in.
- Scan all incoming data from users, server peripherals, diskette, CD-ROM, tape drives, other servers, and the Internet for viruses
- Perform daily incremental backups and full backups weekly.
- Store all monthly backups off site at a secure location and secure daily and weekly backups on-site in a locked area.
- Test recovery procedures annually.
- System and application passwords that conform to the Technology Services Department standards.
- Configurations must conform to security parameters identified by Kane Security{ XE "Security" } Analyst software.
- Perform deleted file purges immediately or no later than 6 days after file deletion.
- Control all remote access using the Port Authority's Remote Access{ XE "Email: Remote Access" } System via a VPN using a PA providor.

2.2.4 Network{ XE "Networks" } Access{ XE "Networks: Access" } and User Account{ XE "User Accounts" } Security{ XE "User Accounts: Security" }{ XE "Security" }

2.2.4.1 Account Creation{ XE "User Accounts: Creation" }

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

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

Example:	**User's Name**	**Novell Login{ XE "Logins" } ID**
	Tony Robinson	trobinson

When the Novell Login{ XE "Logins" } ID is assigned, see the Guide to Systems Administration for additional examples of alternative account names to use.

2.2.4.2 Time Restrictions{ XE "Time Restrictions" }

The standard time restriction for user access is 6 AM to 9 PM, Monday through Friday. Time restrictions may be modified to allow for authorized access where warranted and at the discretion of individual department system managers. Requests and approval for access outside of the standard hours should be documented and retained by the System Administrator{ XE "System Management" }.

2.2.4.3 Concurrent Logins{ XE "Logins: Concurrent" }{ XE "Networks: Logins" }{ XE "Logins" }

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

2.2.4.4 Intruder Detection{ XE "Networks: Intruder Detection" }{ XE "Intruder Detection" }

These system-monitoring features should be active.

- Restrict the count of incorrect login attempts
- The time out feature for which unsuccessful login attempts are retained to determine a possible intruder attack should be used
- The time feature for which a user account remains disabled before the account can be used again should be used.

2.2.4.5 Passwords{ XE "Passwords" }

All user accounts should have passwords conforming to the following standards.

- Minimum length is six (6) characters.
- Should not be easily guessed. It should not be related to one's job and should not be a word in the dictionary or a proper name.
- Should be set to expire at least every 90 days and 30 days for accounts with system or application administrator access.
- Grace logins should be activated and limited to three.
- Users should be notified several days in advance of password expiration.
- Users should be forced to change their password on initial login and once it expires.
- Unique passwords should be required when changed. Users should be prevented from reusing a previous password for a minimum of one-year.
- Users should not be permitted to change their passwords more than once a day.
- Passwords{ XE "Passwords" } should be encrypted in storage.

- Passwords{ XE "Passwords" } must be entered in a non-display field with a re-enter verify function for new passwords.
- Passwords{ XE "Passwords" } must not be available on hard copy.
- Passwords{ XE "Passwords" } used in system startup files and login scripts must be encrypted.
- If an application uses a default password, change it on installation .
- Do not use cyclical passwords, such as the word, February, during the month of February.
- Do not reveal your password to anyone except authorized persons.
- Use both upper and lower case characters and special characters where possible.
- Change password if it has been disclosed or compromised.
- Protect by using a screen saver password with a recommended 15-minute time-out period.
- Passwords{ XE "Passwords" } should not be the same as the user ID

Passwords{ XE "Passwords" } are considered confidential data. They protect the Port Authority's network resources and grant system privileges and access. Disclosure may result in unauthorized access to data, system files and transactions. Passwords are also your signature and identify you as the individual who is responsible for the system activity.

2.2.4.6 Modems{ XE "Modems" }

Staff are prohibited from connecting dial-up modems to workstations that are simultaneously connected to PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } or another internal communication network unless approved by the Information Systems Security{ XE "Security" } Officer.

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

2.2.5 Remote Access{ XE "Email: Remote Access" } System

The use of local modems to establish direct dial connections to devices on the PA network is prohibited. Exceptions to this policy require the approval of the Technology Services Department's Security{ XE "Security" } Officer. There is an approved remote access solution (via a VPN using a PA provider), which provides a secure access to the corporate network, requiring additional software & passwords for the person who will be connecting remotely. The solution is issued to an appropriately authorized individual. Details of the solution will be disclosed on a need to know basis. This access protocol is in addition to the application security access protocols.

2.2.6 Network Resources{ XE "Networks" } Hardware Standards

2.2.6.1 Standard Servers{ XE "Servers: Standard Hardware" }{ XE "Servers" }

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

The standard for all application, database, print, file servers and personal computers is IBM. Specific models, images and part numbers will be provided to the successful proposer.

2.2.6.2 Printers{ XE "Printers" }

The current standard is the Hewlett Packard family of printers.

2.3 *Network{ XE "Networks" } Naming Conventions{ XE "Networks: Naming Conventions" }{ XE "Naming Conventions" }*

2.3.1 Server{ XE "Servers" } Names{ XE "Servers: Names" }

All server names should conform to the standard code and will be supplied to the successful contractor. Novell servers must be configured with an IPX address obtained from the Network{ XE "Networks" } Architecture Division within the Technology Services Department. All information regarding the names and address configuration should be forwarded to the Standards and Guidelines Group.

2.4 *Directory Services and Structure*

The Port Authority uses Novell e-Directory to manage network resources and user access. All network printers should be created as e-Directory objects. NDPS should be utilized.

. Applications are distributed based on the type of workstation and user definitions, using an automated tool. Scheduling of distributions is done in conjunction with client departments.

2.5 *System Management{ XE "System Management" }*

The Port Authority has retained a third party system administrator. The Proposers System Administration proposal will be evaluated against the third party system administrator the PA has retained for functionality and cost.

All computing at the Port Authority is delivered on -workstations through PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" }. Port Authority departments receive support for their network from the Technology Services Department and the authorized Enterprise vendor. There is a division of responsibility between Technology Services Department and those responsible for the management of departmental network resources.

The department is responsible for selecting a Business System Manager{ XE "System Management" } who will manage the departmental network resources. Technology Services Department will oversee the System Administrator(s). The System Administrator provides day-to-day operational support. The following chart delineates the major responsibilities of Technology Services Department System Administrators and the Departmental Business System Managers. Detailed information concerning System Administrator duties can be found in the Guide to System Administration.

[A copy of this Guide will be provided to the successful contractor.]

2.5.1 Technology Services Department and Departmental Business System Manager{ XE "System Management" } Responsibilities

Technology Services Department Responsibilities	Business System Manager{ XE "System Management" } Responsibilities (May be carried out by department staff, contract with TSD or third party)
Select and install: Servers{ XE "Servers" } Desktop PCs{ XE "Workstations" } CAD{ XE "Computer Aided Design" } Workstations Network{ XE "Networks" } & Local Printers{ XE "Printers" } PC Peripherals Routers{ XE "Routers" }{ XE "Port Authority Wide Area Network (PAWANET): Switches and Routers" } and switches Cabling{ XE "Telephone Network: Cabling" }{ XE "Cabling" } Wiring closet hardware	Select and Manage: Business Applications Software
Promulgate Port Authority Standards for, install and maintain: Workstation{ XE "Workstations" } OS{ XE "Operating Systems" } and configuration Network{ XE "Networks" } OS{ XE "Operating Systems" } and configuration Physical and logical security for: Network{ XE "Networks" } Servers{ XE "Servers" } Workstations PC Peripheral Devices User Accounts{ XE "Workstation:	**Review and Verify** Port Authority Standards for installation and maintenance of: Current Workstation{ XE "Workstations" } OS{ XE "Operating Systems" } Current Network{ XE "Networks" } OS{ XE "Operating Systems" } Physical and logical security for: Network{ XE "Networks" } Servers{ XE "Servers" } Workstations PC Peripheral Devices User Accounts{ XE "Workstation: User Accounts" }{ XE "User

Technology Services Department Responsibilities	Business System Manager{ XE "System Management" } Responsibilities (May be carried out by department staff, contract with TSD or third party)
User Accounts" }{ XE "User Accounts" } Databases{ XE "Databases" } Virus Protection{ XE "Virus: Protection" } Back up and Recovery{ XE "System Backup and Recovery" } Hardware Software Addressing/ Naming Conventions{ XE "Naming Conventions" } for Network{ XE "Networks" } devices	Accounts" } Databases{ XE "Databases" } Virus Protection{ XE "Virus: Protection" } Download and install current virus protection software and data files. Back up and Recovery{ XE "System Backup and Recovery" } Maintain tape library
Establish and monitor Performance and Capacity Standards	**Review and verify** Performance and Capacity reports
Set standards for, and provide database administration	**Monitor** database performance
Establish requirements for Business Resumption Plan{ XE "Business Resumption Plan" }	**Develop, validate and document** Business Resumption Plan{ XE "Business Resumption Plan" } **Implement** Business Resumption Plan{ XE "Business Resumption Plan" } if necessary
Conduct Change Management{ XE "Change Management" } Meetings: Establish version control procedures Create a forum to insure good communication in the agency.	**Review and monitor** Change Management{ XE "Change Management" } tasks: Verify version control Document changes in department devices Inform Technology Services Department of all significant changes — hardware and software.

Technology Services Department Responsibilities	Business System Manager{ XE "System Management" } Responsibilities (May be carried out by department staff, contract with TSD or third party)
Maintain Documentation Library containing, for example: Suppliers' manuals on all software and Hardware Configurations of all servers and workstations Physical media, such as back up tapes.	
Select, configure and deploy software distribution tools.	**Monitor and review software** distributions.
Electronic Messaging to include e-Mail, calendaring and message-enabled applications.	Supply users e-mail setup information as needed
Provide direct support to end users on the use of workstation and applications running on the department's network resources.	
Select and provide virus protection software and data files. **Maintain** a log of all virus scan activity for daily review.	Report all suspected instances of computer viruses immediately to the Virus Response Team{ XE "Virus Response Team" } in accordance with established IT security procedures
	Maintain and control software licenses

Note: System Administrator{ XE "System Management" }s do not create patches or upgrades.

To see a more detailed description of System Administrator{ XE "System Management" } responsibilities, see the Guide to System Administration, or click below. This information will be provided to the successful contractor.

2.5.2 Change Management{ XE "Change Management" }

System Administrator{ XE "System Management" }s are responsible for reporting to the Technology Services Department all changes pertaining to:

Departmental hardware:

All network connected devices, such as:

- Printers{ XE "Printers" }

- Print servers
- Scanners{ XE "Scanners" }
- Network{ XE "Networks" } Interface Card{ XE "Network Interface Card" }s

Software:

- Non-standard operating systems
- Non-standard applications

System administrators are responsible for participating in Change Management{ XE "Change Management" } meetings online via the eNet{ XE "eNet" }; or for making sure that a representative participates.

2.5.3 Turning Over a New LAN Resource to the System Administrator{ XE "System Management" }

Whenever a new departmental network resource goes into production, the installation team or vendor is responsible for turning over to the System Administrator{ XE "System Management" } of the new departmental network resource all of the items on the *Information and Documentation Transition List*. This list will be provided to the successful Proposer.

2.6 System Backup and Recovery{ XE "System Backup and Recovery" }

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

- Mainframe—based tools are used to create data backups that will be stored remotely and managed automatically. The use of mainframe backups is required to assure off-site data storage at a secure facility.
- The System Administrator{ XE "System Management" } is responsible for verifying that system backups, both local and remote can be used to restore the data. Tests of the ability to successfully restore from both backup systems will be performed annually. It is recommended that the test data restore be performed on a single non-critical directory only, not the entire server. Tests of the ability to restore system and application files will be performed on a non-production server in the Lab. When incremental or differential backups are routinely used, the test restore procedure should incorporate both.
- Immediately prior to performing the test restore procedure, do a special full backup on the directories being tested.
- Testing a full restore should only be performed on a non-production server.

The product used will depend on the criticality of the data and the need for redundancy.

The standard for all application, database, print, file servers and personal computers is IBM. Specific models, images and part numbers will be provided to the successful proposer.

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

2.6.1 Backup Logs{ XE "System Backup and Recovery: Logs" }

The System Administrator{ XE "System Management" } should maintain the following logs for a period of two years:

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

2.6.2 Backup Scheduling{ XE "System Backup and Recovery: Scheduling" }

The System Administrator{ XE "System Management" } 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 <u>all</u> files on the server including the e-Directory structure.
- 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 <u>full</u> back up.
- A Grandfather, Father, Son (GFS) scheme based on a 33 tape rotation should be used to ensure complete back up and recovery.
- Store daily and weekly back-up media in a locked fire proof cabinet outside of the server room. Monthly media must be stored outside the immediate building.
- Remote Mainframe backups are stored at the Teleport facility and regularly transported to a secure facility for long-term storage.

2.7 *Business Resumption Plan{ XE "Business Resumption Plan" }*

DO WE REQUIRE A CONTACTOR OR VENDOR TO PROVIDE A BUSINESS RESUMPTION PLAN FOR ACQUIRED SYSTEMS ??????????????

[Marie's thoughts: I think the answer is yes, so long as the customer wants them to, and it's in the scope of work. Otherwise, once they use the system & the dependency is there, what does the customer do? This should lead to a discussion on disaster recovery & what needs to be set up in advance.]

2.8 *Telecommunications Standards{ XE "Telecommunications: Standards" } for Enterprise Network{ XE "Networks: Enterprise Network" } Resources{ XE "Networks" }*

The standards and guidelines for the following telecommunications components, will be provided to the successful contractor.

Appendix 3 -- Standards for Setting up Closets & Communication Room{ XE "Communication Room" }s

Appendix 4 -- Standard Cabling{ XE "Telephone Network: Cabling" }{ XE "Cabling" } Schemes

Appendix 5 -- Unified Wiring Specifications

Appendix 6 -- Telephone Closet{ XE "Telephone Closets" } / IDF Termination Blocks{ XE "IDF Termination Blocks" }

Appendix 7 -- Workstation{ XE "Workstations" } Jacks{ XE "Workstations: Jacks" }{ XE "Jacks" }

Appendix 8 -- Standard Switches{ XE "Switches" }{ XE "Port Authority Wide Area Network (PAWANET): Switches and Routers" }

Appendix 9 -- Workstation{ XE "Workstations" } and Lateral Cable Identification Management

2.8.1 Closet and Telecommunications Room{ XE "Telecommunications Room" } Access

The following standards need to be followed regarding access to closets and communication rooms.

- All telecommunications rooms must be physically secured. Remote locations which are not secured by a guard or within line of sight of personnel must be secured by a card access system and/or video cameras.
- The Network{ XE "Networks" } Connections (NC) group is responsible for installing routers, switches and station drops. They also patch connections and troubleshoot LAN cabling.
- System Administrator{ XE "System Management" }s requiring routine maintenance of data communications equipment should call the Port Authority Help Desk{ XE "Support Desk" }. When new devices or reconfigurations are required, the System Administrator must submit a Service Request Form.

2.8.2 Telecommunications Installation Contractor's Responsibilities

1. Adherence to all of the above specifications.
2. Assurance of labor harmony by providing installation technicians whom currently maintains appropriate union membership.
3. The contractor must supply all cable, blocks, brackets, connectors, jacks, housings, face plates, special tools, etc., as necessary to perform an installation which is satisfactory to the Port Authority.
4. The contractor must label every workstation (jack faceplate) and the corresponding cross connect point (punch down block or patch panel) in accordance with the cable identification management plan, as previously described.
5. Install all Category 5e cabling in the proper manner, with the appropriate number of twists, so as to maintain Category 5e integrity and capabilities, as outlined in the TIA/EIA 568-B.2 standard.
6. The contractor must ensure that cable connections are in accordance with standard telecommunications practices and that all cabling maintains normal connectivity and continuity.
7. All materials must be agreed upon by PA Network{ XE "Networks" } 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. Access to this room will be reserved to TSD staff and an agreed upon member of the site where the PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } equipment is located. This procedure is to ensure the security and the integrity of the Port Authority's computer network and its users.

2.8.3 Electrical Requirements{ XE "Telecommunications: Electrical Requirements" }{ XE "Electrical Requirements: Telecommunications" }

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

- Standard 110/120 volt power receptacles
- Standard and/or NEMA 5L-30P 208/220 volt power receptacles
- Dedicated circuit breaker per AC feed, with alternate power source.
- Server{ XE "Servers" } 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{ XE "Uninterrupted Power Supply" } included in the delivered service.

2.8.4 Telephone Company Interface{ XE "Telephone Company Interface" }

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

a) Install a dedicated wall board for Telco demarcs

b) Standard Telco Demarcs:

- P66 Block
- Network{ XE "Networks" } Termination Unit (Rj48 interface) Smartjacks
- Network{ XE "Networks" } Termination Unit (DB15-pin female interface)
- Network{ XE "Networks" } 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

2.9 Documentation

It is the responsibility of the System Administrator{ XE "System Management" } to establish and maintain a library of all documentation designated as standard by the Port Authority. These include archived system files and system backups. System Administrators should refer to the *Guide to System Administration* (to be provided to the successful Proposer) for a list of standard/required documentation.

3.0 Virus Scanning{ XE "Virus: Scanning" } & Management

3.1 Overview

This section describes the standards and guidelines for the prevention, detection and removal of computer viruses and worms. Its purpose is to minimize the risk and negative impact of computer virus infections in the work environment by establishing clearly defined roles, responsibilities and procedures for the effective management of computer viruses. To that end, the Technology Services Department has established a procedure with the Support Desk{ XE "Support Desk" } to provide an expedited response for quick containment. The Support Desk is staffed 24 hours a day, seven days a week.

3.2 Standards

The Contractor will maintain current versions of standard virus protection software and virus detection files established by the Technology Services Department, including configuration-specific instructions for downloading and installing the software on network servers and desktops for use by PC users. The software and instructions will be made available to departmental system administrators through Enet{ XE "eNet" }Standard virus protection software must be installed on all network servers and personal computers, and updated on at least a monthly basis or sooner if notified by Technology Services Department. Departments are required to implement appropriate procedures to ensure adherence to this standard and to promptly report all virus incidents to the Help Desk{ XE "Support Desk" }.

All users must leave the current version of virus scanning software installed on their desktops. The current standards on virus protection software are McAfee. Please contact the TSD Department for the most current information.

REMOVE THE FOLLOWING SECTION

3.3 Virus Protection{ XE "Virus: Protection" } Stand Alone, Laptop{ XE "Laptops" } PCs{ XE "Workstations" } and Personal Digital Assistants{ XE "PDAs" } (PDAs)

Users of stand-alone PCs{ XE "Workstations" }, laptops and PDAs{ XE "PDAs" } are responsible for the virus protection of these devices. When these devices are connected to the network, it is crucial that users follow the PA policy of allowing virus-scanning software to complete its scan before transferring any data into the network. Users of such devices should see their system administrator for assistance in acquiring and installing virus protection software on the device and ensure that the current version of virus scanning software and DAT files are loaded.

All laptop PCs or any PC supplied by a contractor must have the Novell client and virus protection software with current DAT files loaded. The Port Authority requires that all

connectivity to our network be done by logging into Novell prior to accessing any other component of the network.

3.4 Acquisition and Installation

The Technology Services Department will maintain current versions of standard virus protection software and virus detection files, including configuration-specific instructions for downloading and installing the software on network servers and desktops for use by PC users. The software and instructions will be made available to departmental system administrators through eNet{ XE "eNet" }. For assistance in downloading and installing the software, departmental system administrators should contact the Technology Services Department Help Desk{ XE "Support Desk" }.

3.5 Detection{ XE "Intruder Detection" } and Incident Response

When a virus is suspected, the affected user should notify the departmental network System Administrator{ XE "System Management" }. If the System Administrator confirms that a virus may be present, he/she will immediately notify the **Technology Services Department Help Desk{ XE "Support Desk" } at 212-435-7469.** The Help Desk will notify the Virus Response Team{ XE "Virus Response Team" } of the incident. The departmental system administrator will then attempt to eradicate the virus infection and notify the Help Desk of its success or failure.

4.0 Electronic Mail{ XE "Email" }

4.1 E-Mail{ XE "Email" } Overview

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

4.2 Policy on Use of E-Mail{ XE "Email" }: Highlights

The Computing Resources Policy{ XE "Workstations: Computing Resources Policy" }{ XE "Computing Resources Policy" } provides guidance on the appropriate use of e-mail. This policy applies to any person who has access to the E-Mail{ XE "Email" } system. For a complete copy of the policy, contact the TSD Department for the

Computing Resources Policy{ XE "Workstations: Computing Resources Policy" }{ XE "Computing Resources Policy" }

Highlights of the policy are:

- The E-Mail{ XE "Email" } system is not intended to transmit sensitive materials, such as personnel decisions and other similar information.
- All e-mail messages and attachments are property of the Port Authority. The system is not to be used for employee personal gain or in support of any purposes not related to Port Authority business.
- An e-mail message should not be used for disseminating information that is critical and/or needs to be retained longer than 120 days. Such information should only be transmitted as an attachment, for example a Microsoft Word document. The attachment must be filed outside the E-Mail{ XE "Email" } system for retention and security in accordance with the Port Authority Records Retention Program if appropriate.
- The Port Authority reserves the right to review the contents of any e-mail communication when necessary for Port Authority business purposes.
- Employees and other users may not intentionally intercept in any way another person's e-mail messages without prior authorization.
- E-mail may not be used for the solicitation of funds or for messages that are political, harassing, threatening abusive, defamatory, obscene, religious, sexually explicit or unlawful or that infringes on copyrights. Use of e-mail for employee organization business other than communication with management representatives is also prohibited.
- Each message is automatically deleted from a user's mailbox on the Exchange server and from backup media a total of 120 days from the date of receipt or creation. It may be deleted without notice.

- E-mail messages or attachments that you delete may remain active on other recipients' accounts or on backup media, but for no more than seven days on back up media.
- Contractors and other third-party users who are in violation of this e-mail policy may be denied access to the system and legal remedies may be pursued.
- Employees who violate the e-mail policy may be subject to disciplinary action, including dismissal from employment. In addition, misuse of e-mail may be referred for criminal prosecution.
- Passwords{ XE "Passwords" } should be difficult to guess and changed every 90 days to ensure security of the e-mail messages. Users should not share their password with anyone else. Users are accountable for messages sent from their accounts.

4.3 E-Mail{ XE "Email" } Etiquette

Since E-mail is different from paper-based messages, e-mail messages require certain conventions to ensure effective communication. For information on E-mail Etiquette for contract staff please contact the TSD Department for the policy on

E-Mail{ XE "Email" } Etiquette

4.4 E-Mail{ XE "Email" } System Architecture

A managed application service provider hosts the Port Authority E-mail system.

-

4.6 { XE "Email: Remote Access" } to E-Mail{ XE "Email" }

We provide a secure Internet-based web browser access to corporate e-mail utilizing Microsoft's Outlook Web Access. In addition, we have wireless e-mail access utilizing RIM's Blackberry Enterprise Server{ XE "Servers" } and Blackberry handheld devices.

Also, remote access to the Port Authority E-Mail{ XE "Email" } system is available through the Agency provided, VPN based Remote Access{ XE "Email: Remote Access" } System. Please refer to the section on Remote Access System in this document.

5.0 Intranet{ XE "Intranet" }

5.1 Intranet{ XE "Intranet" } Overview

- The Port Authority EmployeeNet (eNet{ XE "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 which are managed as if there were a centralized enterprise resource. It is accessible to all personal computer workstations on the Port Authority Wide-Area Network{ XE "Networks" } (PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" }).

5.3 eNet{ XE "eNet" } Software{ XE "eNet: Software" } Infrastructure Standards & Guidelines

Category	Software Name	Minimum Version
Browser:{ XE "Browsers" }	Microsoft Internet Explorer{ XE "Internet Explorer" }	5.5
Browser{ XE "Browsers" } Plug-in:	Windows Media Player Adobe Acrobat Reader Macromedia Shockwave Player	7.2 4.0 5.0
Web Server{ XE "Servers: Web" }{ XE "Servers" } Software:	Sun Microsystems iPlanet{ XE "iPlanet" } Enterprise Server{ XE "Servers" }	4.0
	Microsoft IIS	4.0
Media Server{ XE "Servers" } Software	Windows Media Server{ XE "Servers" }	6.0
Application Server{ XE "Servers" } Software:	Cold Fusion Enterprise Server{ XE "Servers" }	4.5.2
Development and Design Tools:	Macromedia Dreamweaver{ XE "Dreamweaver" } MX Macromedia Fireworks MX Macromedia Flash MX Adobe Photoshop	6.0 6.0 6.0 7.0
Database{ XE "Databases" }	Oracle{ XE "Oracle" } Database{ XE "Databases" } Microsoft Access	8i 2000

Category	Software Name	Minimum Version
Programming Language/Scripts	ColdFusion{ XE "ColdFusion" } MX Java{ XE "Java" } PERL for Windows JavaScript	6.0 2.0 5.0 1.0
Search Engine Software:	Verity{ XE "Verity" } (Portal One SE)	4.1
Bulletin Board/Discussion:	Chatspace WebBoard	5.0
Streaming Audio:	Windows Media Server{ XE "Servers" }	7.0
Web Performance Monitoring:	WebTrends	7.0
Content Management:	Stellent	6.2

5.3.1 Design Guidelines

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

Departmental Web Site Standards and Guidelines

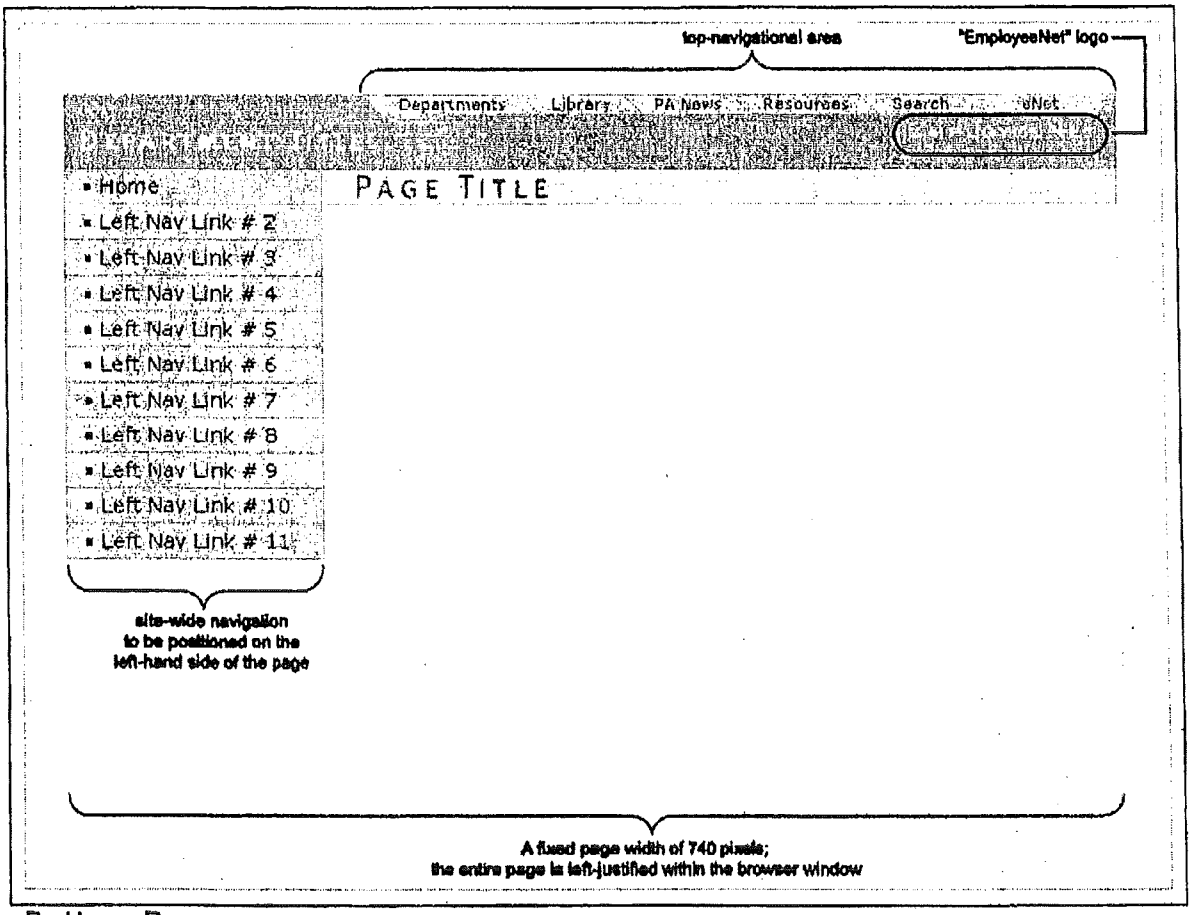
Prescribed standards are assigned to only the following items:

Page Width:	A fixed page width of 740 pixels
Page Justification:	The entire page is left-justified within the browser window
Global Navigation:	A top-navigational area, which provides for global links within eNet{ XE "eNet" }
eNet{ XE "eNet" } Logo:	The top-navigational area includes an accompanying "EmployeeNet" logo whose position is fixed
Resolution:	Pages will be designed for optimal viewing at the 800x600 setting.
Site Navigation:	Site-wide navigation shall be positioned on the left-hand side of each page, except for the home page, where navigational links may be positioned anywhere on the page. All efforts should be made to present the entire navigational scheme without the need to scroll. Positioning of each navigational link must be consistent

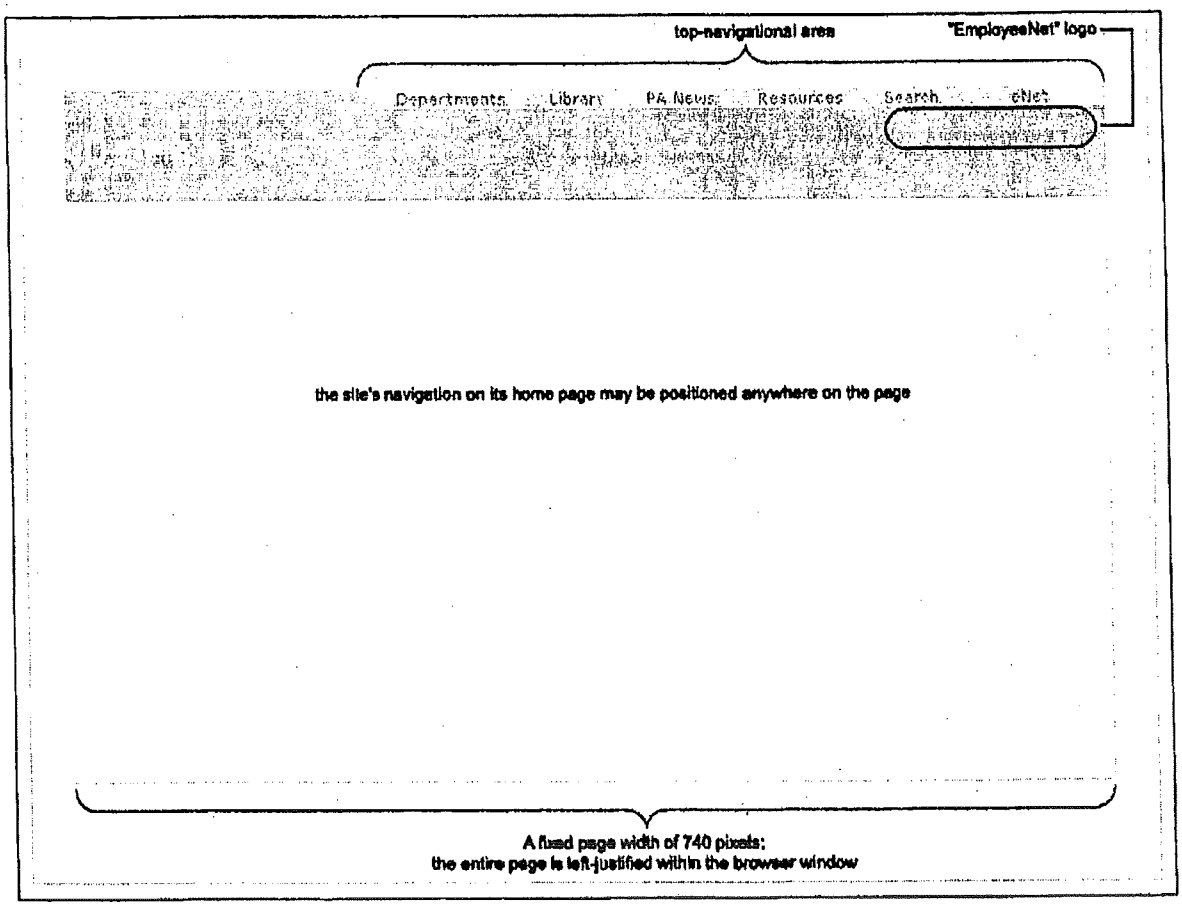
	throughout the entire site.
Masthead - Heading and Subheading:	The design for the masthead area, which included the page heading and sub-heading, shall be flexible and will be developed with the customer department.
Body:	The design for the body area shall be flexible and will be developed with the customer department.

The Departmental Web Site Standards are Illustrated Below:

A. Basic Page



B. Home Page


top-navigational area
"EmployeeNet" logo
Departments
Library
PA News
Resources
Search
eNet
the site's navigation on its home page may be positioned anywhere on the page
A fixed page width of 740 pixels;
the entire page is left-justified within the browser window

6.0 Workstation{ XE "Workstations" } and Workstation Operating System{ XE "Operating Systems" }

6.1 Overview

The Port Authority makes extensive use of workstations networked into an Enterprise Wide Area Network{ XE "Wide Area Network" }{ XE "Networks" } to accomplish its business objectives. In order to ensure compatibility with the agency's Enterprise network and to make optimal use of its resources, this section defines the standards governing workstations and their configuration and use.

6.3 Workstation{ XE "Workstations" } Operating System{ XE "Operating Systems" } Standard

The Port Authority's standard operating system for workstations is Microsoft's Windows 2000. In limited circumstances, where business objectives warrant, alternative operating systems may be deployed with the approval of the department director and concurrence with the Chief Technology Officer.

6.4 Workstation{ XE "Workstations" } Configuration

6.4.1 Workstation{ XE "Workstations" } Naming Conventions{ XE "Workstations: Naming Conventions" }{ XE "Naming Conventions" }

All departmental workstations must contain a unique computer name .

6.4.2 Workstation{ XE "Workstations" } User Accounts{ XE "Workstations: User Accounts" }{ XE "Workstation: User Accounts" }{ XE "User Accounts" }

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

6.4.3 Remote Workstation{ XE "Workstations" } Management{ XE "Workstations: Remote Access" }{ XE "Remote Access" }

The Port Authority also distributes software applications through automated tools.. This will enable remote distribution and updates of software, hardware inventory and workstation troubleshooting.

6.4.4 Drive Mapping{ XE "Workstations: Drive Mapping" }s{ XE "Drive Mappings" }

6.4.5 Standard Workstation{ XE "Workstations" } Hardware Configuration{ XE "Workstations: Hardware Configuration" }{ XE "Hardware Configuration: Workstations" }s

There are standard configurations established for workstations and laptops. The standards specify the product approved for the following devices: processor, memory, storage, CD-ROM/multimedia and monitor. The current workstation will be provided to the successful Proposer:

Workstation{ XE "Workstations" } Hardware Configuration{ XE "Workstations: Hardware Configuration" }{ XE "Hardware Configuration: Workstations" }s

6.5 Standard Department Workstation{ XE "Workstations" } Software{ XE "Workstations: Standard Software" }{ XE "Software: Workstations" }

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

6.5.1 Standard for New Installations

Windows 2000{ XE "Windows 2000" }, Professional Edition

Novell NetWare Client for NT{ XE "Windows NT" }

Novell LAN Workplace Pro

McAfee Associates VShield{ XE "VShield" }

Internet Explore{ XE "Internet Explorer" }r

Microsoft Office 2000 Professional

WinZip

6.5.2 Alternate Standard for Existing Installations

Windows 95{ XE "Windows 95" }B

Novell Client for Windows 95{ XE "Windows 95" }

Novell LAN Workplace Pro

McAfee Associates VShield{ XE "VShield" }

Netscape{ XE "Netscape" } Communicator – Netscape Navigator

Microsoft Office 97

Outlook 98

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

Standard Workstation{ XE "Workstations" } Software

6.6 *Enterprise Software{ XE "Workstations: Enterprise Software" }{ XE "Enterprise Software" }*

The sections below describe the standard Enterprise software.

6.6.1 PeopleSoft

{ XE "PeopleSoft" }

All access to PeopleSoft is obtained upon receipt of properly authorized access forms, signed by the requesting department, and processed through the Human Resources & Comptroller's Department.6.6.2 SAP{ XE "SAP" }

All access to SAP is obtained upon receipt of properly authorized access forms, and an indication by the requesting department of the license to be assigned to the requestor.6.6.3 Other Business Applications

Other Enterprise applications are deployed on occasion to user workstations. This includes systems like the Business Expenses system and others. System Administrator{ XE "System Management" }s are responsible for deploying the workstation clients and network server software according to standards and directions provided by the Technology Services Department. All access to business applications is controlled by the owner departments, and requires authorizations & passwords for each application.

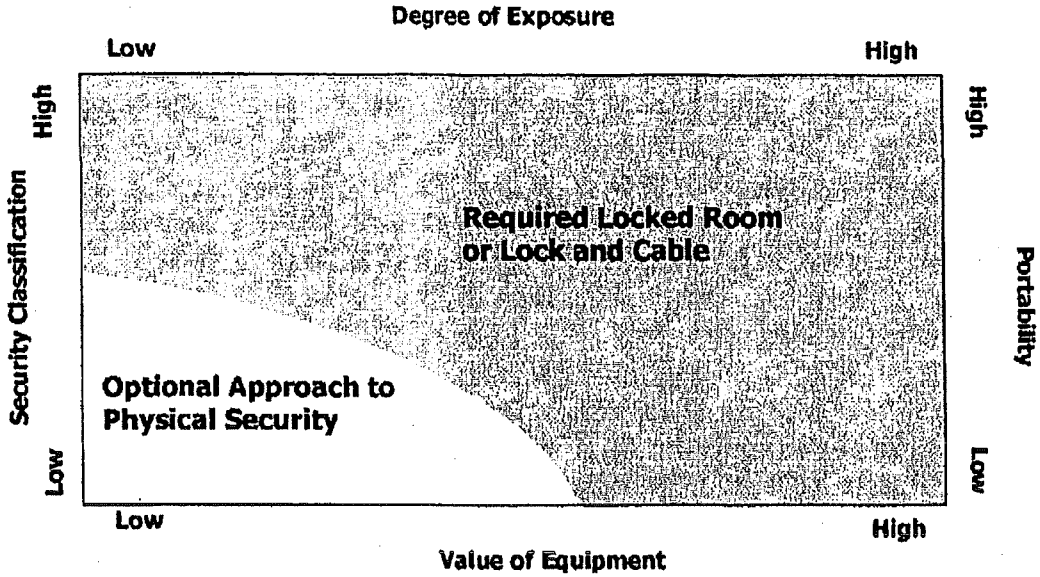
6.7 *Workstation{ XE "Workstations" } Security{ XE "Workstations: Security" }{ XE "Security" }*

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

6.7.1 Physical Security{ XE "Workstations: Security" }{ XE "Security: Physical Security" }{ XE "Security" }

The method of control should be based on the value of the equipment, the sensitivity of the data, its portability and the degree of exposure to theft. The department's Business Systems Manager should make the appropriate determination of physical security required based on their best business judgment. In addition, it is recommended that workstations be assigned a coded theft recovery ID.

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



6.7.2 Logical Security{ XE "Security" }

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

6.8 Support Desk{ XE "Support Desk" }

6.8.1 Functions

The Port Authority Support Desk{ XE "Support Desk" }'s primary role is to provide preliminary troubleshooting, basic assistance, and referral of problems to the appropriate party. Support Desk staff are equipped to answer questions pertaining to vendor packaged software, hardware problems and resetting of passwords. Incoming calls are evaluated and a determination made as to whether the call can be handled by Support Desk staff or must be referred. Support Desk staff maintain records, disseminate and collect information, including listings of appropriate contacts, to ensure that all calls are handled properly.

Using the agency's problem ticketing and referral software, each call is assigned a problem number, then forwarded to one of the following: the System Administrator{ XE "System Management" }, the staff member responsible for that particular problem, or an outside contractor. The ticket number is also given to the employee reporting the problem. When the problem is fixed the Support Desk{ XE "Support Desk" } staff closes the problem ticket. When special issues arise within the agency, Support Desk staff is alerted, who then plan a strategy to resolve the problem and handle incoming calls concerning it.

Reports of outstanding ticketed problems are generated daily by both the Port Authority's referral software, as well the outside contractor's on-line database.

6.8.2 Hours of Staffing

The Port Authority's Support Desk{ XE "Support Desk" } is staffed 24 hours a day, seven days a week. Workstation{ XE "Workstations" } support technicians (SLE) are on site at major facilities from 7:00a.m. to 6:00p.m. Monday through Friday, and on call as needed from 6:00p.m. to 7:00a.m.

6.9 Computing Resources Policy{ XE "Workstations: Computing Resources Policy" }{ XE "Computing Resources Policy" }

Computing resources are intended solely for the Port Authority's business. Resources are not intended for personal gain or in support of any purposes not related to the Port Authority's business. The Port Authority's policy on computing resources is available in the Guide to Port Authority Executive Policy on enet.

7.0 Distributed Systems Environment

7.1 Overview

A number of department and enterprise servers provide critical application and system services. Different operating systems and configurations may be required for specific applications. This section provides information on the standards and guidelines for supported systems within the Port Authority.

7.2 Microsoft Windows Server{ XE "Windows Server" }s{ XE "Servers" }

Microsoft Windows NT{ XE "Windows NT" } v4.0 and Windows 2000{ XE "Windows 2000" }, are supported only as a Network{ XE "Networks" } Operating System{ XE "Networks: Operating Systems" }s{ XE "Operating Systems" } for application servers, and only where required for functionality.

7.2.1 Configuration

Information will be provided to the successful Contractor as appropriate.

All NT{ XE "Windows NT" } servers must be configured with the following parameters:

- Boot partitions)
- All Microsoft Windows servers must be configured as member servers within their assigned domain, or as stand-alone application servers, System proposals containing domain controllers must be submitted to the LAN Planning & Design Group and Standards/QA for review and approval prior to implementation. Submitted documents must contain a design document and an implementation project plan.
- Server{ XE "Servers" } names must adhere to Port Authority standard server naming convention.

7.2.3 Microsoft Windows Server{ XE "Windows Server" }{ XE "Servers" } Logical Security{ XE "Security" }{ XE "Servers: Logical Security" }

All NT{ XE "Windows NT" } servers should be logically secured from unauthorized access. At a minimum, the following configuration settings should be set unless specific services are absolutely required:

- Disable Remote Access{ XE "Email: Remote Access" } Server{ XE "Servers" }
- Physically secure Emergency Repair Disks
- The boot partition should be on a different partition from user data
- Enable weak password filtering
- Enable Administrator account lockout
- Secure and manage event logs

- Encrypt the password database
- Disable Internet Information Server{ XE "Servers" }
- Disable remote registry access

7.3 *Unix{ XE "Unix" }*

7.3.1 Configuration

Sun's Solaris{ XE "Sun Solaris" } 2.5.1 and 2.6 are the currently supported UNIX operating systems for infrastructure and corporate servers, dependent on the level of the operating system supported by the specific application.

7.3.2 Unix{ XE "Unix" } Logical Security{ XE "Unix: Logical Security" }{ XE "Security" }

Unix{ XE "Unix" } servers must be physically and logically secured from unauthorized access. The following settings should be implemented in addition to other server or application security measures taken: IS THIS TOO MUCH INFORMATION?

- The most current security patches must be applied in a timely manner.
- Startup scripts should be modified to disable unnecessary services. Ensure that only the root account can edit startup files.
- Additional logging should be enabled.
- Sendmail should be disabled.
- Verify that a valid account login shell is established for each user.
- Verify that valid home directories are established for all users.
- Restrict access to the crontab file to the administrator account only and ensure crontab and inittab jobs do not access files that are writeable by anyone other than root.
- Disable remote access to the Unix{ XE "Unix" } system as root.
- Disable anonymous FTP{ XE "File Transfer Program" }.
- Never use "xhost+" on an X-server.
- System logfiles containing information about system activity must be reviewed and archived on a regular basis. Logfiles must not be stored in the default location.
- Usage of sensitive commands should be recorded in a system log and reviewed for unusual activity.

Separate accounts should be created for each system administrator who has been granted access to the server. The root account should not be used for daily administrative tasks. The root account should only be accessible via the server console and no remote access provided.

Additional information on these settings is available in the Guide to Systems Administration which will be provided to the successful Proposer.

7.4 OS{ XE "Operating Systems" }/390{ XE "OS/390" }

OS{ XE "Operating Systems" }/390{ XE "OS/390" } (currently release 2.6) is the IBM-supplied operating system on the IBM 3090-400J. This hardware/software supports multiple users and multiple applications. Provided on this platform for transaction-processing applications are TSO/E, ISPF, and CICS. The database is DB2, although other file structures are also supported.

7.5 Databases{ XE "Databases" }

Oracle{ XE "Oracle" } is the preferred database for Port Authority systems. Large databases (those requiring more than 24 hours to recover) should be Oracle 8.0.5 or higher running on a Sun Solaris{ XE "Sun Solaris" } platform utilizing Net8{ XE "Net8" } with a TCP/IP{ XE "TCP/IP" } transport protocol. Medium sized systems should be Oracle 8.0.5 or higher and may be on either a Sun Solaris or Microsoft Windows platform utilizing Net8 with a TCP/IP{ XE "IP Addresses" } transport protocol. Smaller databases may utilize Microsoft's Access and should be selected in consultation with the Technology Services Department customer service manager.

Some specific applications may require Microsoft's SQL Server{ XE "SQL Servers" }{ XE "Servers" }. This database engine should only be used for medium or small databases and in consultation with the appropriate TSD customer technology manager.

For databases, an auditing trail must be enabled for all accounts with administrator privileges.

7.6 Application Security{ XE "Security: Applications" }{ XE "Security" }

Depending on the application residing on the server, security may be administered at the application, database, module, screen, data field, and/or transaction level in addition to network authentication When in production, the administrator responsible for day-to-day administration of the application (Application Administrator) is responsible for maintaining the selected security profiles. At a minimum, all applications must require authentication to Novell Directory Services by way of a network login.

7.7 Server{ XE "Servers" } Physical Security{ XE "Servers: Physical Security" }{ XE "Workstations: Security" }{ XE "Security: Physical Security" }{ XE "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{ XE "System Management" } is responsible for determining the appropriate access control method (receptionist, metal key lock, magnetic card door locks, etc.) He/she must also maintain a list of persons authorized to enter secured areas. Technology Services Department staff is available to provide technical assistance in making this determination.

8.0 Voice Network{ XE "Telephone Network" }{ XE "Networks" }

8.1 Voice Network{ XE "Telephone Network" }s (Telephone) Services

8.1.1 Port Authority Telephone Network{ XE "Networks" }

Most of the Port Authority's telephone services are provided by a Nortel SL100{ XE "Nortel SL100" } Private Branch Exchange{ XE "Private Branch Exchanges" } (PBX) network

9.0 Vendor Provided Dedicated Systems

9.1 Overview

Vendor Provided Dedicated Systems refers to the software and hardware supplied to the Agency by an external provider. Generally these systems are part of a larger Capital Project and are based upon detailed requirements as outlined in a Request For Proposal (RFP). Capital Projects are usually larger scale, multi-year engagements, requiring specialized technical and management staff. These projects have a significant construction component, which typically replaces or adds new physical infrastructure to our facilities and require the coordinated engagement of staff from multiple departments within the Agency and external vendors.

A representative from the Technology Services Department Capital Program Management Group (CPMG) provides a single point of contact for technical oversight, accountability and control.

9.2 Physical Security{ XE "Workstations: Security" }{ XE "Security: Physical Security" }{ XE "Security" } Technology Standards

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

Based upon the Agency's investment in and positive experience with Lenel's access control and alarm monitoring and Loronix's CCTV{ XE "Closed Circuit TV" } and Digital Video recording technologies, these product sets are the Agency's standard (please see below a description of when these standards apply).

The Port Authority has long recognized the need for a corporate architecture for its security systems that would allow us to integrate compatible technologies agency-wide. Terrorist activity in our own region has reinforced the need to maximize the Port Authority's investment while providing for redundancy. Using these standards will improve the Agency's security posture and will permit us to leverage additional operations and business benefits while keeping our operations resources, maintenance and support costs at a minimum.

Guidelines for using the Loronix standard include:

1. If the camera system needs to be recorded
2. When an upgraded or new system is being installed at a PA facility or at a tenant facility monitored or reviewed by Agency personnel or contractors
3. When rule based intelligence is to be added like motion detection and other related algorithm processes
4. If WEB based video needs to be made available
5. When monitoring at remote locations is needed to view on site operations and archived events via the corporate WAN{ XE "Wide Area Network" }
6. When live monitoring is required.
7. When distributed recording is required i.e. at multiple locations, concurrently
8. When network transport (communication) medium has limited bandwidth and the video needs to be sent to designated workstations on the network. Discuss bandwidth issues with Technology Services Department before proposing alternate solutions
9. On all new projects where Loronix is the site base system now.
10. When the OEM department needs override capabilities in the event of an incident.

Guidelines for using the Lenel standard include:

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

10.0 Wireless Technologies

10.1 Wireless Guidelines

{ XE "PDAs" }.

10.1.2 General Policy

When proposing a wireless devices to store, process, transmit or access PA data, the following must be considered:

- Wireless Technologies Vulnerabilities Protection
- Minimum Requirements
- Identification and authentication at both the device and network level.
- Confidentiality encryption of data transmitted is required.
- Data end-to-end over an assured channel (a communication link with security protocol such as Secured Sockets Layer).
- At the device level, implement file system encryption where applicable.
- Devices should not be connected to PA systems for data synchronization, data transfer, or any other purpose without virus protection, mobile code restrictions (executable information delivered to information system and directly executed on any architecture that has appropriate host execution environment) and other preventative measures.

10.1.3 Personal Area Networks - PAN

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

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

Wireless devices should be procured without Bluetooth embedded transmitters, when not possible transmitter should be disabled

10.1.4 Wireless Local Area Networks - WLANs

Advances in wireless technology and pervasive devices create opportunities for new and innovative business solutions. However security risks, if not addressed correctly, could expose the Port Authority to a loss of service, compromise of sensitive information and legal liability.

Wireless is a shared medium. Everything that is transmitted over the radio waves can be intercepted if the interceptor is within the coverage area of the radio transmitters. This represents a potential security issue in the wireless Local Area Networks (LANs). The security exposure is more evident if the wireless LANs are deployed or used in public areas, such as airports, hotels or conference rooms.

The Port Authority has standardized on the Cisco{ XE "Cisco" } wireless technology for LAN & WAN{ XE "Wide Area Network" } which will be supplied to successful proposers.

No wireless network or wireless access point will be installed without being documented, certified and approved by the Port Authority Information Security{ XE "Security" } Officer. Assistance and the appropriate form/checklist for securely implementing and documenting the wireless environment are available directly from the Information Security Officer (ISO) or his/her delegate. It outlines the required security settings to allow you to correctly deploy this technology within the Port Authority.

Suitable controls must be implemented to ensure that a wireless network or access point cannot be exploited to disrupt Port Authority's information services or to gain unauthorized access to PA information. When selecting wireless technologies, 802.1x security features on the equipment must be available and implemented from the beginning of the deployment.

Access to systems that hold non-public information or the transmission of non-public information via a wireless network is not permitted unless appropriate and adequate measures have been implemented and approved by the Port Authority's ISO. Such measures must include authentication, authorization, data protection and logging.

As most wireless networks utilize portable or laptop computers, physical and logical controls should be in place to protect the machine and the information stored on it, including password protection, virus protection, personal firewall software. Laptops{ XE "Laptops" } are to be issued to, and used only by, authorized employees and only for the purpose for which they are issued. The information stored on the laptop is to be suitably protected at all times.

- User level authentication is required for all WLANs.
- Access Points should be an isolated sub-network or virtual LAN.
- Access Points shall be physically secured to prevent unauthorized access, either layer 2 or VPNs meet requirement.
- The following configuration considerations should be taken into account:
- WLAN technologies should not be used for transmitting information without encryption.
- The wired equivalent privacy (WEP) has fundamental flaws because it does not use a FIPS 140-1/2 approved encryption algorithm.
- Virtual Private Network{ XE "Networks" } encryption should be considered for transmission of highly sensitive data.
- WLAN with seamless roaming between access points should have a timeout set at no more than 30 minutes.
- IR (Infrared), Bluetooth and 802.11 peer to peer should be set to "off" as the default setting.

Technology Services reserve the right to audit all WLANs

10.1.5 Portable Electronic Devices (PEDs) – Cellphones, PDAs{ XE "PDAs" }, messaging devices, laptops and tablets.

If a device receives information via a wireless technology, and that device allows that information to be placed directly into the corporate network at the workstation level, then all perimeters and host-based security devices have been bypassed. Therefore the following procedures apply:

- PEDs connected directly to a PA wired network via a hot sync connection to a workstation shall not be permitted to operate wirelessly at the same time. Wireless solutions could create backgrounds into corporate networks.
- IR, Bluetooth and 802.11 peer to peer should be set to "off" as the default setting. Mobile code should be downloaded only from trusted sources over assured channels.
- Anti-virus software should be on devices and workstations that are used to synchronize/transmit data, if available. Where not available on a device, you need to disable the synchronization capability or provide server or workstation based handheld anti-virus protection.
- PEDs are easily lost or stolen therefore approved file system/data store encryption software should be installed.
- PEDs need to be capable of being erased or overwritten to protect data. If the device is no longer needed and cannot be erased or overwritten,it must be physically destroyed.

10.1.6 Cellular and Wireless Email

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

- These devices are not to be allowed into an area where classified information is being discussed unless it is rendered completely inoperable.
- Must have end-to-end encryption.
- PC based redirectors are not allowed as it requires the PC to be active at all times only server based redirectors should be used.
- Electromagnetic sensing shall be periodically performed to detect unauthorized LANs, Bluetooth transmitters etc.

10.1.7 Synchronization

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

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

10.1.8 Responsibilities of Technology Services Department

- Monitor and provide oversight of all PA wireless activities, insure interoperability of wireless capabilities across the agency.
- Develop appropriate technical standards and guidelines for secure wireless and handheld solutions.
- Establish a formal coordination process to ensure protection of PA information with PA information systems employing wireless technologies.
- Review and evaluate wireless technologies, products, solutions that meet PA requirements.
- Identify approved monitoring mechanisms for wireless devices to ensure compliance with policy.
- Periodically review approved wireless technology standards and procedures to ensure products and solutions remain compliant.
- Support risk management activities associated with evaluating wireless services
- Act as central coordination point and final approval authority for any exceptions to this policy.
- Define or approve acceptable wireless devices, products, services and usage.
- Provide immediate consultation to PA units.

10.1.9 Responsibilities of CTO

Ensure end-to-end protection and interoperability by guiding investments and other actions of the agency.

Adhere to wireless procedures and standards, establish procedure for reviewing and approving requests for using wireless devices to store, process, or transmit information.

Establish procedures for periodically reviewing approved wireless devices and services to ensure that the business requirement for device/service/system is still valid and meet current PA guidance.

Establish procedures for inventory and control of wireless devices and equipment.

Establish procedures and implementation plans for auditing wireless connections to the network.

Provide user training.

10.1.10 Responsibilities of Wireless and Handheld Device Users

Coordinate all requests through Technology Services Department...

Read and follow standards and guidelines.

Access information systems using only approved wireless hardware, software, solutions and connections.

Take appropriate measures to protect information, network access, passwords and equipment.

Use approved password policy and bypass automatic password saving features.

Use extreme caution when accessing PA information in open areas where non-authorized persons may see PA info (airport lounge, hotel lobby).

Protect PA equipment and information from loss or theft at all times, especially when traveling.

Keep current anti-virus software on devices.

Use appropriate Internet behavior (e.g. approved downloads).

Exercise good judgments in efficient cooperative uses of these resources and comply with current and future standards of acceptable use and conduct at all times.

Report any misuse of wireless devices, services or systems to management.

Appendices

Appendix 2 -- Business Resumption Plan{ XE "Business Resumption Plan" } Document Format{ XE "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{ XE "System Backup and 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{ XE "Databases" }
   - Emergency equipment
   - Communications
   - Transportation
   - Supplies
   - Security{ XE "Security" }
   - Operations and procedures manuals

VI. OFFICE/FACILITY BUSINESS SITE RESTORATION PROCEDURES

(Procedures for restoring physical facilities)

- identify restoration responsibilities
- assess damage
- develop restoration plan/time frames

VII. BRP UPDATE PROCEDURES

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

Appendix 3 -- Communication Room{ XE "Communication Room" }s/Closets Standards

SPACE

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

ENVIRONMENTAL

The following conditions must be met:

a) Doorways/Entrances must be designed to support at least the minimum space requirements of 90"Hx72" Wx60" D.

b) The room's cooling capabilities must be sufficient to support the heat dissipation requirements for the equipment. This requirement will be measured in minimum and maximum BTUs powered by AC-powered systems. Equipment specs will be supplied by TSD upon request.

c) Backup UPS{ XE "Uninterrupted Power Supply" } systems are necessary to avoid equipment damage in case of site power failure.

d) Telco demarcs must be located in a central location with sufficient space to house Telco termination equipment.

e) The room should be designed with the appropriate fire safety regulations such as Halon.

f) Cables trays must also be installed in the communications room ceiling where appropriate, to support the routing of data communications and Telco cables.

g) Basic 19" W/72" H cabinets or racks must be installed to house communications equipment such as: routers, switches, hubs, DSUs/CSUs and monitors.

h) To create more wall space the use of wall mount racks can be installed. Appropriate sized plywood must be installed prior to mounting racks.

i) Category 5 cable must be terminated in wall/rack mounted patch panel.

j) Fiber patch panel must be installed in fiber IDF panel with SC female interface.

k) The fiber must be neatly tie wrapped and enclosed in flexible inner-duct.

l) Telephone access must be installed in the appropriate location to provide for basic trouble-shooting and vendor support.

m) All communications equipment and cabinets must have ample room for easy access and proper ventilation.

Appendix 4 -- Cabling{ XE "Telephone Network: Cabling" }{ XE "Cabling" }

a) Teflon-coated cables should be installed per fire code regulations.

b) Overhead cable trays and drop post must be installed for cable routing.

c) Cabling{ XE "Telephone Network: Cabling" }{ XE "Cabling" } scheme must be used to label and identify all cables. All cables must be neatly tie-wrapped.

Appendix 5 -- Port Authority Unified Wiring Plan{ XE "Unified Wiring Plan" }

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

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

LATERAL CABLE:

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

Cable specifications:

(3) Cables capable of supporting Category 5e capabilities as outlined in the TIA/EIA-568-B.2 standard. Specifically:

Gauge: 24 AWG

Pair Size: 4

Insulation: Plenum, fire code rating (FEP)

Cable allocations will be as following:

Cable #1: Voice**

Cable #2: Data

Cable #3: Data

- *100.0MHz is the speed the PA wants to deliver to the desktop.
- **Cable #1 is to be split in the workstation to support 2 telephones.

Technical specs for the Cat 5e cable is as follows.

TECHNICAL DATA--ELECTRICAL				
	Horizontal		Patch	
Frequency	Attenuation dB/100 m	Next dB	Attenuation	Next dB min.

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

TECHNICAL DATA--PHYSICAL			
	CMR	CMP	CM (Patch)*
Conductor diameter-in. (mm)	.020 (0.52)	020 (0.52)	024 (0.61)
Cable diameter-in. (mm)	.195 (5.0)	165 (4.2)	215 (5.5)
Nominal cable weight-lb./kft. (kg/km)	21 (31)	21 (31)	23 (34.2)
Max. installation tension-lb. (N)	25 (110)	25 (110)	25 (110)
Min. bend radius-in. (mm)	1.0 (25.4)	1.0 (25.4)	1.0 (25.4)
* Patch cables utilize stranded tinned copper conductors			

PARAMETRIC MEASUREMENTS		
	Horizontal	Patch
Mutual Capacitance	4.6 nF/100 m nom.	5.6 nF/100 m nom.
DC resistance	9.38 Ohms/100 m Max.	9.09 Ohms/100 m max.
Skew	45 ns/100 m max.	45 ns/100 m max.
Velocity of	72% nom. Non Plenum	72% nom.

Propagation	72% nom. Plenum	
Input Impedance	100 + 15% 0.7772-100 MHz	100 + 15% 0.772-100MHz
	ISO/IEC 11801	

COLOR CODE			**TEMPERATURE RATING**	
Pair 1	White/Blue	Blue	Installation	0 degrees C to +50 degrees C
Pair 2	White/Orange	Orange	Operation	-10 degrees C to +60 degrees C
Pair 3	White/Green	Green		
Pair 4	White/Brown	Brown		

Appendix 6 – Telephone Closet{ XE "Telephone Closets" } / IDF Termination Blocks{ XE "IDF Termination Blocks" }

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

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

Each workstation will be assigned a unique station identification number.

Appendix 7 -- Workstation{ XE "Workstations" } Jacks{ XE "Workstations: Jacks" }{ XE "Jacks" }

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

Appendix 8 -- Standard Switches{ XE "Switches" }{ XE "Port Authority Wide Area Network (PAWANET): Switches and Routers" } Inside the Department

Cisco{ XE "Cisco" } series are acceptable.

Appendix 9 -- Desktop and Lateral Cable Identification Management

WORKSTATION AND LATERAL CABLE IDENTIFICATION/MANAGEMENT (Facility)

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

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

2 - Workstations (3 numeric digits)

The cable identification code for Workstation{ XE "Workstations" } 10 in room 3801 at LGA CTB is 3801-010.

The cable identification code for Workstation{ XE "Workstations" } 15 in PA Automotive shop is Auto-015

THE PORT AUTHORITY OF NY & NJ

Standards & Guidelines

for Port Authority Technology

(for distribution in RFP's)

Technology Services Department

Version 7.1

January 22, 2010

Introduction 5

1.0 The Port Authority Wide Area Network (PAWANET) 5

1.1 PAWANET Overview 5

1.2 PAWANET Circuit Diagram (Note: IGXs are no longer in the network)... 7

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 9

1.8 Approved Servers 9

1.9 Enterprise Addressing Scheme (including IP addressing) 10

1.10 Enterprise Network Monitoring Software 10

2.0 Network Resources 10

2.1 Network Overview 10

2.2 Enterprise Network Architecture 11

2.2.1 Operating System and Software 11

2.2.2 Configuration 12

2.2.3 Network Resources Security 14

2.2.4 Network Access and User Account Security 15

2.2.5 Remote Access System 17

2.2.6 Network Resources Hardware Standards 18

2.3 Network Naming Conventions 18

2.3.1 Server Names 18

2.4 Directory Services and Structure 19

2.5 System Backup and Recovery 19

2.5.1 Backup Logs 19

2.5.2 Backup Scheduling 20

2.6 Business Resumption Plan 20

2.7 Telecommunications Standards for Enterprise Network Resources 20

2.7.1 Closet and Telecommunications Room Access 21

2.7.2 Telecommunications Installation Contractor's Responsibilities 21

2.7.3 Electrical Requirements 22

2.7.4 Telephone Company Interface 22

2.8 Documentation 23

3.0 Virus Scanning & Management **24**
3.1 Overview 24
3.2 Standards 24
3.3 Acquisition and Installation 24
4.0 Electronic Mail **25**
4.1 E-Mail Overview 25
4.2 E-Mail System Architecture 25
4.3 E-Mail Environment: Design Considerations and Infrastructure 25
4.4 Integrating Applications Server with Port Authority Email System 26
4.4.1 Requesting SMTP Services 26
4.4.2 Email Restrictions 26
6.0 Workstation and Workstation Operating System **27**
6.1 Overview 27
6.2 Workstation Operating System Standard 27
6.3 Workstation Configuration 27
6.3.1 Workstation Naming Conventions 27
6.3.2 Workstation User Accounts 27
6.3.3 Remote Workstation Management 27
6.3.4 Drive Mappings 28
6.3.5 Standard Workstation Hardware Configurations 28
6.4 Physical Security 28
6.5 Logical Security 29
7.0 Distributed Systems Environment **30**
7.1 Overview 30
7.2 Microsoft Windows Servers 30
7.3 Unix 30
7.3.1 Unix Security 30
7.3.2 Backup 30
7.4 Databases 30
7.5 Application Security 30
7.6 Server Physical Security 31
8.0 Vendor Provided Dedicated Systems **31**
Overview 31
Appendices **32**

Appendix 1 -- Business Resumption Plan Document Format 32
Appendix 2 -- Communication Rooms/Closets Standards 34
Appendix 3 -- Cabling 35
Appendix 4 -- Port Authority Unified Wiring Plan 35
Appendix 5 -- Telephone Closet / IDF Termination Blocks 37
Appendix 6 -- Workstation Jacks 37
Appendix 7 -- Standard Switches Inside the Department 37
Appendix 8 -- Desktop and Lateral Cable Identification Management 38
Appendix 9 -- PA Telephone Network 5/08 39
Appendix 10 -- Fiber Optic Specification for Network Services - PAWANET 40
Appendix 11 -- Public Telephone Ordering Guidelines 41

Introduction

The purpose of this document is to communicate the standards established by the Technology Services Department (TSD) and provide guidance in proposing IT solutions for the Port Authority of New York & New Jersey (PANYNJ), the Agency.

To that end, these guidelines are intended 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 current and mandated business needs and enables departments to work with other departments/offices more effectively.

Easily and efficiently communicate and exchange information throughout the agency.

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

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

1.0 The Port Authority Wide Area Network{ XE "Wide Area Network" }{ XE "Networks" } (PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" })

1.1 PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } Overview

The Port Authority has a modern distributed computing network, called the Port Authority Wide Area Network{ XE "Wide Area Network" }{ XE "Networks" } (PAWANET{ XE "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.

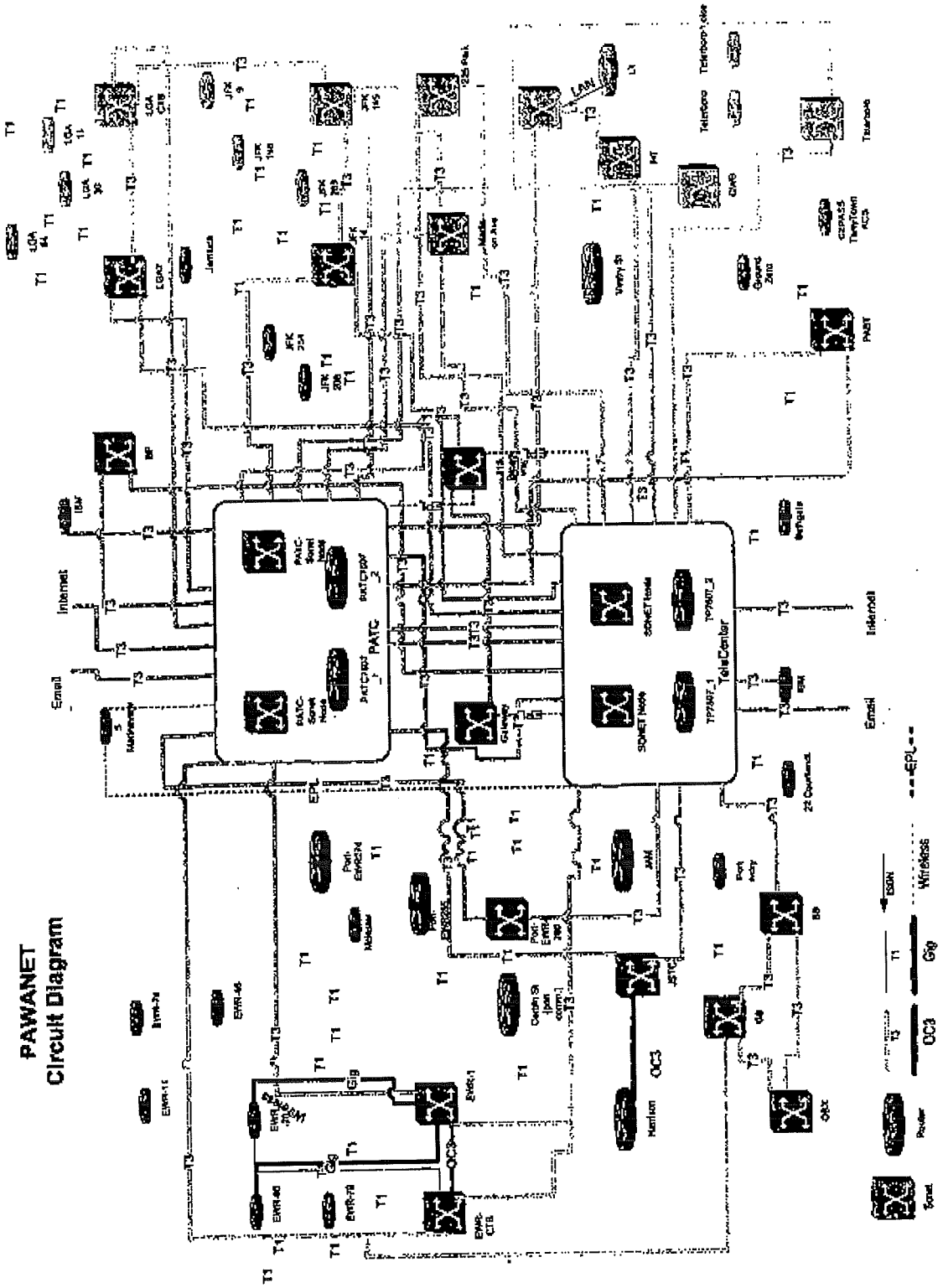
This network is crucial to all Port Authority businesses because it provides the connections for applications such as e-Mail, Internet and Intranet{ XE "Intranet" } access, SAP{ XE "SAP" }, PeopleSoft{ XE "PeopleSoft" }, Electronic Toll Collection, CADD, Lease Image, Closed Circuit Television (CCTV{ XE "Closed Circuit TV" }) surveillance systems, and in the future, videoconferencing, and more.

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

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

The network consists of state-of-the-art Cisco{ XE "Cisco" } Systems equipment and services, such as, high performance Cisco Catalyst switches and routers. The Port Authority use Cisco Systems SMARTnet hardware/software maintenance services, and Cisco's Technical Assistance Center (TAC) to support and maintain the network.

1.2 PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } Circuit{ XE "Networks" } Diagram (Note: IGXs are no longer in the network){ XE "Port Authority Wide Area Network (PAWANET): Diagram" }



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

1.3 Inter-site Services Providers

The Technology Services Department (TSD) has contracted with a variety of companies to provide inter-site services Companies providing communications services for the Wide Area Network{ XE "Networks" } are listed below.

- AT&T{ XE "AT&T" } Local Service{ XE "Local Service" }s
- Verizon{ XE "Verizon" }

1.4 PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } Functions{ XE "Port Authority Wide Area Network (PAWANET): Functions" }

Currently PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } provides the following functions:

Data	Supports the low and high volume transfer of data used for applications, such as SAP{ XE "SAP" } and PeopleSoft{ XE "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 Attached Network{ XE "Networks" } (SAN){ XE "SANs" } for network storage of user files and routing jobs to shared network printers.
CCTV{ XE "Closed Circuit TV" }	The transfer of Closed Circuit TV{ XE "Closed Circuit TV" } (CCTV) data is supported across the entire network to provide security for the Port Authority's key facilities.
Voice	The network provides the hardware capabilities for voice transmission for future implementation.
Videoconferencing { XE "Videoconferencing" }	The network switches and transmission lines are capable of handling videoconferencing to support the agency's future needs.

1.5 Features of PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" }

PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } provides a high performance and reliable fail-safe communications network. These are its key features:

- Alternate paths of communication
- Support of high volume traffic such as CADD, CCTV{ XE "Closed Circuit TV" } and others
- Catalyst 3000, 4000 and 6500 switches at all the major sites, and at the Teleport.
- Cisco{ XE "Cisco" } high performance 2000, 7200 and 7507 router family products with redundant power supplies.

1.6 Supported Protocols{ XE "Port Authority Wide Area Network (PAWANET): Supported Protocols" }{ XE

"Protocols" }{ XE "Port Authority Wide Area Network (PAWANET): Protocols" }

The network supports the following network protocols, allowing dissimilar platforms to communicate within PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" }:

TCP/IP:{ XE "IP Addresses" }{ XE "TCP/IP" }	TCP/IP{ XE "TCP/IP" }{ XE "IP Addresses" } is the universal protocol that allows communications between all systems within the Port Authority's network, as well as other networks.
IPX/SPX:{ XE "IPX/SPX" }	This protocol allows communications between all Novell platforms.
SNA/SDLC:{ XE "SNA/SDLC" }	This protocol allows communications between all IBM systems and other systems that support SNA.

1.7 PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } Switches{ XE "Switches" }{ XE "Port Authority Wide Area Network (PAWANET): Switches and Routers" } and Routers{ XE "Routers" }

The current standard switches and routers used on PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } are:

- Dual SONET OC48 Rings that connects key Port Authority facilities and data centers.
- Cisco{ XE "Cisco" } 7200 high performance routers
  Provide high-speed connectivity and routing capabilities across the ATM{ XE "Port Authority Wide Area Network (PAWANET): ATM Node Assignments" }{ XE "ATMs" } network in support of TCP/IP{ XE "TCP/IP" }{ XE "IP Addresses" }, IPX/SPX{ XE "IPX/SPX" } and bridging functions and provides routing capabilities for Port Authority Internet access.
- Cisco{ XE "Cisco" } 7500 series high-capacity redundant routers
  Serve as the -network backbone core router that provides high speed routing functions between the, Teleport, Port Authority Technical Center and all PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } connected facilities as well as the IBM mainframe. Also provide high-speed connection and routing capabilities to the disaster site for data recovery in the event of a catastrophe.
- Cisco{ XE "Cisco" } 2000 series medium capacity routers
  Provide high-speed connectivity and routing capabilities to the Port Authority's remote locations.

1.8 Approved Servers

IBM File/ Print/Application and NEC Express 5800 series servers may be connected to PAWANET. The use of Vmware's ESXi virtual infrastructure is also an approved

configuration, Specialized servers (e.g., appliances) to support a specific line department application will be reviewed on a 'case-by-case' basis.

Replacement server must conform to the category listed above. Deviation from this policy will not be allowed without prior approval of the Chief Technology Officer or her/his designee.

1.9 Enterprise Addressing Scheme{ XE "IP Addresses" } (including IP addressing)

The Port Authority's Enterprise network is a TCP/IP{ XE "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{ XE "IP Addresses" } addresses via Dynamic Host Configuration Protocol{ XE "Protocols" } (DHCP).

1.10 Enterprise Network{ XE "Networks: Enterprise Network" }{ XE "Networks" } Monitoring Software{ XE "Port Authority Wide Area Network (PAWANET): Network Monitoring Software" }{ XE "Networks: Monitoring Software" }

The Port Authority continually monitors its WAN{ XE "Wide Area Network" } and the availability of its links. To provide for real time monitoring, the following software utilities are used:

- HP Open View Network{ XE "Networks" } Management{ XE "HP Open View Network Management" } software
- Cisco{ XE "Cisco" } Works{ XE "Cisco Works" } for Switched Internetworks

2.0 Network Resources{ XE "Networks" }

2.1 Network{ XE "Networks" } Overview

The Port Authority has a modern distributed computing network, which is managed as an Enterprise resource. The network connects all individual PCs{ XE "Workstations" }, 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{ XE "Networks: Enterprise Network" } consists of the PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } (see Section 1.1) and connected Local Area Networks (LAN's). The line of demarcation between the cable and wiring which is the responsibility of the carrier and the Port Authority's area of responsibility is usually a wiring closet. The Port Authority's Enterprise Network{ XE "Networks" } consists of the following components on the Port Authority side of demarcation:

- Enterprise Devices
    - Cabling{ XE "Telephone Network: Cabling" }{ XE "Cabling" }

- Routers{ XE "Routers" }{ XE "Port Authority Wide Area Network (PAWANET): Switches and Routers" }
- Switches{ XE "Switches" }{ XE "Port Authority Wide Area Network (PAWANET): Switches and Routers" }
- Wiring Closets{ XE "Wiring Closets" }
- Communications Equipment Racks
- Server{ XE "Servers" } Racks{ XE "Servers: Racks" }
- File and Pint Servers{ XE "Servers" }
- Application Servers{ XE "Servers: Application" }{ XE "Servers" }
- Storage Area Networks{ XE "SANs" } (SAN)
- Network{ XE "Networks" } Printers{ XE "Printers" }

- LAN Devices{ XE "LAN Devices" }
  - Desktop PCs{ XE "Workstations" }
  - Workstations
  - Laptops{ XE "Laptops" }
  - Local Printers{ XE "Printers" }
  - Scanners{ XE "Scanners" }
  - Copiers
  - PC Peripherals

2.2 Enterprise Network{ XE "Networks: Enterprise Network" }{ XE "Networks" } 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{ XE "Wide Area Network" }{ XE "Networks" }. The flexibility provided by the use of multiple servers, server clusters and Storage Area Networks{ XE "SANs" } (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 Operating System{ XE "Operating Systems" } and Software

All Enterprise File & Print services in the Port Authority are currently based on the Novell Netware{ XE "Netware" } 6.5 operating system (the agency will be migrating to Microsoft networking services during Y2010). Microsoft Windows 2003 and 2008 servers (Standard and Enterprise) are the primary operating system in use. Sun Solaris{ XE "Sun Solaris" } is also supported as application servers and only when required for functionality.

In addition to the base operating system, all servers must include the following components:

- Virus Protection (minimum: McAfee Engine 8.5.0i, with current DAT files){ XE "Virus: Protection" }
- Network{ XE "Networks" } Security{ XE "Networks: Security" }{ XE "Security" }
- Remote Monitoring and Management
- Intrusion Detection{ XE "Intruder Detection" }
- Systems Backup (minimum: Upstream 3.5.0c)
- Uninterrupted Power Supply{ XE "Uninterrupted Power Supply" } (If central UPS is not installed at the location)
- Current Service Packs and security patches (minimum: SP1)

Note: All operating system and server software will be provided by the Technology Services Department.

2.2.2 Configuration

All network devices--including servers, workstations, network printers, and network faxes--must use IP{ XE "IP Addresses" } addresses which conform to the standards outlined in sections, 1.9 *Enterprise Addressing Scheme*, and 2.3.1, *Server{ XE* "Servers" *} Names{ XE* "Servers: Names" *}*. All servers will be configured using the following parameters:

Base Configuration:

- C: (OS Drive) Minimum 25 GB
- D: (Application Drive) Minimum Based on Application's space requirements
- IP Protocol

2.2.2.1 Drive Mapping{ XE "Workstations: Drive Mapping" }{ XE "Drive Mappings" } Conventions and Organization

Mapping of workstation drive pointers to SAN{ XE "SANs" } or server disk volumes or folders is currently accomplished through a Novell NetWare Login{ XE "Logins" } Script or the Microsoft equivalent. The following drive letters are reserved for Novell installations:

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

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

- Public (Shared) application software installed on file and print servers{ XE "Servers" }, or server cluster must reside on a separate volume named "APPS".

  Example: P:\APPS

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

  Examples: P:\APPS\EXCEL

  P\APPS\LOTUS

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

  Example <Server{ XE "Servers" } _name>:\DATA\SHARE on a single server

  <Cluster_name>:\DATA\<Department_NAME>\SHARE on a server cluster

- Each Department's SHARE folder will contain at least three sub-folders titled Org, Everyone and Projects.
- The Projects folder is provided for storage of project related files. All departmental projects will be kept in a sub-folder under the Projects folder and the folder will be named using the same name as the project. User rights will be assigned by a group having the same name as the project folder. Only colleagues requiring access to the project files should be granted rights to that project folder.
- Under the Projects folder will be two additional folders, one called "Active" and one called "Completed". Active projects reside in the "Active" folder.
- When staff identify a project as being completed, the project folder will be moved to the "Completed" folder and all rights, except for "Read" and "FileScan" will be removed from the folder. This will ensure that the final project documents remain unchanged, while still allowing authorized staff to review the old documents and use them as templates for new documents if desired. The "Completed" folder will be set to archive its data.
- Under the "ORG" folder will be subfolders with names corresponding to the various divisions within the department. By default, only staff within a division will have access to a division's folder. These folders are intended to hold data for a specific division that would not normally be shared departmentally. Staff from other divisions would not have access to these folders unless the division manager of the owning division gives their approval. Having folders setup by divisions will simplify the process of identifying who is responsible for the contents of a folder.
- The "S" and "U" drives should only be used to store business related files.

- The Systems Administrator, at the direction of the Director, may from time to time remove any data deemed to be non-business related.
- A folder called "Everyone" will be created in the Share folder. All staff in the department will have full access to this folder to store and retrieve files that are not related to a project or a division's day-to-day operations.
- Additional shared folders, with access restricted to only specific users, if required, will be created in the Share folder. Access will be restricted through the use of Inherited Rights 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 an internal workflow approval process.
- A user "U" drive will be assigned to each standard network account for use by each individual user to store business related data on the network. Access to the "U" drive is restricted to the account owner only. Users receive all rights to this folder except for "Access Control" and "Supervisory". Users cannot share data on their "U" drive. Files should be shared only by using the Share, ("S") drive.
- Access to a user's home directory, by anyone other than the owning user is prohibited and will be removed after notifying the end-user.
- Installation files used in the installation of desktop software must reside in a sub-folder under the "APPS" volume

  Example P:\APPS\Psoft

2.2.2.2 Connecting LAN Devices{ XE "Networks: Connecting LAN Devices" }{ XE "LAN Devices" } to the Enterprise Network{ XE "Networks: Enterprise Network" }{ XE "Networks" }

The Technology Services Department (TSD) is responsible for connecting all LAN devices to the Enterprise Network{ XE "Networks: Enterprise Network" }{ XE "Networks" } (PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" }) provided they meet the Port Authority's standards.

2.2.3 Network Resources{ XE "Networks" } Security{ XE "Security" }

2.2.3.1 Server{ XE "Servers" } Physical Security{ XE "Servers: Physical Security" }{ XE "Workstations: Security" }{ XE "Security: Physical Security" }{ XE "Security" }

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

2.2.3.2 Server{ XE "Servers" } Logical Security{ XE "Servers: Logical Security" }{ XE "Security" }

To safeguard the Port Authority's Information Technology (IT) systems and data, TSD has implemented a number of processes and procedures, including the requirement that all users accessing the Port Authority's networks authenticate to a Directory Service (using either Novell Netware e-Directory or Microsoft Active Directory (AD). Both Directory Services contain descriptions of all network devices including servers, printers, shared drives and user accounts.

TSD is responsible for providing all Enterprise servers with the following protection of their logical resources:

- Guard against unauthorized access by making sure that servers cannot be booted from a floppy.
- Scan all workstations for viruses daily.
- Scan all laptops for viruses at log-in.
- Scan all incoming data from users, server peripherals, diskette, CD-ROM, tape drives, other servers, and the Internet for viruses
- Perform regularly (daily and/or weekly) backups as defined by the Technology Services Department. (see section 2.5 - System Backup and Recovery)
- Test recovery procedures annually.
- Use system and application passwords that conform to the Technology Services Department standards.
- Configurations must conform to security parameters identified by NetVision Suite software.
- Perform deleted file purges immediately or no later than 6 days after file deletion.
- Control all remote access using the Port Authority's Remote Access{ XE "Email: Remote Access" } System.

2.2.4 Network{ XE "Networks" } Access{ XE "Networks: Access" } and User Account{ XE "User Accounts" } Security{ XE "User Accounts: Security" }{ XE "Security" }

2.2.4.1 Account Creation{ XE "User Accounts: Creation" }

User and Application accounts are unique and provisioned and managed in our Directory Service for both the Novell and Windows{ XE "Windows NT" } network resources. Documentation for the creation of user accounts and authority for access is maintained by the System Administrator{ XE "System Management" }{ XE "Administrator□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□" }.

2.2.4.2 Time Restrictions{ XE "Time Restrictions" }

Due to the fact that The Port Authority serves its clients 24 hours a day, we do not have Login Time Restrictions on network resources. All staff may access their Novell account 24 X 7{ XE "System Management" }{ XE "Administrator□ □□□" }.

2.2.4.3 Concurrent Logins{ XE "Logins: Concurrent" }{ XE "Networks: Logins" }{ XE "Logins" }

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

2.2.4.4 Intruder Detection{ XE "Networks: Intruder Detection" }{ XE "Intruder Detection" }

These system-monitoring features must be active:

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

2.2.4.5 Passwords{ XE "Passwords" }

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

- Minimum length is six (6) characters.
- Should not be easily guessed. It should not be related to one's job and should not be a word in the dictionary or a proper name.
- Should be set to expire at least every 90 days and 30 days for accounts with system or application administrator access.
- Grace Logins should be activated and limited to three.
- Users should be notified several days in advance of password expiration.
- Users should be forced to change their password on initial login and once it expires.
- Unique passwords should be required when changed. Users should be prevented from reusing a previous password for a minimum of one-year.
- Users should not be permitted to change their passwords more than once a day.
- Passwords{ XE "Passwords" } should be encrypted in storage.
- Passwords{ XE "Passwords" } must be entered in a non-display field with a re-enter verify function for new passwords.
- Passwords{ XE "Passwords" } must not be available on hard copy.

- Passwords{ XE "Passwords" } used in system startup files and login scripts must be encrypted.
- If an application uses a default password, change it on installation.
- Do not use cyclical passwords, such as the word, February, during the month of February.
- Do not reveal your password to anyone except authorized persons.
- Use both upper and lower case characters and special characters where possible.
- Change password if it has been disclosed or compromised.
- Protect by using a screen saver password with a recommended 15-minute time-out period.
- Passwords{ XE "Passwords" } should not be the same as the user ID

Passwords{ XE "Passwords" } are considered confidential data. They protect the Port Authority's network resources and grant system privileges and access. Disclosure may result in unauthorized access to data, system files and transactions. Passwords are also your signature and identify you as the individual who is responsible for the system activity.

2.2.4.6 Modems{ XE "Modems" }

Staff are prohibited from connecting dial-up modems to workstations that are simultaneously connected to PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" } or another internal communication network unless approved by the Technology Services Department (TSD).

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

2.2.5 Remote Access{ XE "Email: 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 Services Department (TSD).

The approved mechanism for remote access to the Port Authority network is through the Remote Access{ XE "Email: Remote Access" } System (RAS). The Remote Access System utilizes an Internet-based Virtual Private Network{ XE "Networks" } (VPN) tunnel established over the Internet linking remote users to the Port Authority Wide Area Network{ XE "Wide Area Network" } (PAWANET{ XE "Port Authority Wide Area Network (PAWANET)" }) (remote client to PA site). It is designed to provide authorized Port Authority users with secure access to corporate applications and to files available on their departmental file servers. This access to applications and resources is delivered through a thin-client environment consisting of a farm of Citrix MetaFrame/Microsoft Terminal Services servers capable of supporting 200 or more simultaneous users each. There is no provided access to the user's office PC desktop. The system also provides access to IBM enterprise server ("mainframe") applications. Port Authority offices without direct connection to the Port Authority Wide Area Network (PAWANET) can use this system to establish remote access to corporate applications located on PAWANET.

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

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

2.2.6 Network Resources{ XE "Networks" } Hardware Standards

2.2.6.1 Standard Servers{ XE "Servers: Standard Hardware" }{ XE "Servers" }

A representative sample of standard servers is as follows:

PORT AUTHORITY SERVER STANDARDS

Server Description	IBM Model
WEB Server, Small applications server	xSeries 3550M2
Medium applications server	xSeries 3650M2
Database Server, Multiple and Large application server	xSeries 3850M2

Each server shall have at least 3 network interface ports to support a production, management and backup network, and redundant power supplies.

The Port Authority manages servers models via a lifecycle process with a minimum 'in service' life of three (3) years.

2.3 Network{ XE "Networks" } Naming Conventions{ XE "Networks: Naming Conventions" }{ XE "Naming Conventions" }

2.3.1 Server{ XE "Servers" } Names{ XE "Servers: Names" }

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

Static IP addresses for servers, printers and faxes will be assigned by Technology Services Department (TSD).

2.4 Directory Services and Structure

The Port Authority uses Novell e-Directory and Microsoft 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 as e-Directory objects. NDPS should be utilized.

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

2.5 System Backup and Recovery{ XE "System Backup and Recovery" }

The Port Authority, for distributed servers, has standardized on FDR Upstream software for data backups.

- The System Administrator{ XE "System Management" }{ XE "Administrator" } is responsible for verifying that system backups, both local and remote can be used to restore the data. Tests of the ability to successfully restore from the backup system will be performed annually. It is recommended that the test data restore be performed on a single non-critical directory only, not the entire server. Tests of the ability to restore system and application files will be performed on a non-production server in a controlled environment. When incremental or differential backups are routinely used, the test restore procedure should incorporate both.
- Immediately prior to performing the test restore procedure, do a special full backup on the directories being tested.
- Testing a full restore should only be performed on a non-production server.

Depending on the criticality of the data and the redundancy needs, other products are in use within the Port Authority. Double-Take software is used for 'file-level' copies across distributed servers. IBM's SAN-to-SAN replication (block level copy) for database protection.

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

2.5.1 Backup Logs { XE "System Backup and Recovery: Logs" }

The System Administrator{ XE "System Management" }{ XE "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{ XE "System Backup and Recovery: Scheduling" }

The System Administrator{ XE "System Management" }{ XE "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.
- Store daily and weekly back-up media in a locked fire proof cabinet outside of the server room. Monthly media must be stored outside the immediate building at a location defined by the Port Authority.

2.6 Business Resumption Plan{ XE "Business Resumption Plan" }

The Vendors will work with the Technology Services Department (TSD) to develop a disaster recovery and contingency plan. The System Administrator{ XE "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{ XE "Business Resumption Plan" } will be reviewed quarterly and tested at least annually.

2.7 Telecommunications Standards{ XE "Telecommunications: Standards" } for Enterprise Network{ XE "Networks: Enterprise Network" } Resources{ XE "Networks" }

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

Appendix 2 -- Standards for Setting up Closets & Communication Room{ XE "Communication Room" }s

Appendix 3 -- Standard Cabling{ XE "Telephone Network: Cabling" }{ XE "Cabling" } Schemes

Appendix 4 -- Unified Wiring Specifications

Appendix 5 -- Telephone Closet{ XE "Telephone Closets" } / IDF Termination Blocks{ XE "IDF Termination Blocks" }

Appendix 6 -- Workstation{ XE "Workstations" } Jacks{ XE "Workstations: Jacks" }{ XE "Jacks" }

Appendix 7 -- Standard Switches{ XE "Switches" }{ XE "Port Authority Wide Area Network (PAWANET): Switches and Routers" }

Appendix 8 -- Workstation{ XE "Workstations" } and Lateral Cable Identification Management

Appendix 9 - Fiber Optics Specifications for Network Services - PAWANET

2.7.1 Closet and Telecommunications Room{ XE "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{ XE "Networks" } 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 Administrator{ XE "System Management" }s requiring routine maintenance of data communications equipment should call the Customer Support Desk when new devices or reconfigurations are required{ XE "Support Desk" }.

2.7.2 Telecommunications Installation Contractor's Responsibilities

1. Adherence to all of the above specifications.
2. Assurance of labor harmony by providing installation technicians whom currently maintains appropriate union membership.
3. The contractor must supply all cable, blocks, brackets, connectors, jacks, housings, face plates, special tools, etc., as necessary to perform an installation which is satisfactory to the Port Authority.
4. The contractor must label every workstation (jack faceplate) and the corresponding cross connect point (punch down block or patch panel) in accordance with the cable identification management plan, as previously described.
5. Install all Category 5e cabling in the proper manner, with the appropriate number of twists, so as to maintain Category 5e integrity and capabilities, as outlined in the TIA/EIA 568-B.2 standard.

6. The contractor must ensure that cable connections are in accordance with standard telecommunications practices and that all cabling maintains normal connectivity and continuity.
7. All materials must be agreed upon by PA Network{ XE "Networks" } 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 TSD staff and an agreed upon member of the site where the PAWANET{ XE "Port Authority Wide Area Network (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{ XE "Telecommunications: Electrical Requirements" }{ XE "Electrical Requirements: Telecommunications" }

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 208/220 volt power receptacles
- Dedicated circuit breaker per AC feed, with alternate power source.
- Server{ XE "Servers" } 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{ XE "Uninterrupted Power Supply" } included in the delivered service if central UPS is not installed at the equipment location.

2.7.4 Telephone Company Interface{ XE "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{ XE "Networks" } Termination Unit (Rj48 interface) Smartjacks
- Network{ XE "Networks" } Termination Unit (DB15-pin female interface)
- Network{ XE "Networks" } 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{ XE "System Management" }{ XE "Administrator□□" } to establish and maintain a library of all documentation designated as standard by the Port Authority. These include archived system files and system backups. Vendors will be provided our "Guide to Systems Administration" during the implementation phase of a project. The "Guide to Systems Administration" covers the provisioning and setup of computing & networking resources to successfully implement a project within the Port Authority.

3.0 Virus Scanning{ XE "Virus: Scanning" } & Management

3.1 Overview

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

3.2 Standards

Standard virus protection software must be installed on all network servers and personal computers, and updated on a regular basis. To that end, the Technology Services Department (TSD) has designated McAfee VirusScan Enterprise + AntiSpyware Enterprise 8.5.0*i* (at the time of this writing) as the standard for virus management on both Windows desktops and servers.

3.3 Acquisition and Installation

The Technology Services Department (TSD) 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.

4.0 Electronic Mail{ XE "Email" }

4.1 E-Mail{ XE "Email" } Overview

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

4.2 E-Mail{ XE "Email" } System Architecture

The Port Authority's E-Mail system is hosted by AT&T Corp. who acquired USinternetworking, a managed application service provider, and consists of Microsoft Exchange servers connected to the Port Authority's enterprise network. Authorized Port Authority staff access their corporate e-mail through Microsoft Outlook desktop software on the network. The system has multiple Exchange servers containing mailboxes and Public Folder{ XE "Public Folder" }s{ XE "Public Folders" }{ XE "Email: Public Folders" }. Additional servers host Outlook Web Access, Blackberry services, and perform Internet-based e-mail services including anti-spam and anti-virus e-mail checking.

The hosted Exchange site is on a Windows { XE "Windows NT" } resource domain with a one-way trust to the Port Authority's corporate user account Windows domain located on the Port Authority network. This Port Authority Windows domain is used for Windows authentication services when the Outlook client is opened. In addition, the Port Authority hosts DNS servers to satisfy requests from the Outlook client as needed.

High-speed, secure, and redundant network connections connect the AT&T's data center and network to the Port Authority network.

4.3 E-Mail{ XE "Email" } Environment: Design Considerations and Infrastructure

The E-mail environment is further described below:

- The E-Mail{ XE "Email" } system is comprised of Microsoft Outlook 2007 desktop software accessing e-mail (via MAPI{ XE "MAPI" } mail protocol) stored on several Microsoft Exchange 2007 servers
- The servers are currently configured for the following messaging protocols:
  - MAPI{ XE "MAPI" } (Microsoft's Messaging Mail protocol)
  - Internally for X.400 mail protocol (which Exchange servers use)
- IMAP4 and POP3 mail protocols, NNTP news protocol, and LDAP directory protocol are disabled.
- RIM's Blackberry Enterprise Server{ XE "Servers" } software for Exchange provides wireless e-mail and calendar access to Blackberry wireless handheld device users.
- The two supported forms of SMTP addresses are:
  - Primary form: Flastname@panynj.gov
    FLastname where F is the first initial of the user's first name and Lastname is the

last name, and FLastname conforms to the corporate standards for a unique Novell user's username (also known as Novell ID). Flastname is also used as the Alias for a user in the Global Address List. Note that an earlier format with truncating the above to a maximum of eight characters is still in use for accounts created prior to Sept. 2001 (example: Flastnam@panynj.gov).

  - Secondary form: Firstname.Lastname@panynj.gov

- Exceptions are governed by Novell directory structure and user account requirements.

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 Services Department

If the server is Windows-based and has an antivirus program installed, its settings will need to be changed if port 25 is blocked.

4.4.2 Email Restrictions

The following restrictions are in place to protect the SMTP system and the "credibility" of Agency mail servers on the Net:

- 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 30. This includes "To", "cc", and "bcc"; maximum size with attachments is 5MB. 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.

6.0 Workstation{ XE "Workstations" } and Workstation Operating System{ XE "Operating Systems" }

6.1 Overview

The Port Authority makes extensive use of workstations networked into an Enterprise Wide Area Network{ XE "Wide Area Network" }{ XE "Networks" } to accomplish its business objectives. In order to ensure compatibility with the agency's Enterprise network and to make optimal use of its resources, this section defines the standards governing workstations and their configuration and use.

6.2 Workstation{ XE "Workstations" } Operating System{ XE "Operating Systems" } Standard

The Port Authority's standard operating systems for workstations is Microsoft's Windows XP Professional (32-bit), Service Pack 2.

In limited circumstances, where business objectives warrant, alternative operating systems may be deployed with the approval of the department director and concurrence with the Chief Technology Officer.

6.3 Workstation{ XE "Workstations" } Configuration

6.3.1 Workstation{ XE "Workstations" } Naming Conventions{ XE "Workstations: Naming Conventions" }{ XE "Naming Conventions" }

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

Example: Workstation{ XE "Workstations" } name: 23AAH86

System Administrator{ XE "System Management" }s are responsible for naming workstations and maintaining an up-to-date inventory of equipment and names used.

6.3.2 Workstation{ XE "Workstations" } User Accounts{ XE "Workstations: User Accounts" }{ XE "Workstation: User Accounts" }{ XE "User Accounts" }

Windows workstations must have user accounts that correspond to the user's network user identification.

6.3.3 Remote Workstation{ XE "Workstations" } Management{ XE "Workstations: Remote Access" }{ XE "Remote Access" }

The Port Authority also distributes software applications and upgrades via Novell's ZENworks. Each workstation should have Novell's Workstation{ XE "Workstations" }

Management module installed as part of the NetWare workstation client. This will enable remote distribution and updates of software, hardware inventory and workstation troubleshooting.

6.3.4 Drive Mapping{ XE "Workstations: Drive Mapping" }s{ XE "Drive Mappings" }

Drive mappings for workstations should be accomplished only through a Novell login script and should conform to the standard outlined.

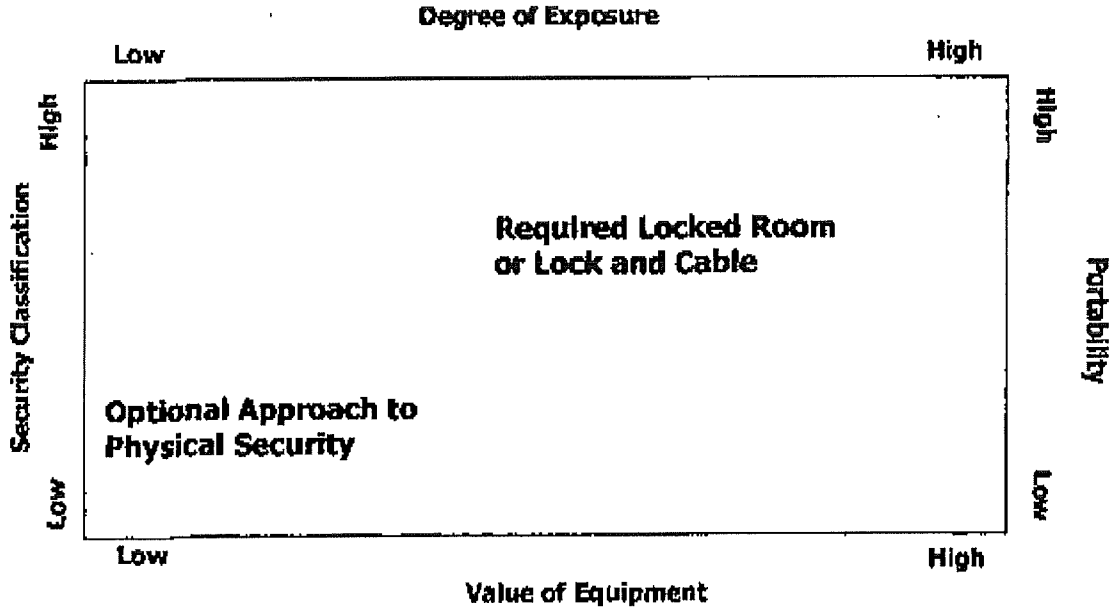
6.3.5 Standard Workstation{ XE "Workstations" } Hardware Configuration{ XE "Workstations: Hardware Configuration" }{ XE "Hardware Configuration: Workstations" }s

There are standard configurations established for workstations and laptops. The current configurations are managed via a 'lifecycle' process within the Technology Services Department (TSD).

6.4 Physical Security{ XE "Workstations: Security" }{ XE "Security: Physical Security" }{ XE "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).

6.5 Logical Security{ XE "Security" }

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

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

7.0 Distributed Systems Environment

7.1 Overview

A number of department and enterprise servers provide critical application and system services. This section provides information on the standards and guidelines for supported systems within the Port Authority. Solutions requiring different operating system environments must have approval from the Chief Technology Officer.

7.2 Microsoft Windows Server{ XE "Windows Server" }s{ XE "Servers" }

Microsoft Windows 2003 & 2008 Server (Standard and Enterprise) are supported Operating Systems for application servers.

7.3 Unix{ XE "Unix" }

Sun's Solaris{ XE "Sun Solaris" } is a supported UNIX operating system for infrastructure (e.g., SMTP services) and corporate servers (e.g., SAP, Peoplesoft). Red Hat Linux may also be supported, via exception and approval by the Chief Technology Officer.

7.3.1 Unix{ XE "Unix" } Security{ XE "Unix: Logical Security" }{ XE "Security" }

Unix{ XE "Unix" } servers must be physically and logically secured from unauthorized access. Operating system logical security is defined by the Technology Services Department (TSD.

7.3.2 Backup

Critical system backup must be performed regularly (daily and/or weekly) utilizing our centralized backup strategy and associated tools as defined by the Technology Services Department. (see prior section on backup software standards)

7.4 Databases{ XE "Databases" }

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

7.5 Application Security{ XE "Security: Applications" }{ XE "Security" }

Depending on the application, security may be administered at the application, database, module, screen, data field, and/or transaction level in addition to network authentication. Prior to implementation, the Business System Manager{ XE "System

Management" } should review the capabilities of the application and consult with Technology Services Department (TSD) staff to ensure implementation of the appropriate security levels. When in production, the administrator responsible for day-to-day administration of the application (Application Administrator{ XE "Administrator□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□" }) is responsible for maintaining the selected security profiles. At a minimum, all applications must require authentication to Microsoft Active Directory by way of a network login.

7.6 Server{ XE "Servers" } Physical Security{ XE "Servers: Physical Security" }{ XE "Workstations: Security" }{ XE "Security: Physical Security" }{ XE "Security" }

All servers and communication equipment must be located in the Port Authority's centralized data centers. On occasion, and with Chief Technology Officer approval, local (e.g., in facility) computing resources may be required. For those occasions, servers must be located in an environmentally controlled, and locked rooms or secured with a cable and lock with the keyboard secured to prevent tampering and unauthorized usage. Technology Services Department (TSD) staff must be consulted during the implementation phase of a project.

8.0 Vendor Provided Dedicated Systems

Overview

Vendor provided dedicated systems refers to the Information Technology software, hardware and infrastructure furnished and installed through a contract with an external provider. Generally, this refers to systems that are designed to support a large Capital Project, 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

A representative from the Technology Services Department (TSD) provides a single point of contact for technology oversight, accountability, adhering to Standards and systems integration, which is required under the Roles and Responsibilities of the Chief Technology Officer (CTO) and is expected by our client departments.

To ensure a successful project, and honor our responsibility to our customers and the Port Authority, one of the steps undertaken by TSD, is to provide guidance with, and focus attention on, adherence to and compliance with our Technology Standards and Guidelines (as described in this document). Deployment, integration and testing will be monitored by TSD to ensure that equipment or infrastructure is not duplicated, that the integration and migration plan will not adversely impact existing systems, and to integrate new systems under existing maintenance contracts where applicable.

In cases where a specific vendor or system is so specialized that it normally does not adhere to the hardware, software, infrastructure and operations guidelines of this document, the vendor will be directed to work with TSD in exploring all options, and if an exception is deemed required, the vendor will work with TSD to prepare the necessary Business Case to receive written concurrence from the Chief Technology Officer for this deviation from the Port Authority Technology standards.

Appendices

Appendix 1 -- Business Resumption Plan{ XE "Business Resumption Plan" } Document Format{ XE "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{ XE "System Backup and 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{ XE "Databases" }

Emergency equipment

Communications

Transportation

Supplies

Security{ XE "Security" }

Operations and procedures manuals

VI. OFFICE/FACILITY BUSINESS SITE RESTORATION PROCEDURES

(Procedures for restoring physical facilities)

identify restoration responsibilities

assess damage

develop restoration plan/time frames

VII. BRP UPDATE PROCEDURES

responsibility for updating and communicating BRP changes

frequency of review/update

Appendix 2 -- Communication Room{ XE "Communication Room" }s/Closets Standards

SPACE

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

ENVIRONMENTAL

The following conditions must be met:

a) Doorways/Entrances must be designed to support at least the minimum space requirements of 90"Hx72" Wx60" D.

b) The room's cooling capabilities must be sufficient to support the heat dissipation requirements for the equipment. This requirement will be measured in minimum and maximum BTUs powered by AC-powered systems. Equipment specs will be supplied by TSD upon request.

c) Backup UPS{ XE "Uninterrupted Power Supply" } systems are necessary to avoid equipment damage in case of site power failure. Vendors must consult with the Technology Services Department (TSD) for the approved UPS systems.

d) Telco demarcs must be located in a central location with sufficient space to house Telco termination equipment.

e) The room should be designed with the appropriate fire safety regulations such as a FM200.

f) Cables trays must also be installed in the communications room ceiling where appropriate, to support the routing of data communications and Telco cables.

g) Basic 19" W/72" H cabinets or racks must be installed to house communications equipment such as: routers, switches, hubs, DSUs/CSUs and monitors.

h) To create more wall space the use of wall mount racks can be installed. Appropriate sized plywood must be installed prior to mounting racks.

i) Category 5e cable must be terminated in wall/rack mounted patch panel.

j) Fiber patch panel must be installed in fiber IDF panel with SC female interface.

k) The fiber must be neatly tie wrapped and enclosed in flexible inner-duct.

l) Telephone access must be installed in the appropriate location to provide for basic trouble-shooting and vendor support.

m) All communications equipment and cabinets must have ample room for easy access and proper ventilation.

Appendix 3 -- Cabling{ XE "Telephone Network: Cabling" }{ XE "Cabling" }

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{ XE "Telephone Network: Cabling" }{ XE "Cabling" } scheme must be used to label and identify all cables. All cables must be neatly tie-wrapped.

Appendix 4 -- Port Authority Unified Wiring Plan{ XE "Unified Wiring Plan" }

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

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

LATERAL CABLE:

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

Cable specifications:

(3) Cables capable of supporting Category 5e capabilities as outlined in the TIA/EIA-568-B.2 standard. Specifically:

Gauge: 24 AWG

Pair Size: 4

Insulation: Plenum, fire code rating (FEP)

Cable allocations will be as following:

Cable #1: Voice**

Cable #2: Data

Cable #3: Data

- *100.0MHz is the speed the PA wants to deliver to the desktop.
- **Cable #1 is to be split in the workstation to support 2 telephones.

Technical specs for the Cat 5e cable is as follows.

TECHNICAL DATA--ELECTRICAL				
	Horizontal		Patch	
Frequency MHz	Attenuation dB/100 m	Next dB min.	Attenuation dB/100 m max.	Next dB min.

	max.			
1	2	62.3	2.4	62.3
4	4.1	53.2	4.9	53.2
10	6.5	47.3	7.8	47.3
16	8.2	44.2	9.8	44.2
20	9.3	42.7	11.1	42.7
31.25	11.7	39.8	14.1	39.8
62.5	17	34.3	20.4	34.3
100	22	32.3	26.4	32.3

TECHNICAL DATA--PHYSICAL			
	CMR	CMP	CM (Patch)*
Conductor diameter-in. (mm)	.020 (0.52)	020 (0.52)	024 (0.61)
Cable diameter-in. (mm)	.195 (5.0)	165 (4.2)	215 (5.5)
Nominal cable weight-lb./kft. (kg/km)	21 (31)	21 (31)	23 (34.2)
Max. installation tension-lb. (N)	25 (110)	25 (110)	25 (110)
Min. bend radius-in. (mm)	1.0 (25.4)	1.0 (25.4)	1.0 (25.4)
* Patch cables utilize stranded tinned copper conductors			

PARAMETRIC MEASUREMENTS		
	Horizontal	Patch
Mutual Capacitance	4.6 nF/100 m nom.	5.6 nF/100 m nom.
DC resistance	9.38 Ohms/100 m Max.	9.09 Ohms/100 m max.
Skew	45 ns/100 m max.	45 ns/100 m max.
Velocity of	72% nom. Non Plenum	72% nom.
Propagation	72% nom. Plenum	

Input Impedance	100 + 15% 0.7772-100 MHz	100 + 15% 0.772-100MHz
	ISO/IEC 11801	

COLOR CODE			TEMPERATURE RATING	
Pair 1	White/Blue	Blue	Installation	0 degrees C to +50 degrees C
Pair 2	White/Orange	Orange	Operation	-10 degrees C to +60 degrees C
Pair 3	White/Green	Green		
Pair 4	White/Brown	Brown		

Appendix 5 -- Telephone Closet{ XE "Telephone Closets" } / IDF Termination Blocks{ XE "IDF Termination Blocks" }

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

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

Each workstation will be assigned a unique station identification number.

Appendix 6 -- Workstation{ XE "Workstations" } Jacks{ XE "Workstations: Jacks" }{ XE "Jacks" }

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

Appendix 7 -- Standard Switches{ XE "Switches" }{ XE "Port Authority Wide Area Network (PAWANET): Switches and Routers" } Inside the Department

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

Cisco{ XE "Cisco" } 5500

Cisco{ XE "Cisco" } 3500 series – low capacity

Cisco{ XE "Cisco" } 4000 series - medium capacity

Cisco{ XE "Cisco" } 6000 series - high capacity

Cisco 4507 series - high capacity - New

Appendix 8 -- Desktop and Lateral Cable Identification Management

WORKSTATION AND LATERAL CABLE IDENTIFICATION/MANAGEMENT (Facility)

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

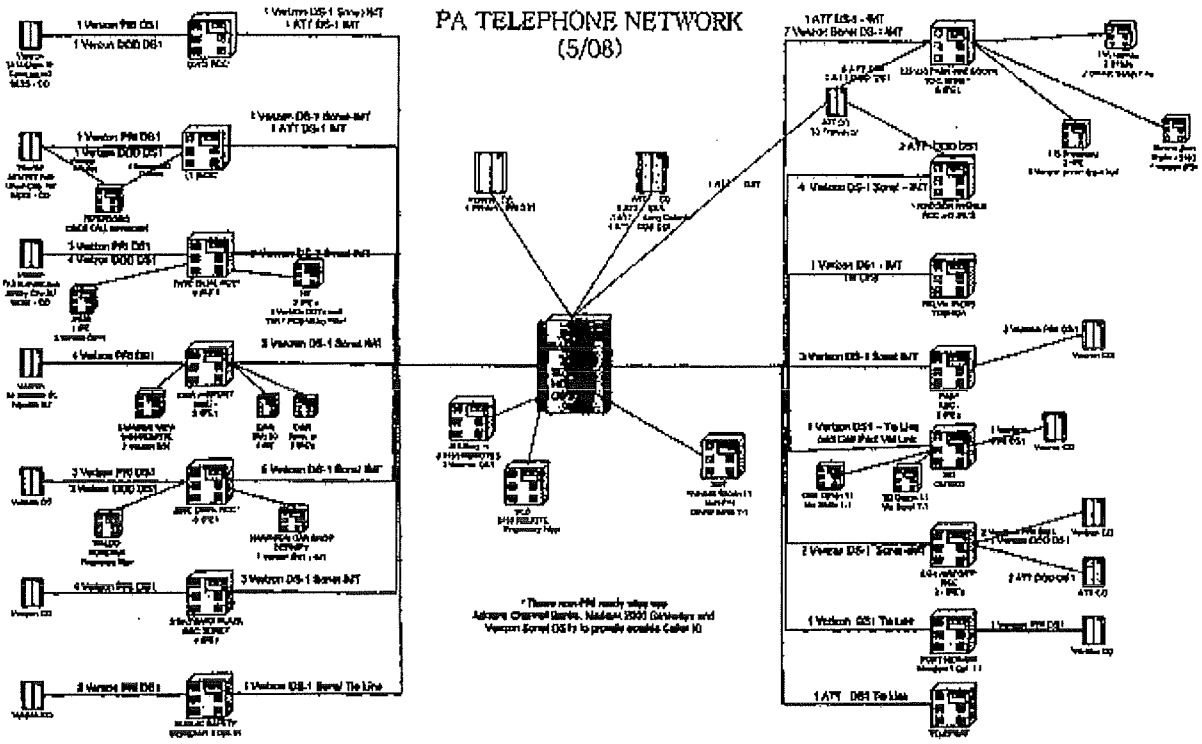
1 - Room number or department name (acronyms are acceptable).

2 - Workstations (3 numeric digits)

The cable identification code for Workstation{ XE "Workstations" } 10 in room 3801 at LGA CTB is 3801-010.

The cable identification code for Workstation{ XE "Workstations" } 15 in PA Automotive shop is Auto-015

Appendix 9 – PA Telephone Network{ XE "Nortel SL100" } 5/08



Appendix 10 – 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 will be loose tube, gel filled, with aramid yarn water block:
   a. Multimode Fiber – **50/125*** micron diameter. Manufacturer of cable TBD
6. Fiber optic cable attenuation from the factory, before installation, shall not exceed:
   a. For multimode – 3.5 db per km @ 850nm / 1.0 db per km @ 1300nm
7. All fiber optic cable is to be labeled on each end and at any junction or patch panel with, 28 gauge, 2" wide embossed with ¼" high letters. The labels are to be fastened to the fiber optic cable using sealed wrap around labels or pliable Velcro ties.
8. Fiber optic cable shall be installed in accordance with the manufacturer's specifications. Any portion of the cable damaged during installation will be repaired or 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.

2. Fiber optic technicians will perform OTDR test on all terminated fibers unless otherwise noted in the Scope of Work.
3. Fiber optic test results shall be recorded, and reports provided to the PA in hardcopy and via a readable txt file (PDF or RTF is acceptable).

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

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

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

Appendix 11 -- Public Telephone Ordering Guidelines

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

General Guidelines

All public telephone requests – that is both coin and non coin in any Port Authority space or any area of the tenant space – both "public" and "club" locations 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 Services Department (TSD) whom will review the request and provide coordination with the appropriate service provider.

General Index

Administrator, 19
Administrator, 15, 16
Administrator, 19
Administrator, 19
Administrator, 20
Administrator, 23
Administrator, 31
AT&T, 5, 8
ATMs, 5, 9
Business Resumption Plan, 20, 33
  Document Format, 33
Cabling, 10, 20, 36
Cisco, 5, 8, 9, 10, 18, 38, 39
Cisco Works, 10
Closed Circuit TV, 5, 8
Communication Room, 20, 35
Databases, 30, 34
Drive Mappings, 12, 28
Electrical Requirements
  Telecommunications, 22
Email, 25
  Public Folders, 25
  Remote Access, 15, 17
Hardware Configuration
  Workstations, 28
HP Open View Network Management, 10
IDF Termination Blocks, 20, 38
Intranet, 5
Intruder Detection, 12, 16
IP Addresses, 9, 10, 12
IPX/SPX, 9
Jacks, 20, 38
LAN Devices, 11, 14
Laptops, 11
Local Service, 8
Logins, 12, 16
  Concurrent, 16
MAPI, 25
Modems, 17
MS/SQL, 30
Naming Conventions, 18, 27
Netware, 11
Networks, 5, 6, 8, 10, 11, 12, 14, 15, 17, 18, 20, 21, 22, 27
  Access, 15
  Connecting LAN Devices, 14
  Enterprise Network, 10, 11, 14, 20
  Intruder Detection, 16
  Logins, 16
  Monitoring Software, 10
  Naming Conventions, 18
  Security, 12
Nortel SL100, 40
Operating Systems, 11, 27
Oracle, 30
Passwords, 16, 17
PeopleSoft, 5, 8
Port Authority Wide Area Network (PAWANET), 5, 6, 8, 9, 10, 14, 17, 22
  ATM Node Assignments, 5, 9
  Diagram, 6
  Functions, 8
  Network Monitoring Software, 10
  Protocols, 9
  Supported Protocols, 8
  Switches and Routers, 9, 11, 20, 38
Printers, 11

Protocols, 8, 10
Public Folder, 25
Public Folders, 25
Remote Access, 27
Routers, 9, 11
SANs, 8, 11, 12
SAP, 5, 8
Scanners, 11
Security, 12, 14, 15, 28, 29, 30, 31, 34
  Applications, 30
  Physical Security, 14, 28, 31
Servers, 11, 12, 13, 14, 18, 22, 25, 30, 31
  Application, 11
  Logical Security, 14
  Names, 12, 18
  Physical Security, 14, 31
  Racks, 11
  Standard Hardware, 18
SNA/SDLC, 9
Sun Solaris, 11, 30
Support Desk, 21
Switches, 9, 11, 20, 38
System Backup and Recovery, 19, 33
  Logs, 19
  Scheduling, 19
System Management, 15, 16, 19, 21, 23, 27, 30
TCP/IP, 9, 10
Telecommunications
  Electrical Requirements, 22
  Standards, 20
Telecommunications Room, 21
Telephone Closets, 20, 38
Telephone Company Interface, 22
Telephone Network
  Cabling, 10, 20, 36
Time Restrictions, 15
Unified Wiring Plan, 36
Uninterrupted Power Supply, 12, 22, 35
Unix, 30
  Logical Security, 30
User Accounts, 15, 27
  Creation, 15
  Security, 15
Verizon, 8
Videoconferencing, 8
Virus
  Protection, 12
  Scanning, 24
Wide Area Network, 5, 10, 11, 17, 27
Windows NT, 15, 25
Windows Server, 30
Wiring Closets, 11
Workstation
  User Accounts, 27
Workstations, 10, 11, 20, 21, 27, 28, 38, 39
  Drive Mapping, 12, 28
  Hardware Configuration, 28
  Jacks, 20, 38
  Naming Conventions, 27
  Remote Access, 27
  Security, 14, 28, 31
  User Accounts, 27

ATTACHMENT I – Port Authority Control Requirements

The following Exhibits outline the Port Authority Control Requirements included in this Attachment:

Exhibit 1	Application Controls Checklist
Exhibit 2	Control Security Requirements
Exhibit 3	Disaster Recovery Checklist and Requirements
Exhibit 4	Security Administration Function
Exhibit 5	Security Requirements
Exhibit 6	Systems Administration & Operation Manual Requirements
Exhibit 7	Web Based Application Checklist

Exhibit 1: Application Controls Checklist

General

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

Hardening of operating system/database that supports the application:

- Disable unnecessary ports/services.
- Remove all samples from the box.
- Change all default passwords; delete all default content and scripts.
- Limit user account access.
- Document system accounts like administrator, root, oracle, and sys.
- Document user/group access rights
    - Users/groups should be setup with least access required to perform job responsibilities.
- Follow Port Authority password standards (90-day expiration, lockout after 3 incorrect password attempts, concurrent logins, 6 alphanumeric characters)
- Set "automatic session timeout" to 15 minutes of inactivity and require user to log back in with a valid ID and password.
- Implement access control at the database level (i.e. user roles and permissions, passwords, secure links)
- Apply all new patches and fixes to operating system and application software for security.
- Use secure, encrypted remote access methods.
- If the application is a web application, log (and monitor) web traffic and trend the activity looking for abnormal activity.
- Ensure that appropriate security and vulnerability assessment tools are running.

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

- Procedures to grant/revoke access should be documented.
    - Access request forms for adding/modifying/deleting users should be used.
- Ensure that security administrator procedures exist to:
    - create/remove application access in a timely manner
    - review user roles/permissions
- Validate that all users have accessed the application within the past 90 days.
    - Review dormant accounts

Exhibit 1: Application Controls Checklist

- Ensure that password controls for the application are consistent with Port Authority requirements
  - Passwords must be at least six (6) alphanumeric characters long
  - Passwords must be changed every 90 days
  - Passwords must not be shared
  - UserID accounts should be locked after a three logon failures.
- Password file should be securely stored with limited access and encrypted.
- Application forces initial Passwords to be changed and the initial passwords should not be easily guessable.
- Each user has a unique userID.
- Should have a segregation of duties/roles. Roles are setup with least access required to perform job responsibilities.

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. Additionally, should specify how long active data is kept.
- Sensitive data like credit card #s and social security #s should be encrypted.

Application Interfaces

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

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. Additionally, documentation of approval for change and evidence of testing should be in place.

Application Logging, Audit Trails and Record Retention

- Users and roles should be tracked and reviewed; Maintain documentation
- All failed logon attempts should be logged.
- All sensitive transactions and changes should be logged and an audit trail created.

Exhibit 1: Application Controls Checklist

- 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

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

Contingency Planning, Disaster Recovery and Backup Management

- A Business contingency plan and a disaster recovery plan for the application should be documented.
- Plans should be tested and the outcomes of the tests (success/failure) should be documented.
- Backup copies of these plans should be stored off-site.
- Backup procedures should be documented and regular backups of the application and the application data should be stored off-site.
- Application executables should be stored off-site or in escrow.
- Application configurations should be documented and backed-up.

Performance Monitoring

- Incident monitoring procedures should be documented and incidents logs should be reviewed to ensure that appropriate action is taken.
- Performance statistics should be examined and reviewed periodically by system administrators/business owner(s).
    - There should be SLA and /or requirement with the vendor for "uptime".

Exhibit 2: Control Security Requirements

System Configuration

- Default accounts are secured/locked/or removed.
- Public and Guest accounts/profiles should be secured with no access.
- Controlled use of administrative accounts.
- Limited assignment of administrative privileges and roles.
- Access violation reports.
- Audit trails for operating, application and database systems
- Not display last user who signed on
- No use of login scripts for accounts.
- LDAP compliant
- Encryption of data in storage and transmission of data via the network.
- Unnecessary services removed and/or disabled.
- Secured and approved remote access strategy.
- Data archiving in place.
- Data Retention Policy and Procedures in place.
- Requirement for user name and password
- System timeout for inactivity set to 15 minutes.
- All default settings or passwords changed.
- Test facility which replicates the production system.
- Patching up to date. Patch Management Procedures and documentation includes testing.
- Virus software implemented and up to date.

Physical Protection

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

Backup

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

Access Controls

- Background checks are performed on all personnel.
- Account expiration for contractors and consultants
- Account password is not the same as account name

Exhibit 2: Control Security Requirements

- No concurrent login capabilities
- No accounts assigned to individuals who no longer require the account
- Default accounts are locked or secured.
- Accounts never logged into are removed.
- Accounts adequately identify the user – no generic accounts.
- Accounts not used by multiple individuals
- Administrator account passwords adequately secured.
- Disabled accounts are deleted.
- No test accounts on production.
- No generic accounts
- No excessive privileges on accounts – least privilege granted.
- Guest accounts are removed
- Inactive accounts are removed
- Review of profiles, access levels, privileges
- Access reports by user and privilege
- All user account profile should include Employee ID number and full user name.
- Assigned Security Administrator
- Baseline tools or security products are implemented on a quarterly basis.
- Adequate network zoning
- Adequate performance monitoring
- Intrusion Detection System in place
- Secured and authorized remote access
- Firewalls in place
- Warning message/banner
- No modems (dial up or wireless)

Password Controls

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

Documentation / Procedures

- Security Administration Procedures documented
- Procedure for granting, modifying or deleting access to the system are documented
- Access request forms authorized

Exhibit 2: Control Security Requirements

- Access request forms retained
- Access request forms are used to assign access
- Change Management procedures documented
- Test results documented
- Backup, restart and recovery procedures documented
- Disaster Recovery Plans and Business Resumption Plans documented and comprehensive.
- Documentation is current for System Manuals, Operating Instructions
- Documentation is up to date for Firewall rule sets.
- Inventory listings of equipment and software.
- Adequate training
- Password reset procedures controlled (Help desk function)
- System Administration procedures documented
- Data retention and archiving procedures documented
- Roles and Responsibilities defined and documented
- Virus Patch Management procedures documented
- Batch and Interface Management procedures documented
- Patch Management procedure documented
- Escalation procedures documented
- Incident Response procedures documented
- Incident and Error logging/tracking.
- Topologies exist and are up to date (system/network diagrams)
- System monitoring/performance
- Log reviews
- Management reporting – like Access Reports, Exception transaction reporting

Exhibit 3: *DISASTER RECOVERY PLAN CHECKLIST*

Disaster recovery is a plan, which could be executed in the event of a total disaster in order to bring the computer systems back to a functioning whole. Typically, the disaster in question is one, which destroys a complete site that requires restoration of support, particularly Information Technology support. Most commonly considered causes of disasters are fire, explosion, flooding, hurricanes and tornados. Disaster recovery planning normally involves alternate locations for major systems as well as the planning and testing of switch over measures, emergency transportation and so on.

The Disaster Recovery plan should include at a minimum the following areas.

1. Disaster Recovery
   - Manager Responsibilities
   - Plan Administration
     - Distribution of the Disaster Recovery Plan – All team members, LAN and an offsite location should have a copy of the current plan and its attachments.
     - Maintenance of the Business Impact Analysis
     - Training of the Disaster Recovery Team
     - Testing of the Disaster Recovery Plan
     - Evaluation/Review of the Disaster Recovery Plan and Tests – the DR Plan should be reviewed and the DR Test should be performed at a minimum twice a year. Update the plan to reflect changes in activities, procedures, performance, staff, and etc. Set a regular time for the review.
     - Maintenance of the Disaster Recovery Test Results – Maintain copies of the test results and what scenarios and areas of the plan were tested.

2. Business Impact Analysis - Minimize the impact on the business with respect to dollar losses and operational interference
   - Critical Time Frame - Recover the system and/or component of the system within the critical time frames established and accepted by the user community. This should include the time estimate of how long it would take to recover the whole system or any sub components.
   - Application System Impact Statements - This area is where a business owner decision of what areas of the system has a priority in how it is brought back into normal operation. How long could these operations be performed without computer support?
     - Essential – Are systems or components of the system that are very critical and need to be back in operation immediately because the business cannot function.
     - Delayed – Are systems that are needed but could be delayed and could not adversely effect the business process.
     - Suspended – Are system or components that are not critical and can wait until the full system is back to normal operation.
   - Recovery Strategy & Approach

3. Disaster Definition – All possible interruptions should be defined, and then the steps to minimize their impact need to be documented. This includes disk array failure, power loss, loss of network, loss of wireless network, loss remote access, equipment, computer processor failures, etc.

Exhibit 3: *DISASTER RECOVERY PLAN CHECKLIST*

- Detailed Recovery Steps for each Disaster Definition - This should be the technical steps to recover the different areas of the system like the Operating system, database, application, routers, firewall, and etc.
- Escalation Plans and Decision Points

4. Data Center Systems – Dependencies should be notated.
   - System Components- A copy of all essential office equipment and records should be stored off-site. Specify any special computer hardware, software, databases, networks or other technology.

     - Backup Strategy
       - Storage Rotation
       - Back-up Files
       - Off Site Storage of Back-up Files
       - Back-up Files Retrieval Process, Vendor information and Forms for Off Site Storage

     - Hardware -
       - Hardware inventory for system in operation
       - Desktop Workstations (In Office)
       - Desktop Workstation location
       - Desktop Workstations (Offsite including at home users)
       - Laptops

     - Software -
       - Software inventory of the system in operation
       - Systems, Applications and Network Software
       - Communications
       - Operations

     - Off-Site Inventory

     - Supplemental Hardware/Software Inventory

5. Escalation Plans and Decision Points

6. Disaster Recovery Emergency Procedures
   - Plan Procedure Checklist - should have a checklist of the plan procedures and area for documenting exceptions where the plan was not adhere to and what was done in its place. Disaster Recovery Procedures in a check list with approval format.

   - Disaster Recovery Organization – should have the full disaster recovery team listed by position or individual and what are their responsibilities. This section of the plan should include Port Authority and PATH personnel, PA/PATH management, and all vendors that work or have responsibilities during a disaster. This area should be reviewed semi-annually for updates and changes.
     - Recovery Organization Chart

Exhibit 3: *DISASTER RECOVERY PLAN CHECKLIST*

- Disaster Recovery Team & Recovery Team Responsibilities
- Recovery Management & Senior Manager Responsibilities
- Damage Assessment and Salvage Team & Team Responsibilities

Problems and Changes - Need to be documented and what was done to rectify them.

Essential Position – Require back-up personnel to be assigned.

7. Pre-Disaster - What steps need to be in place prior to a disaster for this plan to work? If there are any assumptions, they should be notated here.
   - Recovery Management
   - Damage Assessment and Salvage
   - Hardware Installation

8. Contacts information - This area should be reviewed semi-annually for updates and changes.
   - Disaster Recovery Team - This should include primary and secondary phone numbers, home address, emergency contact information, and their backups information.
   - Vendor Phone/Address List – Include account information and account representative information.
   - Command Center – Primary and Alternative site locations, hot spots, phone numbers, time scheduling

9. Post-Disaster – Detail what steps need to be taken to move from disaster mode back to normal operations.

Exhibit 4: Security Administration Function

Responsible for:

- Establishment of access rights, groups, profiles etc. for a system or application for which they are responsible and documenting their use and definitions.
- The development of security procedures which define the granting of access and the administration of security functions of their system or application. The ongoing review and update of these security procedures.
- Responsible for the development of add/change/delete access requests forms.
- The development of procedures for changing or deleting accounts or privileges when staff leave or change assignments. Execution of these procedures in a timely manner.
- Regular review of who has access to their data and determining if it is appropriate and still required.
- Ensuring that users are required to acknowledge, in writing, that they have been informed of the organization's position on security and confidentiality of information prior to access being given.
- Assigning appropriate expiration dates for accounts used by temporary/consulting staff.
- The development of procedures for responding to, documenting and escalating security incidents.
- The investigation and appropriate escalation of a security incident matter.
- Setting any global system or application controls (i.e. password controls, time out, concurrent logins) consistent with the Standards and Guidelines for Port Authority Technology.
- Restricting remote access and monitoring and reviewing the activity log. (Limit or no use of modems. Modems should be configured according to the Standards and Guidelines a certified by the Information Systems Security Officer.)
- Development and review of reports such as Kane Security Analyst, ISS or ESM to monitor areas of security exposure.
- Daily event log reviews for irregular activities and security violations.
- Keeps management and the business unit informed on security issues.

- Development of regular processing schedules for the production of security reports i.e. unsuccessful logon attempts, audit trail reports.
- Development of procedures for reviewing the reports and logs on a regular basis and taking appropriate corrective action.
- Responsible for ensuring that the system complies with the Standards and Guidelines for Port Authority Technology.
- Determining high-risk activities, establishing logs of those activities and tables and determining appropriate review cycles.
- Ensuring that operating system, database system and application security issues are coordinated.
- Keeping abreast of vulnerabilities of systems, databases, or application as they are discovered and patching them or implementing compensation controls.
- Development of procedures for the disposal of unneeded confidential data produced from the application.
- Ensure all system hardware (i.e. servers, comm. rooms, backup tapes, etc.) and software are secured from tampering or damaging.
- Ensure that operating systems at a minimum complies with the Distributed Systems Environment in the Standards and Guidelines and industry standards.
- Document a virus protection and recovery plan.
- Firewall Administration, Firewall configuration, rules, logs, and patches
- Intrusion Detection System Administration, monitoring network traffic across the firewall and in the DMZ.
- Router and Switches Administration, configuration file, backups, patches, and change controls.

Exhibit 6: Systems Administration & Operation Manual Requirements

General Information

1) Server name
   a) IP address
   b) Location
   c) Operating system – version, patch level
   d) Database – version, patch level
   e) Application
2) LDAP and Domain Controller Configuration
3) Diagrams
   a) Network topology
   b) Application flowcharts

System

4) System Configuration
5) System Applications and Services
6) Network Time Synchronization
7) Patch Management
   a) Normal and Emergency Procedures
8) System Schedule
   a) System downtime
   b) System backups
   c) System batch processing

Access Controls

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

Password Controls

12) Password Configuration
   a) Length
   b) Alpha/numeric
   c) Password dictionary
   d) Password age
   e) Password expiration

13) Account Policies
   a) Concurrent log in
   b) Vendor/Consultant Account Expiration (usually the length of the contract)

Remote Access

14) Strategy/Approach
15) Approvals

Operation

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

Physical

21) Server Location
   a) Site Security
   b) Server Mounting
      i) What is the rack configuration and who has access to the keys
   c) Environmental Controls
      i) Humidity and Temperature Monitoring

Anti-Virus Management

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

Change Management

25) Testing Environment
26) Normal Procedures
27) Emergency Procedures
28) Requests are documented
29) Specific timetables/scheduling are documented

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

Patch Management

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

Reporting and Monitoring

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

Problem & Incident Management

40) Problem reporting/resolution tracking system
   a) Problems are appropriately logged and prioritized.
   b) Corrective measures are documented.

Segregation of Duties

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

ATTACHMENT J – Existing RWIS System Schematics

The following Exhibits outline each Airport's existing RWIS layout:

Exhibit A	JFK
Exhibit B	LGA
Exhibit C	EWR
Exhibit D	SWF
Exhibit E	TEB