

THE PORT AUTHORITY OF NY & NJ

**PROCUREMENT DEPARTMENT
4 WORLD TRADE CENTER
150 GREENWICH STREET, 21ST FL.
NEW YORK, NY 10007**

3/16/2016

ADDENDUM # 3

To prospective Proposer(s) on RFP # 45178 for Design, Fabricate and Deliver Four (4) Switching Locomotives for PATH

- Questions now due 3/23/2016, no later 3:00PM
- Questions were due 3/16/2016, no later than 3:00PM
- Proposals now due 4/5/2016, no later than 2:00PM
- Proposals originally due 3/8/2016, no later than 2:00PM

I. CHANGES/MODIFICATIONS

The following changes/modifications are hereby made to the solicitation documents:

1. Add the attached Contract Drawings as Attachment H.
2. Add the following attached documents as Attachments
Attachment I. Audit Control Checklists
Attachment J. Technology Standards for the Port Authority
3. In the RFP, page 9. Section 5, "Evaluation Criteria and Ranking" delete the first two paragraphs and the listing of items A-D, in their entirety and replace with the following:

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

A. Technical Proposal

The ability of the proposer to meet the functional requirements of this RFP based on, among other things, (a) an analysis of the proposer's design solutions, as represented by drawings, illustrations, catalog cuts, and other submittals intended to demonstrate the proposer's understanding of PATH's design guidelines, (b) an analysis of the features of the switching locomotives proposed for this project,

Addendum # 3

and the extent to which each of these addresses the technical specifications and requirements of the RFP, (c) the anticipated requirements for maintaining the installed system, (d) the proposed schedule for undertaking and completing the work, and (e) ability to meet the FTA Buy America requirements.

B. Cost Proposal

The cost to PATH for this switching locomotives project, based on (a) the proposer's proposal for design, fabrication, delivery, commissioning, and warranty of the switching locomotives, (b) the proposed cost of required spare parts and any other recommended spare parts.

C. Management Approach

The proposer's management approach as demonstrated by its submission of the following:

- (a) A proposed staffing plan, organizational structure, and management approach to be used for this project, (b) a tracking system for deliverables, controlling costs, and management of the fabrication, (c) procedures for keeping the PATH team informed of issues and progress during project, (d) approach to quality control, and (e) the proposer's DBE plan and the extent to which it meets or exceeds PATH Requirements.

D. Experience of the firm and personnel

The potential of the proposer to provide the types of locomotive equipment required by PATH based on (a) the proposer's past experience in successfully providing similar design, fabrication, and delivery for similar switching locomotives, (b) the proposer's past experience in maintaining comparable systems following delivery, (c) the experience of the contractor's lead engineer who will manage the design services, including but not limited to mechanical design, commissioning, and final acceptance testing of similar locomotives, and (d) indication of its success on past projects.

4. In Section 8 of the RFP, "Proposal Submission Requirements":

- a. Delete paragraph (F)(1)(C)(c) titled "Technical Proposal" on page 13 in its entirety and replace with the following:

"c. The anticipated requirements for maintaining the installed system inclusive of computer systems and software."

- b. After "Appendix A1 DBE Goals Statement in accordance with" in paragraph F(1)(4)(f), "FTA Proposal Submission Requirements" on

page 13, delete “Part III clause entitled ‘DBE Program’” and replace it with “Attachment F, ‘Disadvantaged Business Enterprise (DBE) Program.’”

c. Add the following new section on page 13 after (F)(1)(4)(e)”:

“(f) Consistent with Attachment D, PATH Locomotive Specifications Information Technology Provisions, provide system diagram and matrix listing all computer systems and software components that are used within the overall solution, whether they are on the locomotive or used in maintenance, warranty or other functionality.

- (i) The matrix shall be all inclusive, including all fields necessary for the Authority to understand the following fields at a minimum: name of the software product, manufacturer, version being used, indication if software is open source software, list of and copies of software license agreement (sometimes known as end user license agreement (EULA)), confirmation that any and all license agreements are transferable to and are/will be in name of the Authority, list of and copies of any maintenance or support agreements and which, if any, maintenance plans were selected, if there are ongoing software maintenance costs, on what those costs are based and when the current maintenance terms included with locomotive expires.
- (ii) Include a statement on adherence to Authority Audit Control Checklists, Attachment I; and Port Authority Technical Standards and Guidelines, Attachment J. Any areas of non-compliance shall be detailed.
- (iii) Provide a statement confirming compliance with all applicable NIST and other standards and include a discussion on any internet or other external connectivity requirements and the ability to/impact of not having internet connectivity.
- (iv) Include a statement on how software escrow requirements, in Section J of Attachment D shall be satisfied.”

5. RFP Attachment B – Cost Proposal

In “1. Pricing Sheet(s)” in the first sentence under the caption “LEAD TIME”, delete, “Part III, paragraph” on page 3 and replace it with “Attachment E, section 4”.

6. RFP Attachment C – Locomotive Specifications:

- (i) In Section 1, 1.0, “Scope of Specification”, add the following to Section 1.6.1 after “Endurance Limit” on page 7:

“‘Equipment’ shall mean the Locomotives, all parts and equipment contained therein, including software, and spare parts”

- (ii) In Section 1, 1.0, “Scope of Specification”, add the following to Section 1.6.1 after the definition of "Service" or "Service Use" on page 11:

“Software” shall mean any and all computer application programs which are incorporated as part of any System, Subsystem, assembly, subassembly or components thereof, or any interface system control between or among the Systems, Subsystems, assemblies, subassemblies, or component thereof, in the Locomotives, or which are used in connection with a system (which use involves microprocessors, controllers, drivers, or other electronic data processing elements) or which are used in connection with any related diagnostic or testing equipment (if any), together with all related Documentation, including without limitation the object code, source code and pseudo-code versions of such assemblies, subassemblies, programs, firmware containing such programs, know-how protocols, listings, instruction sets, indices and other intellectual property necessary for the Authority’s use of the Software for the Approved Purposes in the form prepared by the Contractor, Subcontractor, Supplier or Manufacturer in the regular course of its business, or to the extent that the Technical Specifications require a different form, then in the form required by the Technical Specifications.

- (iii) Add the following paragraph as the last paragraph of Section 15.1 General on page 138.

“All work on computer systems and associated Software shall be done consistent with industry best practices and performed in accordance with Authority provided Audit Control Checklists, Technical Standards and Guidelines (attached as Attachments I and J).”

- (iv) Section 20.1.3.2, remove the third bullet point and its text on page 291.
- (v) After Section 20.1.3.4.5 on page 294, Add a new Section 20.1.3.4.6, as follows:

“Software Training

The Contractor shall provide PATH with necessary training to operate and maintain all Software to be provided hereunder for use with the Locomotives.”

7. Attachment D – Path Locomotive Specifications --Information Technology Provisions

In Section 1, “Authority’s Rights In Property”:

- a. Delete “1 - Authority’s Rights In Property” and replace it with “I - Authority’s Rights In Property”;
- b. In Section 1.A.2., delete i - iii in their entirety, and replace with;
 - i. “use of the Locomotives and maintenance and repair of the Locomotives;
 - ii. preparation of specifications for future production orders of Locomotives employing some or all of the Licensed Technology (the “Specification Purpose”);
 - iii. evaluation and qualification for the purposes of future Locomotive procurements of Systems, Subsystems and components of Subsystems on the Locomotives to be delivered under this Contract;”
- c. In Section I.B., “Software License,” delete the second paragraph in its entirety.
- d. In Section I.J – in the first sentence, insert the words “at its cost” after “maintain” and before “an escrow account”
- e. In Section I.J. – at the end of the Section, add the following language:

“Updates to software shall be deposited into the escrow account within 10 days of release, with updates following implementation, if necessary.”

In Section II, “Patents, Copyrights, etc., Infringement Claims”:

- 8.** Section II.B.1. – delete the following words from the first sentence:

“shall implement the Policy and Procedure of its Escrow Agent as set forth in paragraph J. and”

- 9.** Attachment E – Contract Specific Terms and Conditions

- (i) Replace the Table of Contents with the attached Table of Contents.
- (ii) Section 12. Equipment Warranty, add the following language at the end of the last paragraph:

“The warranty set forth in this section also applies to Software provided under this Contract.”

- (iii) Add the following after Section 19:

20. CONTRACT REVIEW AND COMPLIANCE AUDITS

The Contractor, and any subcontractors, shall provide prompt system access and reasonable assistance to the Authority's External and Internal Audit staff or its consultants in their performance of work under the contract, including producing specific requested information, extraction of data and reports. The Contractor, and any subcontractors, shall promptly support requests related to audits of the contract, administrative functions and operations covered by this Contract. The Authority will require access to the Contractor's environment which supports the systems used to provide services required under the contract on a periodic basis; the hours to be determined, at the convenience of the authority.

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 operations related to this Port Authority contract.

21. AUTHORITY ACCESS TO RECORDS

The Authority shall have access during normal business hours to all records and documents of the Contractor relating to any service provided under this Contract, amounts for which it has been compensated, or claims the Contractor should be compensated, by the Authority above those included in the compensation set forth elsewhere herein. All Contractor records shall be kept in the Port District (as defined in McKinney's Unconsolidated Laws §6403). The expenditures incurred for an audit of records outside the Port District shall be paid by the Contractor. The Contractor shall obtain for the Authority similar access to similar records and documents of subcontractors. Such access shall be given or obtained both before and within a period of three (3) years after Final Payment to the Contractor, provided, however, that if within the aforesaid one year period the Authority has notified the Contractor in writing of a pending claim by the Authority under or in connection with this Contract to which any of the aforesaid records and documents of the Contractor or of his subcontractors relate either directly or indirectly, then the period of such right of access shall be extended to the expiration of six (6) years from the date of Final Payment with respect to the records and documents involved.

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

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

- (iv) Delete all references to "Part III" at the bottom of the pages.

This communication should be initialed by you and annexed to your Proposal upon submission.

In case any Proposer fails to conform to these instructions, its Proposal will nevertheless be construed as though this communication had been so physically annexed and initialed.

THE PORT AUTHORITY OF NY & NJ

Selene Ortega, Manager
Commodities and Service Division

PROPOSER'S FIRM NAME: _____

INITIALED: _____

DATE: _____

QUESTIONS CONCERNING THIS ADDENDUM MAY BE ADDRESSED TO RICHARD GREHL, WHO CAN BE REACHED AT (212) 435-4633 OR AT RGREHL@PANYNJ.GOV.

DRAWING NO.	DRAWING TITLE
L1-000	DRAWING INDEX
P-0001	PATH PA4 CARBODY KINOMATIC ENVELOPE
P-0002	PATH PA4 DIMENSION DIAGRAM
P-0003	PATH PA4 CLEARANCE LIMITING OUTLINE- UNDERCAR
P-0004	PATH PA4 STATIC ENVELOPE
P-0005	PATH TUNNEL AND OUTSIDE AREA
P-0006	PATH BLEV OF CONTACT RAIL AND PROTECTION RAIL OPEN AREA
P-0007	PATH ASSY OF CONTACT RAIL AND PROTECTION BOARD TUNNEL
P-0008	PATH CONTACT RAIL IN HIGHEST POSITION
P-0009	PATH- AUTOMATIC TRAIN STOP TRIPPER ARM
P-0010	PATH- COUPLER ARRANGEMENT
P-0011	PATH- COUPLER HEAD FORM 8501
P-0012	PATH- FLAT CAR PIPING ARRANGEMENT
P-0013	PATH-F LATCAR ELECTRICAL CIRCUIT

WORKING LOCOMOTIVE DRAWING INDEX

DRAWN BY - ASH RAHMAN
CHECKED BY - VICTOR SEGARRA

ISSUED - 7/21/2014

SIZE
SCALE

FSCM NO
NOT TO SCALE

DWG No
L1 - 000

SHEET

REV
0.0

1 OF 1

INSPECTION & MAINTENANCE MANUAL
CARBODY

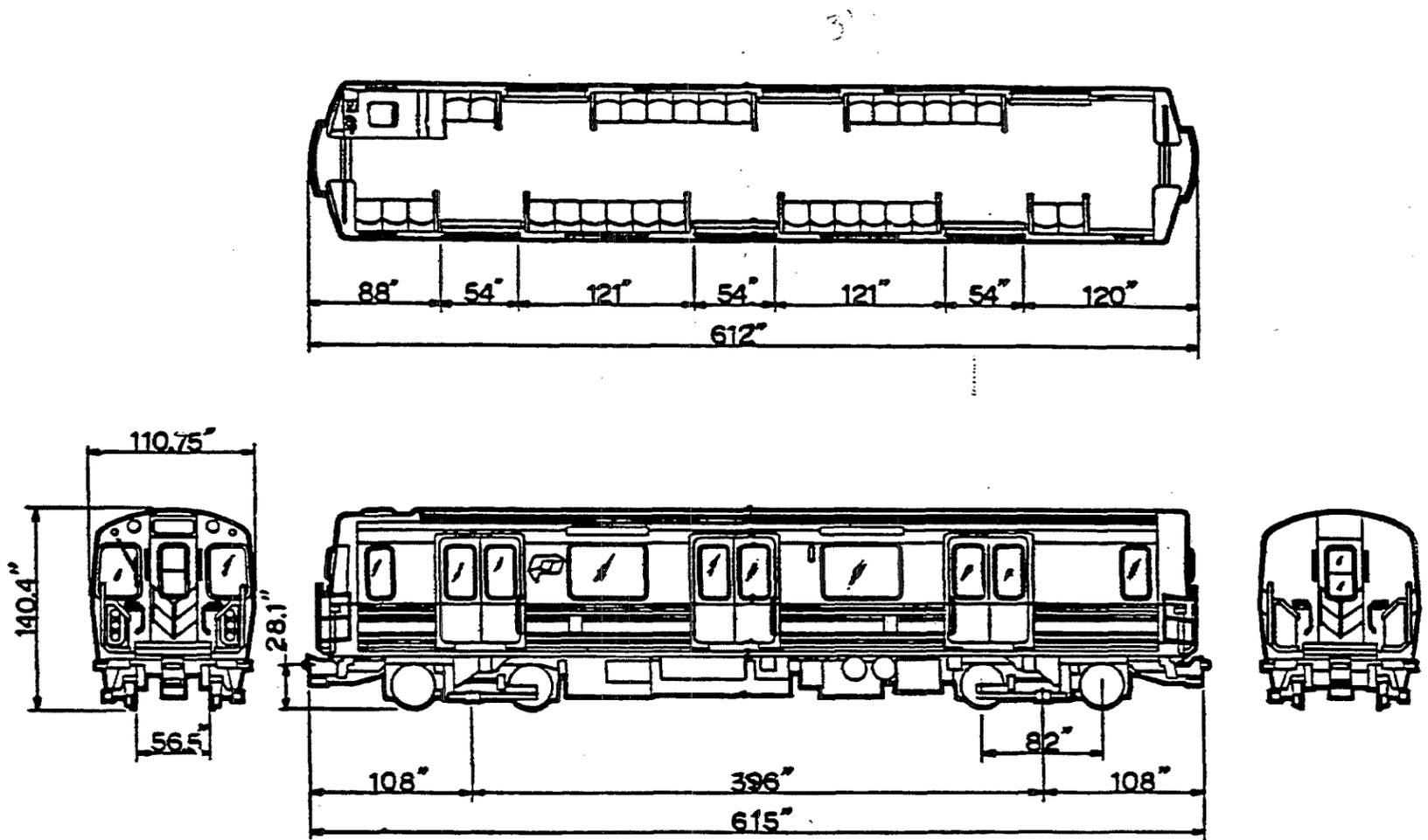
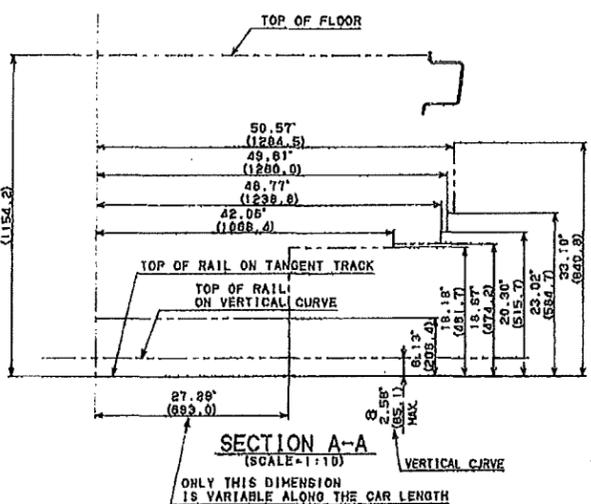
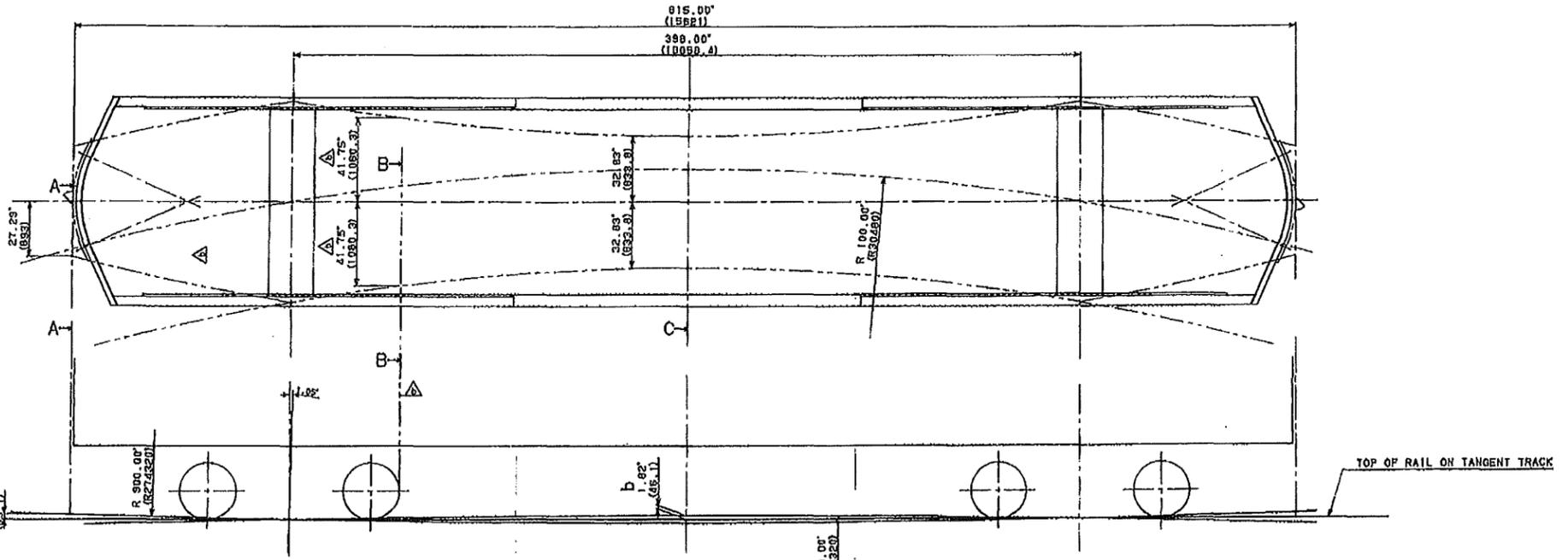


Figure 1-5: DIMENSION DIAGRAM (PA-4 CAR)

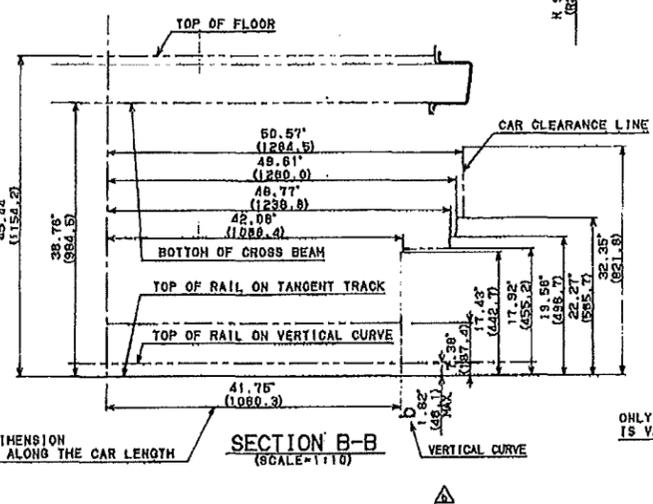
P-0002

13023-03501b

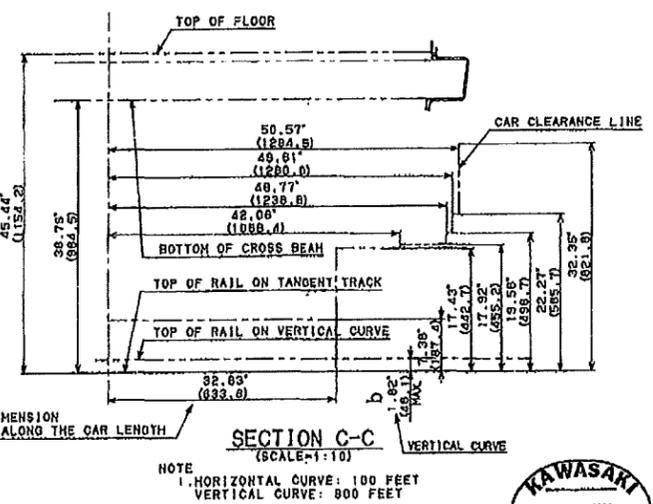
R
PE
B
C
D
E
F
G
H
Y



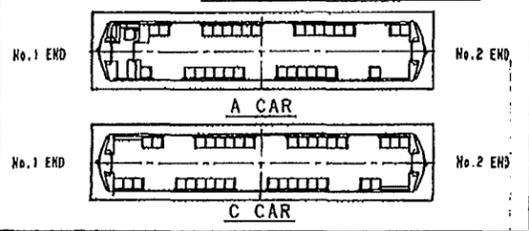
ONLY THIS DIMENSION IS VARIABLE ALONG THE CAR LENGTH



ONLY THIS DIMENSION IS VARIABLE ALONG THE CAR LENGTH



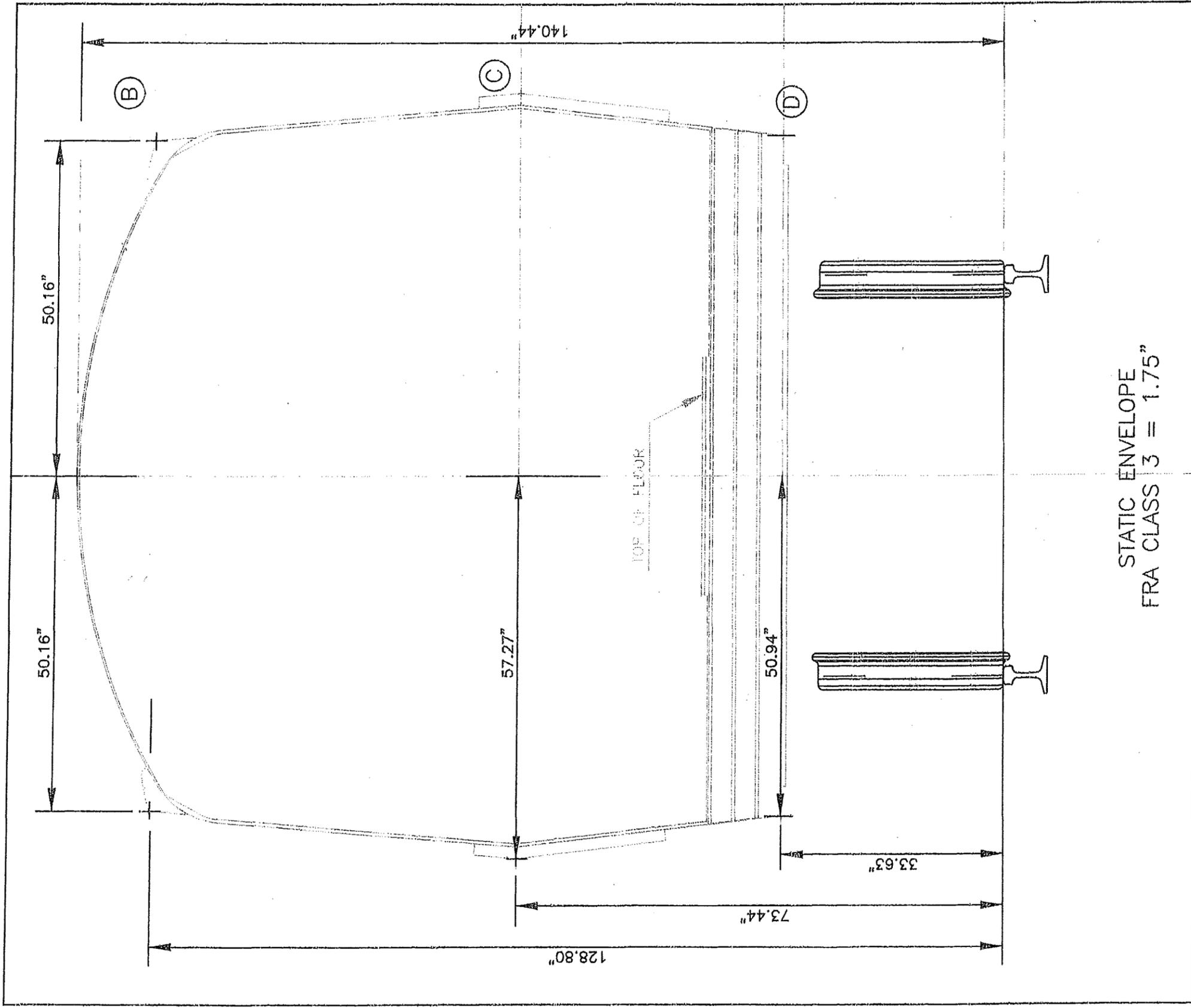
ONLY THIS DIMENSION IS VARIABLE ALONG THE CAR LENGTH



TYPE	NO. OF CARS	WEIGHT	APPROXIMATE
A	1	17,000	ALL CARS
C	1	17,000	ALL CARS

Subject to the Railcar's rights and interests...
 This drawing is the property of Kawasaki Railcar Inc. and shall remain the property of Kawasaki Railcar Inc. if it is used for any other purpose without the written consent of Kawasaki Railcar Inc. or its licensees.

UNLESS OTHERWISE SPECIFIED	CLASSIFICATION	SCALE
VALUANCE OF DIMENSIONS	M R R B	1:30
1.00" = 1'-0"		
2.00" = 2'-0"		
4.00" = 4'-0"		
8.00" = 8'-0"		
16.00" = 16'-0"		
32.00" = 32'-0"		
64.00" = 64'-0"		
128.00" = 128'-0"		
256.00" = 256'-0"		
512.00" = 512'-0"		
1024.00" = 1024'-0"		
2048.00" = 2048'-0"		
4096.00" = 4096'-0"		
8192.00" = 8192'-0"		
16384.00" = 16384'-0"		
32768.00" = 32768'-0"		
65536.00" = 65536'-0"		
131072.00" = 131072'-0"		
262144.00" = 262144'-0"		
524288.00" = 524288'-0"		
1048576.00" = 1048576'-0"		
2097152.00" = 2097152'-0"		
4194304.00" = 4194304'-0"		
8388608.00" = 8388608'-0"		
16777216.00" = 16777216'-0"		
33554432.00" = 33554432'-0"		
67108864.00" = 67108864'-0"		
134217728.00" = 134217728'-0"		
268435456.00" = 268435456'-0"		
536870912.00" = 536870912'-0"		
1073741824.00" = 1073741824'-0"		
2147483648.00" = 2147483648'-0"		
4294967296.00" = 4294967296'-0"		
8589934592.00" = 8589934592'-0"		
17179869184.00" = 17179869184'-0"		
34359738368.00" = 34359738368'-0"		
68719476736.00" = 68719476736'-0"		
137438953472.00" = 137438953472'-0"		
274877906944.00" = 274877906944'-0"		
549755813888.00" = 549755813888'-0"		
1099511627776.00" = 1099511627776'-0"		
2199023255552.00" = 2199023255552'-0"		
4398046511104.00" = 4398046511104'-0"		
8796093022208.00" = 8796093022208'-0"		
17592186044416.00" = 17592186044416'-0"		
35184372088832.00" = 35184372088832'-0"		
70368744177664.00" = 70368744177664'-0"		
140737488355328.00" = 140737488355328'-0"		
281474976710656.00" = 281474976710656'-0"		
562949953421312.00" = 562949953421312'-0"		
1125899906842624.00" = 1125899906842624'-0"		
2251799813685248.00" = 2251799813685248'-0"		
4503599627370496.00" = 4503599627370496'-0"		
9007199254740992.00" = 9007199254740992'-0"		
18014398509481984.00" = 18014398509481984'-0"		
36028797018963968.00" = 36028797018963968'-0"		
72057594037927936.00" = 72057594037927936'-0"		
144115188075855872.00" = 144115188075855872'-0"		
288230376151711744.00" = 288230376151711744'-0"		
576460752303423488.00" = 576460752303423488'-0"		
1152921504606846976.00" = 1152921504606846976'-0"		
2305843009213693952.00" = 2305843009213693952'-0"		
4611686018427387904.00" = 4611686018427387904'-0"		
9223372036854775808.00" = 9223372036854775808'-0"		
18446744073709551616.00" = 18446744073709551616'-0"		
36893488147419103232.00" = 36893488147419103232'-0"		
73786976294838206464.00" = 73786976294838206464'-0"		
147573952589676412928.00" = 147573952589676412928'-0"		
295147905179352825856.00" = 295147905179352825856'-0"		
590295810358705651712.00" = 590295810358705651712'-0"		
1180591620717411303424.00" = 1180591620717411303424'-0"		
2361183241434822606848.00" = 2361183241434822606848'-0"		
4722366482869645213696.00" = 4722366482869645213696'-0"		
9444732965739290427392.00" = 9444732965739290427392'-0"		
18889465931478580854784.00" = 18889465931478580854784'-0"		
37778931862957161709568.00" = 37778931862957161709568'-0"		
75557863725914323419136.00" = 75557863725914323419136'-0"		
151115727451828646838272.00" = 151115727451828646838272'-0"		
30223145490365729366544.00" = 30223145490365729366544'-0"		
60446290980731458733088.00" = 60446290980731458733088'-0"		
120892581961462917466176.00" = 120892581961462917466176'-0"		
241785163922925834932352.00" = 241785163922925834932352'-0"		
483570327845851669864704.00" = 483570327845851669864704'-0"		
967140655691703339729408.00" = 967140655691703339729408'-0"		
1934281311383406678458816.00" = 1934281311383406678458816'-0"		
3868562622766813356817632.00" = 3868562622766813356817632'-0"		
7737125245533626713635264.00" = 7737125245533626713635264'-0"		
15474250491067253427270528.00" = 15474250491067253427270528'-0"		
30948500982134506854541056.00" = 30948500982134506854541056'-0"		
61897001964269013709082112.00" = 61897001964269013709082112'-0"		
123794003928538027418164224.00" = 123794003928538027418164224'-0"		
247588007857076054836328448.00" = 247588007857076054836328448'-0"		
49517601571415210967265696.00" = 49517601571415210967265696'-0"		
99035203142830421934531392.00" = 99035203142830421934531392'-0"		
198070406285660843869062784.00" = 198070406285660843869062784'-0"		
396140812571321687738125568.00" = 396140812571321687738125568'-0"		
792281625142643375476251136.00" = 792281625142643375476251136'-0"		
1584563250285286750952502272.00" = 1584563250285286750952502272'-0"		
3169126500570573501905004544.00" = 3169126500570573501905004544'-0"		
6338253001141147003810009088.00" = 6338253001141147003810009088'-0"		
12676506002282294007620018176.00" = 12676506002282294007620018176'-0"		
25353012004564588015240036352.00" = 25353012004564588015240036352'-0"		
50706024009129176030480072704.00" = 50706024009129176030480072704'-0"		
101412048018258352060960145408.00" = 101412048018258352060960145408'-0"		
202824096036516704121920290816.00" = 202824096036516704121920290816'-0"		
405648192073033408243840581632.00" = 405648192073033408243840581632'-0"		
8112963841460668164876761163264.00" = 8112963841460668164876761163264'-0"		
1622592768321333632955352326528.00" = 1622592768321333632955352326528'-0"		
3245185536642667265910706531056.00" = 3245185536642667265910706531056'-0"		
6490371073285334531821413062112.00" = 6490371073285334531821413062112'-0"		
1298074214570669066364282612224.00" = 1298074214570669066364282612224'-0"		
2596148429141338132728856524448.00" = 2596148429141338132728856524448'-0"		
5192296858282676274577371089696.00" = 5192296858282676274577371089696'-0"		
10384593716565352549154421779392.00" = 10384593716565352549154421779392'-0"		
20769187433130705098308843558784.00" = 20769187433130705098308843558784'-0"		
41538374866261410196617687117568.00" = 41538374866261410196617687117568'-0"		
83076749732522820393235344235136.00" = 83076749732522820393235344235136'-0"		
166153499465045640786470688470272.00" = 166153499465045640786470688470272'-0"		
332306998930091281572941371340544.00" = 332306998930091281572941371340544'-0"		
664613997860182563144582742681088.00" = 664613997860182563144582742681088'-0"		
1329227995720365126289165485361728.00" = 1329227995720365126289165485361728'-0"		
2658455991440730252578330970723456.00" = 2658455991440730252578330970723456'-0"		
5316911982881460505156661401446912.00" = 5316911982881460505156661401446912'-0"		
1063382396576292101031332280293824.00" = 1063382396576292101031332280293824'-0"		
2126764793152584202062664560587648.00" = 2126764793152584202062664560587648'-0"		
42535295863051684041253291211755136.00" = 42535295863051684041253291211755136'-0"		
8507059172610336808250658242310272.00" = 8507059172610336808250658242310272'-0"		
17014118345220673616501316484620544.00" = 17014118345220673616501316484620544'-0"		
34028236690441347233002632969241088.00" = 34028236690441347233002632969241088'-0"		
68056473380882694466005265938483776.00" = 68056473380882694466005265938483776'-0"		
13611294676176538933201053187775552.00" = 13611294676176538933201053187775552'-0"		
27222589352353077866402106755511104.00" = 27222589352353077866402106755511104'-0"		
544451787047061557328042135110222208.00" = 544451787047061557328042135110222208'-0"		
1088903574094123114656084270220444416.00" = 1088903574094123114656084270220444416'-0"		
2177807148188246231312168844048888832.00" = 2177807148188246231312168844048888832'-0"		
435561429637649246262437768809777664.00" = 435561429637649246262437768809777664'-0"		
8711228592752984925248755376155553328.00" = 8711228592752984925248755376155553328'-0"		
17422457185505969704495111512211066656.00" = 17422457185505969704495111512211066656'-0"		
348449143710119394089902220244221333312.00" = 348449143710119394089902220244221333312'-0"		
696898287420238788179804440488442666624.00" = 696898287420238788179804440488442666624'-0"		
139379657484047757635960888977689332512.00" = 139379657484047757635960888977689332512'-0"		
2787593149680955152719321779553786624.00" = 2787593149680955152719321779553786624'-0"		
55751862993619103044386435591075733248.00" = 55751862993619103044386435591075733248'-0"		
11150372598723820608877287118151466496.00" = 11150372598723820608877287118151466496'-0"		
22300745197447641217754574236302932992.00" = 22300745197447641217754574236302932992'-0"		
44601490394895282435509148472605865984.00" = 44601490394895282435509148472605865984'-0"		
89202980789790564871018296945211731968.00" = 89202980789790564871018296945211731968'-0"		
17840596157958112974203659389043463936.00" = 17840596157958112974203659389043463936'-0"		
35681192315916225948407318778086927872.00" = 35681192315916225948407318778086927872'-0"		
71362384631832451896814637556173855744.00" = 71362384631832451896814637556173855744'-0"		
142724769263664903793629271112		

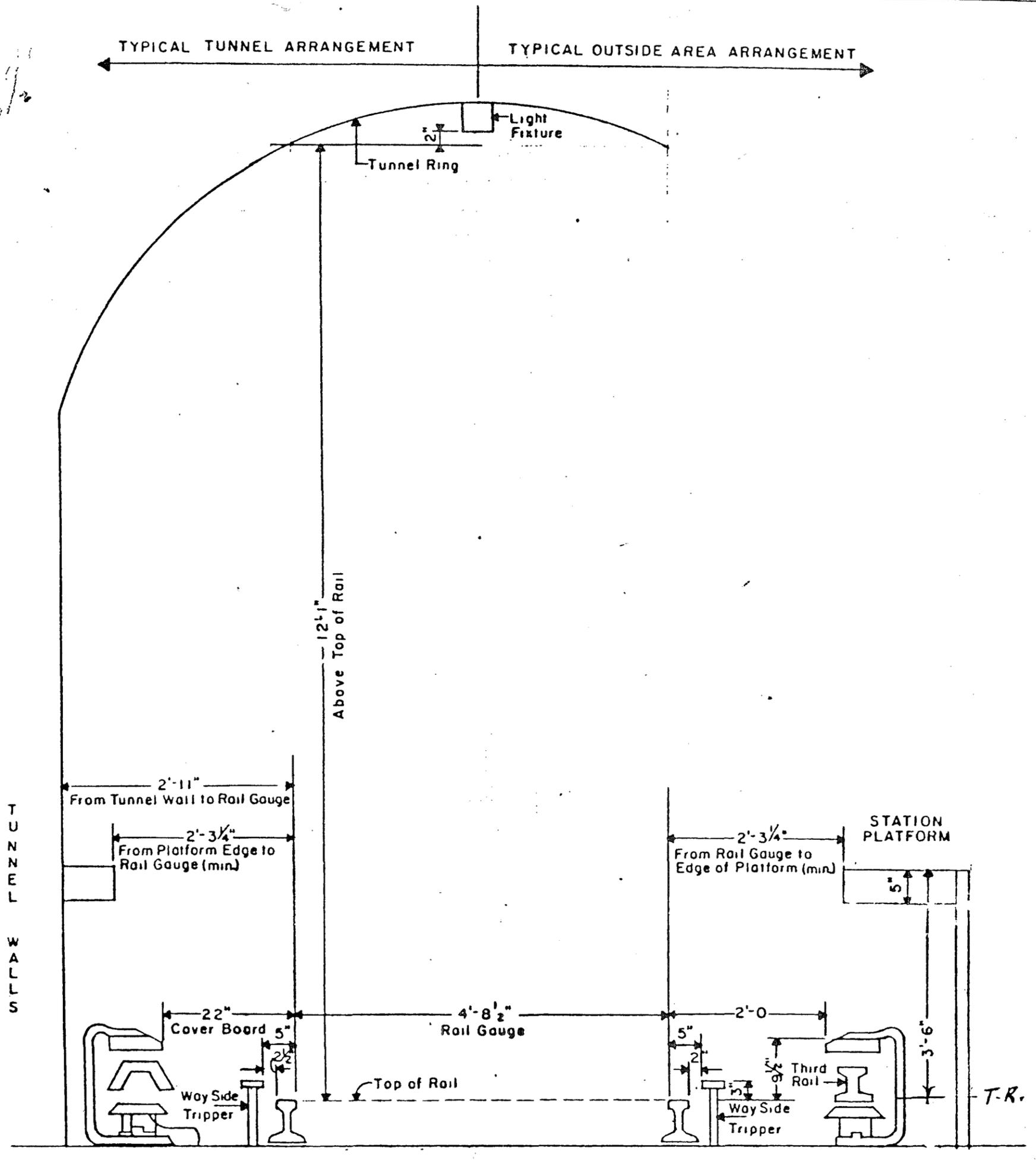


STATIC ENVELOPE
FRA CLASS 3 = 1.75"

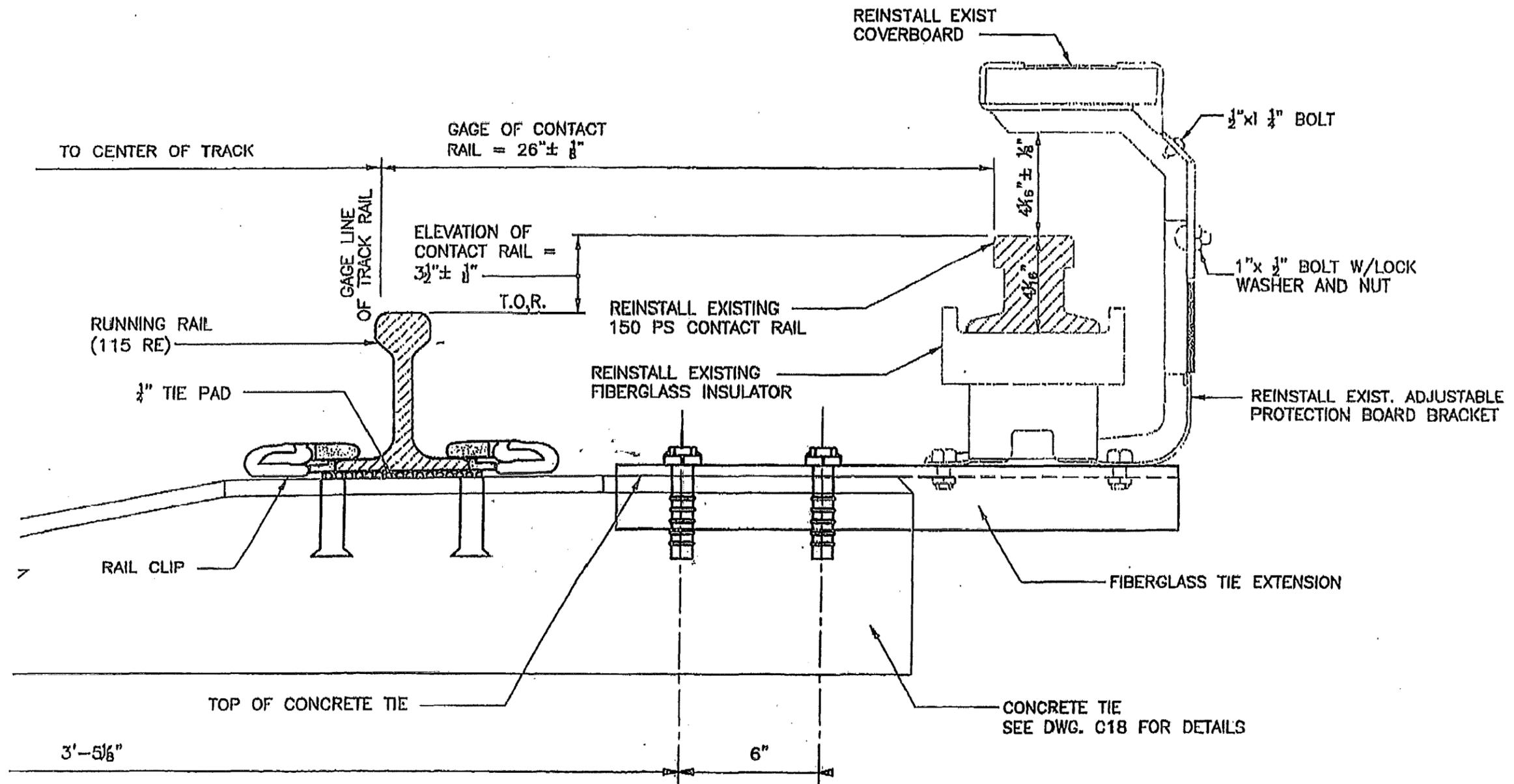
Designed by _____ Drawn by _____ Checked by _____	Discipline _____	Date _____	of _____ Worksheet Number
		Contract Number _____	Drawing Number _____
		PIID Number _____	

P-0004

3-8/2

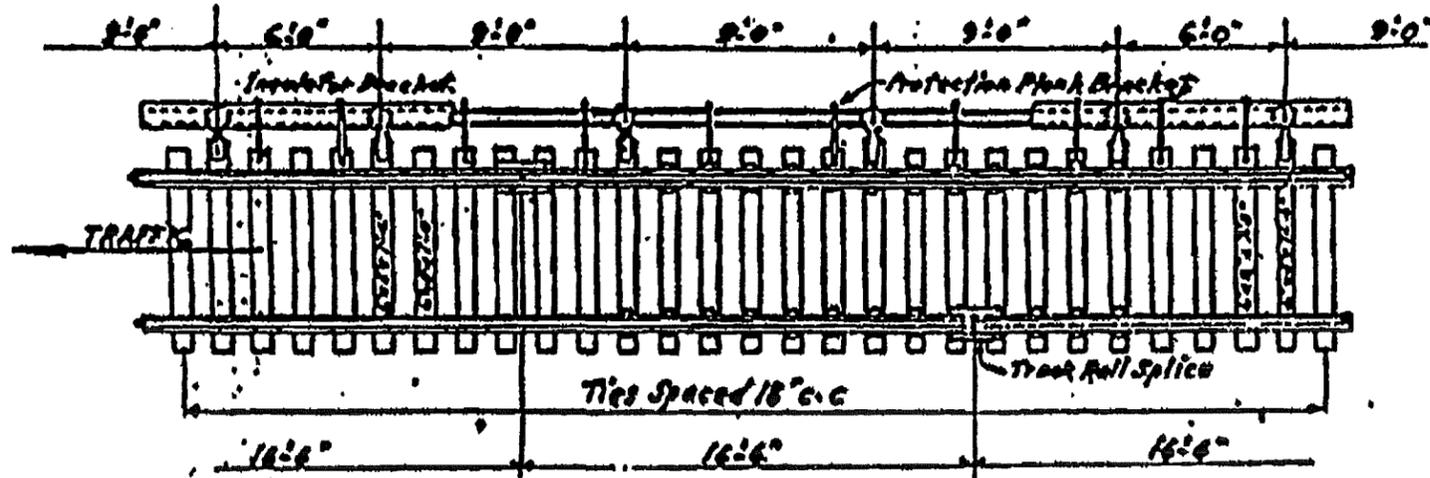


PORT AUTHORITY TRANS-HUDSON CORPORATION Track & Structures Division PATH TRACK FEATURES TUNNEL & OUTSIDE AREAS		 Dwg. No. WPS-124	Ck. by: S. W.
			Dr. by: L. A.
			Scale: 1" = 1'-0"
			Date: 5 Feb '82



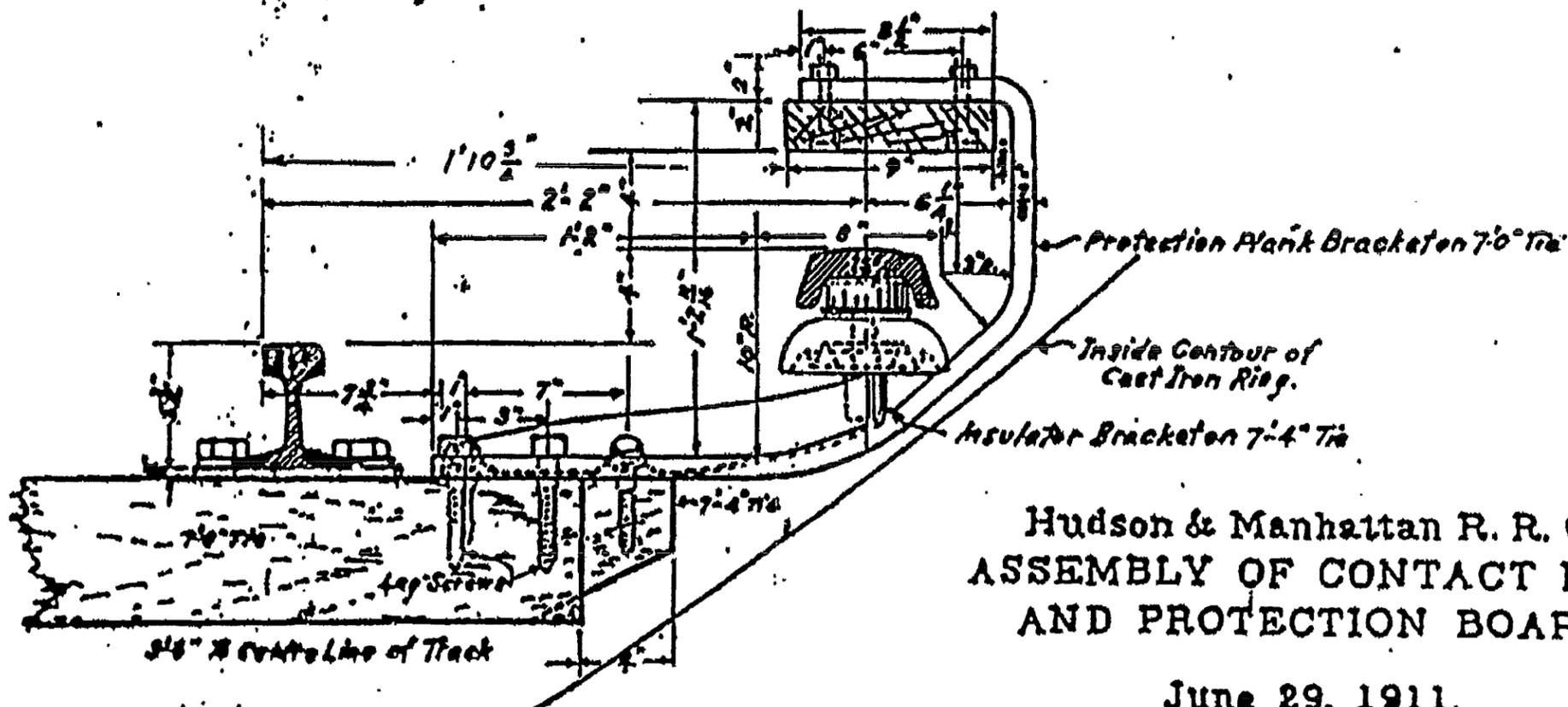
ELEVATION OF CONTACT RAIL AND PROTECTION BOARD ASSY.

N.T.S.



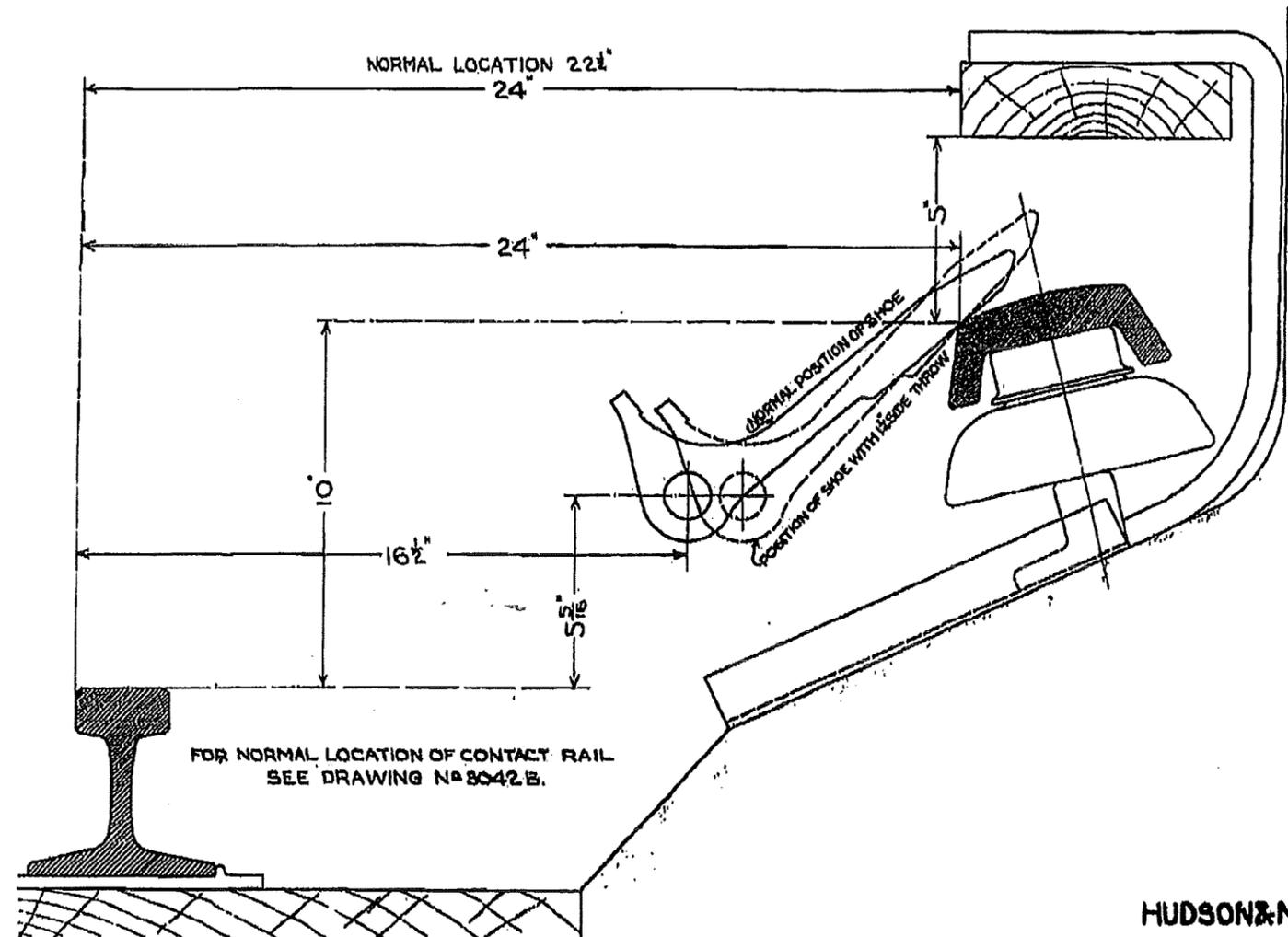
NOTE: In case must a lag No come under a Track Rail Splice.

Spacing of Insulator & Protection Plank Brackets



Hudson & Manhattan R. R. Co.
 ASSEMBLY OF CONTACT RAIL
 AND PROTECTION BOARD.

June 29, 1911.

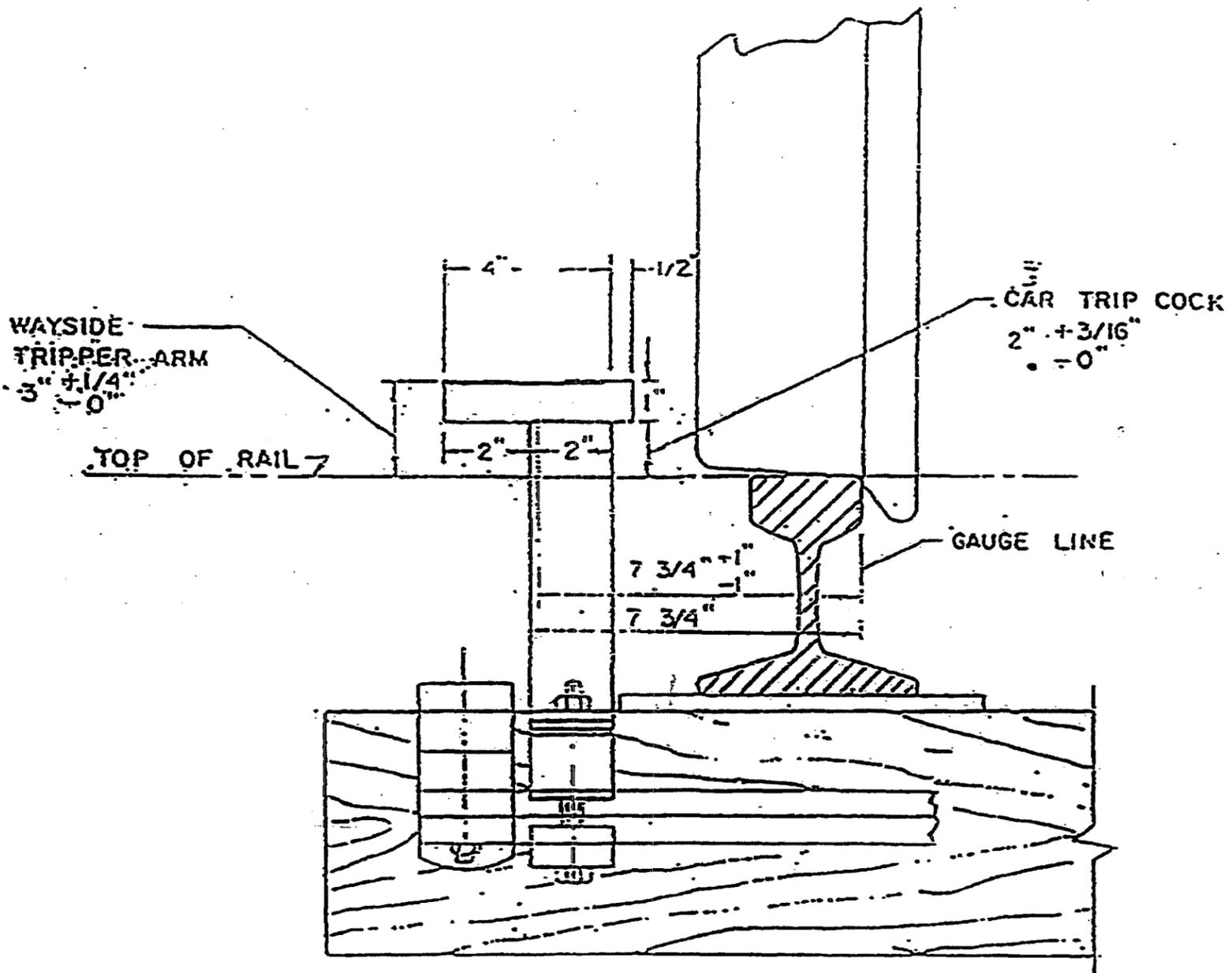


FOR NORMAL LOCATION OF CONTACT RAIL
SEE DRAWING NO 8042 B.

HUDSON & MANHATTAN R.R.CO.
LOCATION OF CONTACT RAIL
IN HIGHEST POSITION ABOVE TRACK RAIL
TUNNEL UNDER RIVER BET. STA. 1194+869 & 1191+42.8
 SCALE-HALF SIZE SEPT. 30, 1910.

NOTE:-
 TRACED FROM ELEC. DEPT'S SHEET No. C-141, JULY 29, 1910.

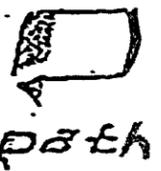
DRAWN BY E. DEPT. 2275
 TRACED - WEMMS
 CHECKED -
 CORRECT FILE NO. 93 SERIAL NO. 4486



REVIS
S 1

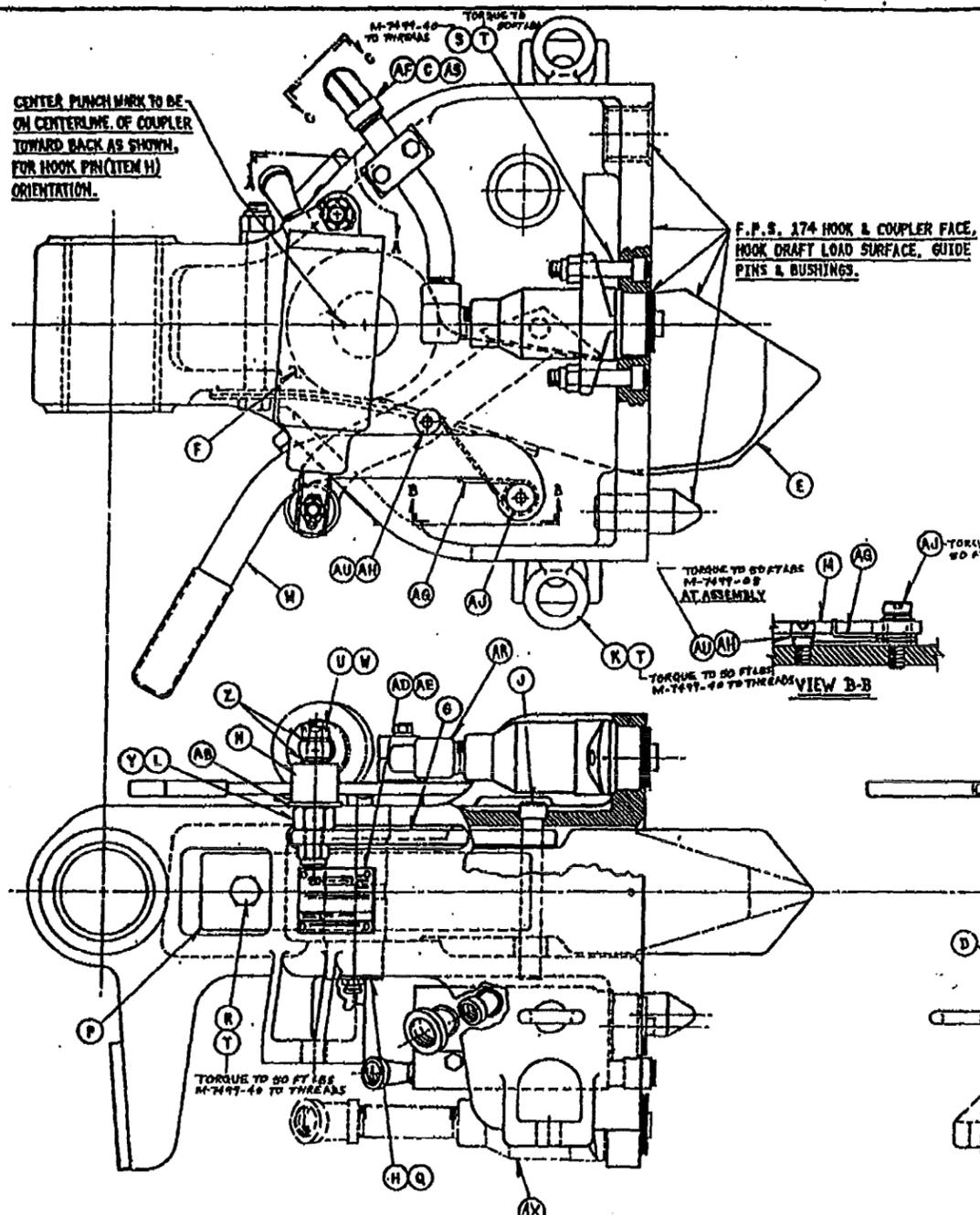
PORT AUTHORITY TRANS-HUDSON CORP.
(PATH)

AUTOMATIC TRAIN STOP TRIPPER ARM



DATE: 1-20-93

DWG. NO SK-CL 001 SHEET 1 OF 2



CENTER PUNCH MARK TO BE ON CENTERLINE OF COUPLER TOWARD BACK AS SHOWN FOR HOOK PIN (ITEM H) ORIENTATION.

F.P.S. 174 HOOK & COUPLER FACE, HOOK DRAFT LOAD SURFACE, GUIDE PINS & BUSHINGS.

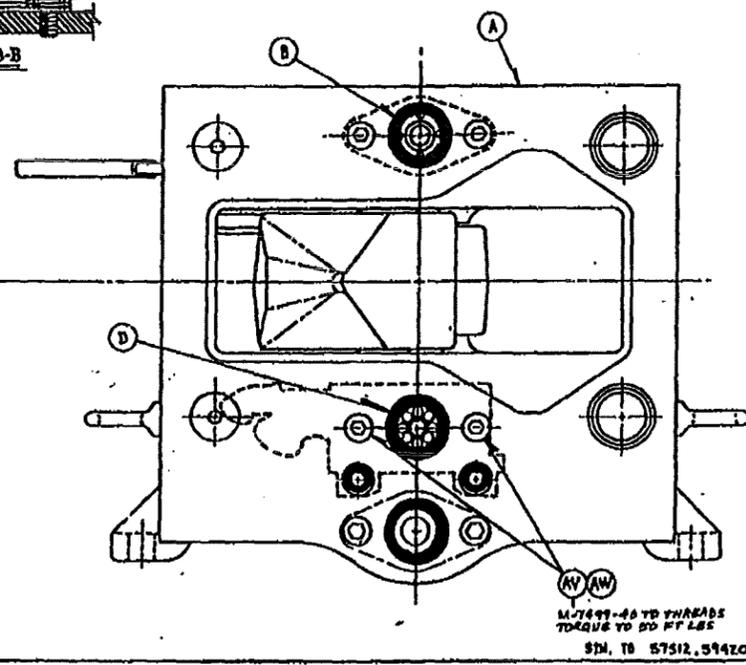
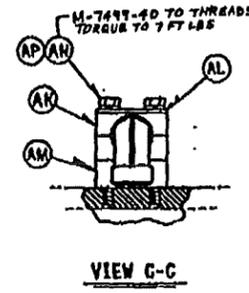
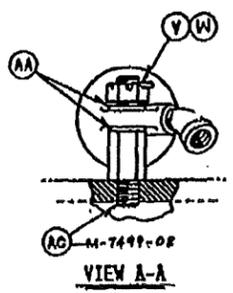
TORQUE TO 80 FT LBS AT ASSEMBLY

TORQUE TO 80 FT LBS M-7499-48 TO THREADS

TORQUE TO 80 FT LBS M-7499-48 TO THREADS

NOTE:

- 1- F.P.S. 174 SLIDING WEARING SURFACES OF CAM (IT. G), HOOK (IT. E), SPRING (IT. P), CYLINDRICAL SURFACE OF HOOK PIN (IT. W) & CYLINDER BEARINGS (IT. F).
- 2- TOUCH UP WITH M-7445-00 (BLACK ENAMEL).
- 3- M-7499-18 APPLIED TO ALL NPT (TAPERED PIPE THREADS) PNEUMATIC CONNECTIONS.



LIST OF MATERIAL		57719		
1	A	57773-3001	STL.	COUPLER HEAD SUB-ASSY
1	B	59421-3001	---	UPPER TAPPET VALVE ASSY
1	C	18-4110	STL.	1/2" BLOW-90°
1	D	59424-3001	---	BRAKE TAPPET VALVE ASSY
1	E	58443-3001	---	HOOK
1	F	59886-3007	---	UNCOUPLING CYLINDER ASSY
1	G	57761-4001	C.S.	UNCOUPLING CAM
1	H	57534-4001	STL.	HOOK PIN
1	J	57936-4001	STL.	CAM PIN
2	K	57128-4024	STL.	EYE BOLT 1/2"
1	L	57780-4002	STL.	FRONT STUD
1	M	57777-3001	---	UNCOUPLING LEVER ASSY
1	N	57760-4003	STL.	ROLLER
2	P	8481-4001	SPSTL	HOOK SPRING
1	Q	11-4318	STL.	GREASE FITTING
1	R	3-4870	STL.	BOLT 1/2" X 8-1/2"
4	S	56210-4712	STL.	SOC HD CAP SCR 1/2" X 2-1/2"
7	T	3-4049	STL.	1/2" STOPNUT
1	U	2-4759	STL.	1/2" STOPNUT
1	V	2-4810	STL.	5/8" SLOTTED NUT
2	W	3-4343	STL.	1/8" COTTER PIN X 1-3/4"
2	X	3-4344	STL.	1/8" COTTER PIN X 1-1/2"
1	Y	3-4053	STL.	5/8" STOPNUT
2	Z	3-4807	STL.	1/2" WASHER
2	AA	3-4618	STL.	5/8" WASHER X 1-1/16" D.
1	AB	3-4623	STL.	3/4" WASHER X 1-3/4" D.
1	AC	57780-4001	STL.	REAR STUD
1	AD	59042-4001	MJM.	NAMEPLATE
1	AE	57219-4001	STL.	ORIPHAEL STUD
1	AF	57598-4001	STL.	1/2" PIPE NIPPLE
1	AG	57787-4001	STL.	LEVER SPRING
1	AH	57780-4007	STL.	SPACER
1	AJ	24-4434	STL.	SOC HD SHOULDER SCR 1/2"
1	AK	57537-4001	PLAS.	PIPE CLAMP
1	AL	57537-4002	STL.	CLAMP COVER
1	AM	57780-4006	STL.	3/4" SPACER
2	AN	1-4572	SSY	1/4" BOLT X 2-3/4"
2	AP	18779-4025	STL.	1/4" LOCKWASHER
1	AQ			
1	AR	10-4107	STL.	3/4" X 1/2-20" STREET ELBOW
1	AS	8-4091	PLAS.	CAPLUM-1/2 NPT
1	AT			
1	AV	56210-4701	STL.	SOC HD CAP SCR 1/2" X 1"
2	AW	56210-4713	STL.	SOC HD CAP SCR 1/2" X 1-3/4"
2	AX	18779-4046	STL.	1/2" LOCKWASHER
1	AY	59421-3002	---	LOWER TAPPET ASSY

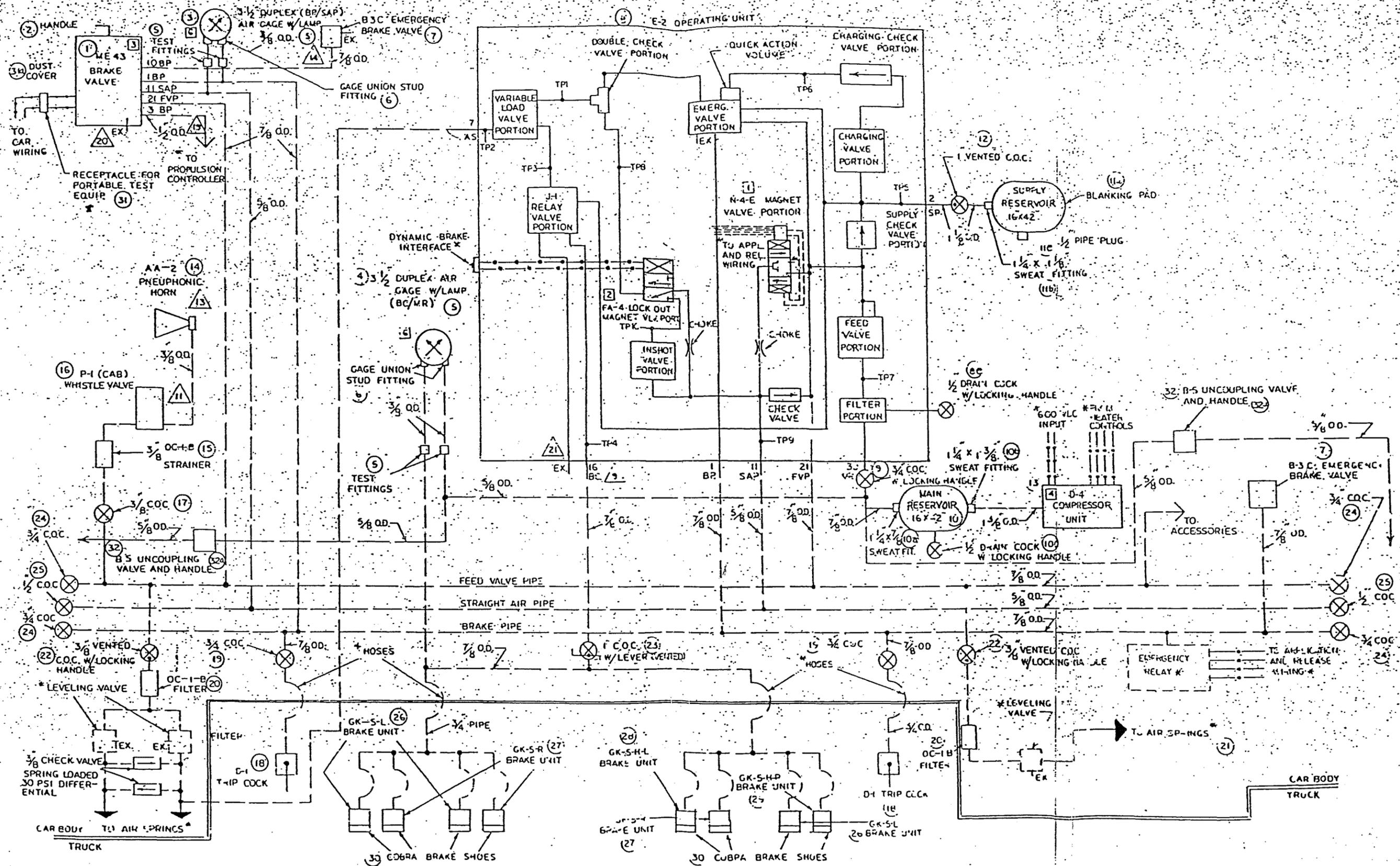
SOUL	DATE	BY	CHKD

WALSCO Forming Division
 THE DRAWING CONTAINS PROPRIETARY INFORMATION OF WALSCO, P.T.D. AND SHALL NOT BE REPRODUCED OR TRANSMITTED TO OTHERS IN WHOLE OR IN PART WITHOUT WRITTEN CONSENT OF THE COMPANY.

57724

COUPLER HEAD ASSEMBLY 57719

FORM 0201



PATH PA-4 "RT-2" BRAKE EQUIPMENT — ELECTRICAL & PIPING DIAGRAM (DA-85248-1) Sheet 1 of 2

P-0012-A

IMPORTANT

1. DRAWING REPRESENTS RECOMMENDED COMPONENTS AND PIPE ARRANGEMENTS. THE CHOICE OF BRAKE DEVICES AND THE INSTALLATION OF THE COMPONENTS, PIPING, WIRING, AND SYSTEM CHECK OF THE TOTAL BRAKE FUNCTION IS THE RESPONSIBILITY OF THE CAR BUILDER AND/OR USER.
2. ITEMS AND STATEMENTS SHOWN IN ASTERISKED (*) AND DASH DOT LINES ARE SHOWN FOR REFERENCE PURPOSES ONLY. NONE OF THESE ARE SUPPLIED BY WABO AND WABO WILL NOT BE RESPONSIBLE FOR THEIR INSTALLATION AND/OR THEIR PERFORMANCE.
3. THIS DRAWING DA85248-1 SHEETS 1 AND 2 MUST BE USED IN CONJUNCTION WITH MATERIAL LIST 77-PATH-244A.
4. BRAKE EQUIPMENT PIPE BRACKET MANUFACTURED OF AAG061-T6 AND ALCOA #356 ALUMINUM, COATED WITH A CHEMICAL FILM TREATMENT (ALLODINE). NO METALS SHALL BE PUT IN CONTACT WITH OTHER METALS SUCH THAT WITH THE CONTACT, GALVANIC CORROSION OCCURS. WHERE IT IS NECESSARY THAT ANY COMBINATION OF DISSIMILAR METALS BE ASSEMBLED, ALL SURFACES OF CONTACT MUST BE SEALED WITH NON-CONDUCTIVE FILMS (TEFLON TAPE) OR PLASTIC CEMENT (BITUMINOUS) OR SEPARATED BY OTHER INERT MATERIAL.

5. ELECTRICAL AND PIPING DIAGRAM LEGEND.

- △ REFERENCE PNEUMATIC NOTES
- REFERENCE ELECTRICAL NOTES
- REFERENCE ITEMS ON MATERIAL LIST
- ELECTRICAL ITEMS NOT SUPPLIED BY WABO
- — — PNEUMATIC PIPING NOT SUPPLIED BY WABO
- * NOT SUPPLIED BY WABO

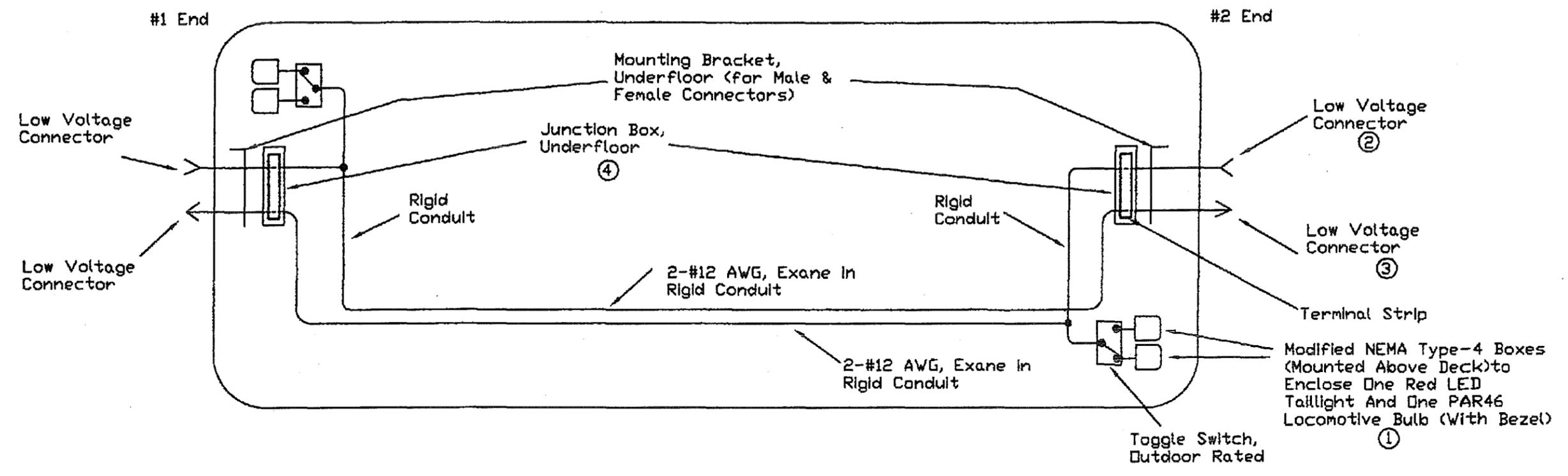
PNEUMATIC

1. ALL PIPE DIMENSIONS SHOWN TO BE O.D. "L" TYPE COPPER TUBING, UNLESS OTHERWISE STATED.
2. ALL PIPE TO WABO SUPPLIED EQUIPMENT THAT IS NOT DIMENSIONED, IS TO BE 1/2 INCH O.D. "L" TYPE COPPER TUBING.
3. PIPE DIMENSIONS FOR DEVICES NOT SUPPLIED BY WABO ARE TO BE PER BUILDER SPECIFICATION.
4. ALL TUBING AND IRON PIPE ARE SHOWN AS AMERICAN STANDARD SIZE. REFERENCE U.S. NATIONAL BUREAU OF STANDARD HANDBOOK H 28.
5. CAR PIPING MUST BE CLEAR OF ALL CONTAMINATION AND DEBRIS BEFORE INSTALLATION OF EQUIPMENT.
6. COPPER FITTING SOLDER JOINTS TO BE MADE USING NON-CORROSIVE SOLDERING FLUX AND AUTHORITY APPROVED SOLDER.
7. DO NOT SWEAT ADAPTER COUPLINGS WHILE IN PLACE ON OPERATING UNIT PIPE BRACKET. HEATING WILL DAMAGE PIPE BRACKET CEMENT.
8. HOSES DESIGNATED BY 180° DASHED ARC ARE NOT PROVIDED BY WABO.
9. EQUIVALENT PIPE LENGTH FROM E-2 OPERATING UNIT TO THE TRUCK PIPING MUST BE KEPT TO A MINIMUM.
10. BRANCH PIPE LENGTH MUST NOT EXCEED SIX (6) EQUIVALENT FEET OF PIPING.
11. EQUIVALENT PIPE LENGTH FROM HORN TO P-1 WHISTLE VALVE MUST BE KEPT TO A MINIMUM.
12. TEST FITTINGS MUST BE ACCESSIBLE.
13. WABO SUPPLIED HORN SHOULD BE POINTED IN THE DIRECTION THE SOUND IS REQUIRED AND SHOULD BE LOCATED IN AN AREA WHERE THERE WILL BE NO OBSTRUCTION THAT WILL DEFLECT THE SOUND WAVES. THE HORN SHOULD BE LOCATED FREE FROM FLYING BALLAST AND WATER SPRAY OR SPLASH.
14. LENGTH OF PIPE FROM ME-43 BRAKE VALVE TO B-3-C EMERGENCY VALVE NOT TO EXCEED 13 FEET IN LENGTH WITH NOT MORE THAN ONE 90° ELBOW.
15. ALL PNEUMATIC COMPONENTS SHOULD BE SHIELDED FROM WHEEL SPRAY. ALL PNEUMATIC VENTS (EX) MUST BE LOCATED SO THAT WHEEL SPRAY, SPLASHING, AND CAR WASH SPRAY IS NOT DIRECTED AT THESE VENTS.
16. ALL PIPING AND FITTINGS SHOULD BE ARRANGED SO THAT MOISTURE IS NOT DIRECTED TO OR TRAPPED BY WABO SUPPLIED PNEUMATIC BRAKE CONTROL EQUIPMENT.
17. TREAD BRAKE UNIT DETAILS INCLUDE A BRAKE SHOE KEY WITH EACH UNIT. MOUNTING BOLTS FOR TREAD BRAKE UNITS ARE NOT PROVIDED IN THIS PROPOSAL AND MUST BE FURNISHED BY THE TRUCK SUPPLIER OR CAR BUILDER.
18. RESERVED
19. #3 LINE SHOULD BE A MAXIMUM OF 4 FEET OF 1/2 O.D. TYPE L COPPER TUBING.
20. THE ME-43 BRAKE VALVE EXHAUST SHOULD BE PIPED AWAY FROM THE CAB AREA.

ELECTRICAL NOTES

1. APPLICATION AND RELEASE MAGNET VALVE PORTION (N-4-E).
 - A. CONNECTION TO BE MADE WITH CAR BUILDER SUPPLIED CA3106A-20-175-F80 CONNECTOR (WABO PC. 588952).
 - B. VALVE TO OPERATE BETWEEN 22* AND 44* VDC ON THE VEHICLE.
2. LOCKOUT MAGNET VALVE PORTION (FA-4).
 - A. CONNECTION TO BE MADE WITH CAR BUILDER SUPPLIED CA3106A-18-105-F80 CONNECTOR (WABO PC. 588955).
 - B. VALVE TO OPERATE WITH 21.7* TO 137.5* VDC APPLIED ON SOURCE SIDE OF 1 OHM VARIABLE SERIES RESISTOR.
 - C. DROP OUT CURRENT TO BE NOT LESS THAN .060 AMPS.
3. ME-43 BRAKE VALVE CONTACTS ARE RATED MAXIMUM AT 750 VOLT-AMP.
4. D-4 COMPRESSOR UNIT
 - A. THE CIRCUIT BREAKER OR FUSE TRON FOR THE COMPRESSOR CIRCUIT MUST HAVE A CONTINUOUS RATING OF 15 AMPS IN ACCORDANCE WITH ANSI C37.16. THIS MUST BE FURNISHED BY THE CAR BUILDER.
 - B. CONNECTION TO HEATER ELEMENTS MADE WITH WABO SUPPLIED CONNECTORS, CA-3106F-10SL-45-F80 (WABO PC. 588607) FOR THE DRAIN VALVE, AND THE AIR DRYER.
 - C. COMPRESSOR MOTOR TO OPERATE BETWEEN 400 AND 700 VDC.
 - D. RESERVED.
 - E. HEATERS TO OPERATE BETWEEN 22* TO 44* VDC ON THE VEHICLE.
 - F. 600 VDC CONNECTOR-POSITIVE LEAD TO BE CONNECTED TO PIN #A* AND THE NEGATIVE LEAD TO PIN #B* TO THE WABO SUPPLIED CONNECTOR (CA3106A-22-85-F80) WABO PC. 588956.
 - G. AIR COMPRESSOR IS SHIPPED WITHOUT OIL AND IS NOT TO BE RUN UNTIL PROPER OIL LEVEL IS ATTAINED WITH OIL MEETING WABO'S MATERIAL SPEC. M-7616-20. CRANKCASE CAPACITY IS APPROXIMATELY 10 QTS. (9.46 LITERS).
 - H. THE MOTOR CARRIAGE RESTRAINTS MUST BE RELEASED PRIOR TO OPERATING THE AIR COMPRESSOR.
 - I.
5. THIS DRAWING IS TO BE USED IN CONJUNCTION WITH ELECTRICAL INTERFACE DOCUMENT EA1691-501 AND WIRING DIAGRAM DA85248-21, LATEST REVISION.
6. DUPLEX AIR GAGE (LAMPS)
 - A. CONNECTION TO BE MADE TO TERMINAL BOARD WITH #6 RING TERMINALS: 1(+), 3(-)
 - B. OPERATE AT 22-44 VDC

- Notes:
- ① LED Taillight, PAR 46, Red; Luminator #110103001; Locomotive Bulb, 150PAR46, GE#19512.
 - ② Male Plug, NEMA Config. 5-15P, 15 Amp, 125V, 3 Wire, single Phase; Leviton #5266C, or Approved Equal.
 - ③ Female Receptacle Housed in: Weatherproof Single Outlet box (Cooper/Crouse-Hinds # TP7074, or approved equal) and Weatherproof Outlet Cover With Self-closing Cover (Cooper/Crouse-Hinds #TP7214, or approved equal).
 - ④ Stainless Steel Junction Box, NEMA Type-4 (Wiegmann/Hubbell #BN4100604CHWW)



P-0013

Flatcar Electrical Circuit

Audit Department Controls Requirement Contract Checklist

General

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

System/Security Administration

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

Hardening of operating system/database that supports the application:

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

License Management

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

Logical Access Controls

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

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

Password Controls

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

Application Controls

Data Validation & Input Controls

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

Data Retention and Management

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

Data Integrity and Security

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

Application Interfaces

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

Processing Controls

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

Change Management

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

Application Logging, Audit Trails and Record Retention

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

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

Contingency Planning, Disaster Recovery and Backup Management

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

Performance Monitoring

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

Patch Management

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

Physical Protection

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

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

Anti-virus/Malware/ Integrity/Vulnerability Software Management

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

Wireless Device

- Devices should be using WPA2 WPA enterprise (802.1x protocols) and AES encryption or better.
- Devices should disallow broadcasting of the SSID.
- All default parameters should be changed.
- Devices should have MAC address filtering enable or some type of authentication mechanism in place.

Web Application Vulnerabilities and Controls

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

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

Credit Card Processing Checklist

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

Disaster Recovery

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



THE PORT AUTHORITY OF NY&NJ

Technology Department

TECHNOLOGY STANDARDS FOR THE PORT AUTHORITY

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

Revised December 2015

Table of Contents

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

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

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

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

FOR REFERENCE

Introduction

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

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

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

1.0 The Port Authority Wide Area Network (PAWANET)

1.1 PAWANET Overview

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

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

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

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

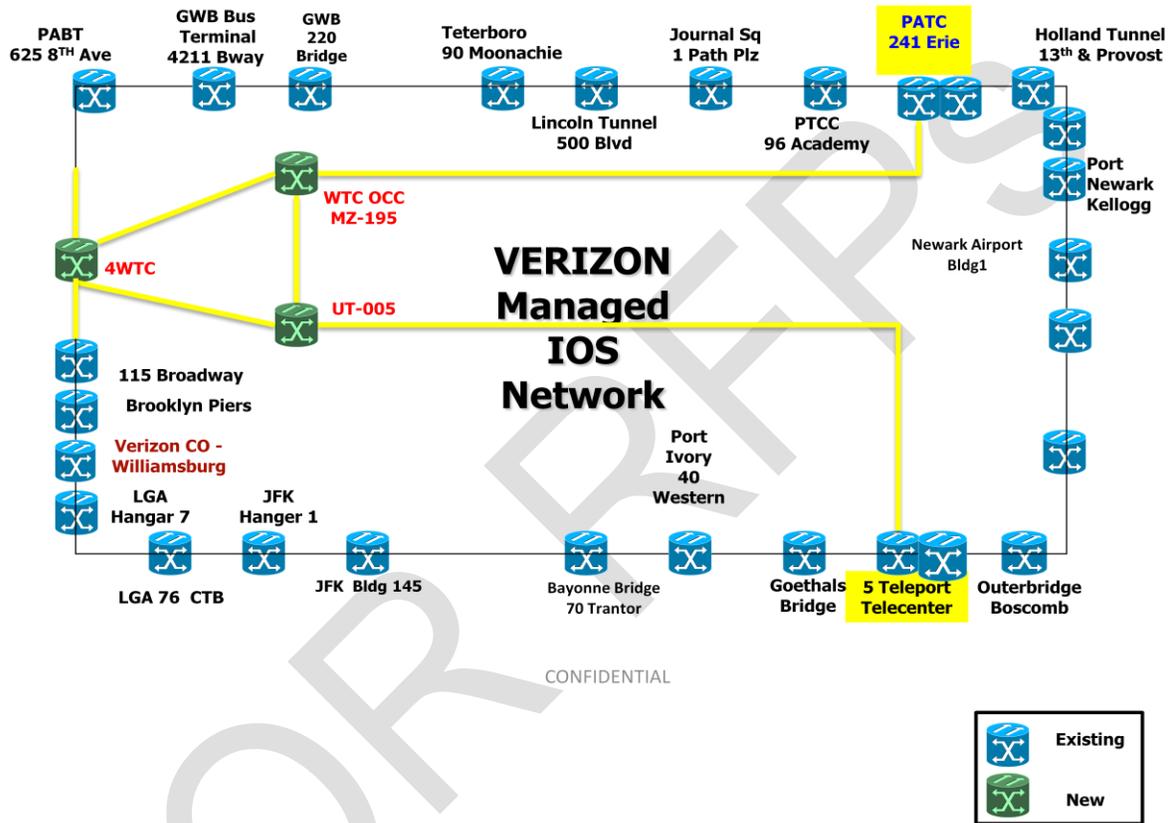
The network consists of state-of-the-art Cisco Systems equipment and services, such as, high performance Cisco Catalyst switches and routers. The Port Authority uses a managed Network Monitoring Services to monitor PAWANET, and Cisco Systems SMARTnet hardware/software maintenance services, and Cisco's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

1.2 PAWANET Circuit Diagram

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

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

The new design will replace the current PAWANET Circuit Diagram.



1.3 Inter-site Services Providers

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

- AT&T Local Services
- Verizon

1.4 PAWANET Functions

Currently PAWANET is used to transport the following:

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

1.5 Features of PAWANET

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

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

1.6 Supported Protocols

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

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

1.7 PAWANET Switches and Routers

The current standard switches and routers used on PAWANET are:

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

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

1.8 Approved Servers

Only IBM servers may be connected to PAWANET.

This includes turnkey, distributed systems, where Application servers are being used. Any replacement servers must be IBM servers. Deviation from this policy will not be allowed without prior approval of the Chief Technology Officer or their designee.

1.9 Enterprise Addressing Scheme (including IP addressing)

The Port Authority's enterprise network is a TCP/IP Class B network allowing for a maximum of 255 subnet assignments. Subnets are assigned on a geographical basis according to the number of resources required. Workstations are configured for dynamic assignment of IP addresses via Dynamic Host Configuration Protocol (DHCP).

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

1.10 Enterprise Network Monitoring Software

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

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

2.0 Network Resources

2.1 Network Overview

The Port Authority has a modern distributed computing network, which is managed as an Enterprise resource. The network connects all individual PCs, servers, printers, and other devices in a unified computing infrastructure that makes it possible for the Port Authority to conduct its business.

The Enterprise Network consists of the PAWANET (see Section 1.1) and connected Local Area Networks (LAN's). The line of demarcation between the cable and wiring is the responsibility of the carrier and the Port Authority's area of responsibility is usually a wiring closet. The Port Authority's Enterprise Network consists of the following components on the Port Authority side of demarcation:

Enterprise Devices

- Cabling
- Routers
- Switches

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

LAN Devices

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

2.2 Enterprise Network Architecture

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

2.2.1 Server Operating System and Software

All Enterprise servers in the Port Authority are currently based on the Windows operating system. Microsoft Windows, RedHat Linux servers, and Sun Solaris are supported as application servers when required for functionality.

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

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

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

2.2.2 Configuration

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

2.2.2.1 Drive Mapping Conventions and Organization

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

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

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

Share folder. Access will be restricted through the use of Windows file and folder security permissions and access will be granted through the use of groups. These groups will be named using the same name as the folder name.

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

Example P:\APPS\Psoft

2.2.2.2 Connecting LAN Devices to the Enterprise Network

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

2.2.3 Network Resources Security

2.2.3.1 Server Physical Security

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

2.2.3.2 Server Logical Security

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

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

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

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

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

2.2.4 Network Access and User Account Security

2.2.4.1 Account Creation

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

2.2.4.2 Time Restrictions

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

2.2.4.3 Concurrent Logins

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

2.2.4.4 Login Management

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

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

2.2.4.5 Password Management

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

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

Examples of safe passwords:

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

Choose a password using a phrase:

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

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

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

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

Passwords are considered confidential data. They protect the Port Authority's network resources and grant system privileges and access. Disclosure may result in unauthorized access to data, system files and transactions. Passwords are also your signature and identify you as the individual who is responsible for the system activity.

2.2.4.6 Modems and Switches

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

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

2.2.5 Remote Access System

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

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

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

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

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

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

2.2.6 Hardware Standards

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

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

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

2.2.6.1 Standard Servers

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

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

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

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

2.3 Network Naming Conventions

2.3.1 Server Names

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

2.4 Directory Services and Structure

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

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

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

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

Scheduling of distributions is performed in conjunction with client departments.

2.5 System Backup and Recovery

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

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

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

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

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

2.5.1 Backup Logs

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

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

2.5.2 Backup Scheduling

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

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

2.6 Business Resumption Plan

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

2.7 Telecommunications Standards for Enterprise Network Resources

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

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

2.7.1 Closet and Telecommunications Room Access

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

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

2.7.2 Telecommunications Installation Contractor's Responsibilities

1. Adherence to all of the above specifications
2. Assurance of labor harmony
3. The contractor must supply all cable, blocks, brackets, connectors, jacks, housings, face

plates, special tools, etc., as necessary to perform an installation which is satisfactory to the Port Authority.

4. The contractor must label every workstation (jack faceplate) and the corresponding cross connect point (punch down block or patch panel) in accordance with the cable identification management plan, as previously described.
5. Install all Category 5e/6 cabling in the proper manner, with the appropriate number of twists, to maintain Category 5e/6 integrity and capabilities, as outlined in the TIA/EIA 568-B.2 standard.
6. The contractor must ensure that cable connections are in accordance with standard telecommunications practices and that all cabling maintains normal connectivity and continuity.
7. All materials must be agreed upon by PA Network Services prior to the start of installation.
8. All computer or network communication rooms and closets are to be isolated, locked, and secured. No other equipment, storage area, or smoking area are to be located in this room. This room must provide appropriate cooling and ventilation. Access to this room will be reserved to TEC staff and an agreed upon Facility Manager or designee of the site where the PAWANET equipment is located. This procedure is to ensure the security and the integrity of the Port Authority's computer network and its users.

2.7.3 Electrical Requirements

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

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

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

2.7.4 Telephone Company Interface

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

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

2.8 Documentation

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

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

3.0 Virus Scanning & Management

3.1 Overview

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

3.2 Standards

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

3.3 Acquisition and Installation

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

3.4 Virus Detection and Response

The Technology Department is responsible for responding to all virus outbreaks, as well as eradicating them and, where possible, preventing them.

The speedy reporting of all computer viruses is essential for the protection of the information stored on Port Authority LANs. Much of that information is important to the safety of the public, as well as the day-to-day business of the PA.

If the anti-virus software has detected a virus and cleaned it, no further action is required on the end user's part. If the virus is not cleaned, or the end-user suspects that a virus still exists, the end-user should immediately contact the Customer Support Desk, and they will work to remove the virus. The Technology Department will respond quickly to all such alerts by doing the following:

Assess the risk

- Confirm the existence of a virus.
- Take appropriate measures to quarantine the virus so that it does not infect other Port Authority devices.

Notify Appropriate Parties

- Contact the originating party who introduced the virus to the Port Authority.
- If it is a new virus, contact our antivirus vendor, McAfee, for further assistance.

Remove the virus

- Work with appropriate parties until the virus is removed.

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

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

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

4.0 Electronic Mail

4.1 E-Mail Overview

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

4.2 E-Mail System Architecture

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

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

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

4.3 E-Mail Environment: Design Considerations and Infrastructure

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

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

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

4.4 Integrating Applications Server with Port Authority Email System

4.4.1 Requesting SMTP Services

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

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

4.4.2 Email Restrictions

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

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

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

5.0 Intranet

5.1 Intranet Overview

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

Examples of business information hosted on eNet include:

- Departmental Websites
- Directories
- Corporate Announcements
- Reference Materials
- Document Collections
- Library Services
- News Displays
- Enterprise and Departmental Applications

5.2 Direction of eNet Development

eNet is intended to provide a convenient, timely and accurate source of information for Port Authority employees as well as providing access to enterprise and departmental applications. The owner of content on eNet is responsible for authorizing its publication, its accuracy and timeliness. Technology Services provides a common infrastructure and technical support for those departments that electronically publish agency information or make available electronic resources. Infrastructure standards are recommended to ensure compatibility and facilitate maintenance. Departments requesting specific applications should discuss their requirements with eNet staff to determine a solution that best meets the department’s business needs.

5.3 eNet Software Infrastructure Standards

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

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

5.3.1 Design Standards

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

Departmental Web Site Standards

Prescribed standards are assigned to only the following items:

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

5.3.2 Accessibility Standards

TEC's eBusiness Unit is committed to making all eNet content accessible to persons with disabilities. In order to ensure that all eNet web content is in compliance with accessibility standards and applicable legal requirements, contact the Webmaster via email at webmaster@panynj.gov, or call 212-435-3294.

6.0 Workstation Hardware and Operating System Software

6.1 Overview

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

6.2 Workstation Operating System Standard

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

- Microsoft Windows 7, Enterprise
- Apple OS X

6.3 Workstation Configuration

6.3.1 Workstation Naming Conventions

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

Example: Workstation name: 23AAH86

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

6.3.2 Automated Software Distribution for Computers

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

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

6.3.3 Remote Workstation Management

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

6.3.4 Drive Mappings

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

6.3.5 Standard Workstation Hardware Configurations

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

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

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

6.3.6 Standard Workstation Software

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

6.3.6.1 Standard Workstation Software

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

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

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

6.3.7 Enterprise Software

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

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

6.3.8 Other Business Applications

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

Current list of Enterprise applications, is shown below –

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

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

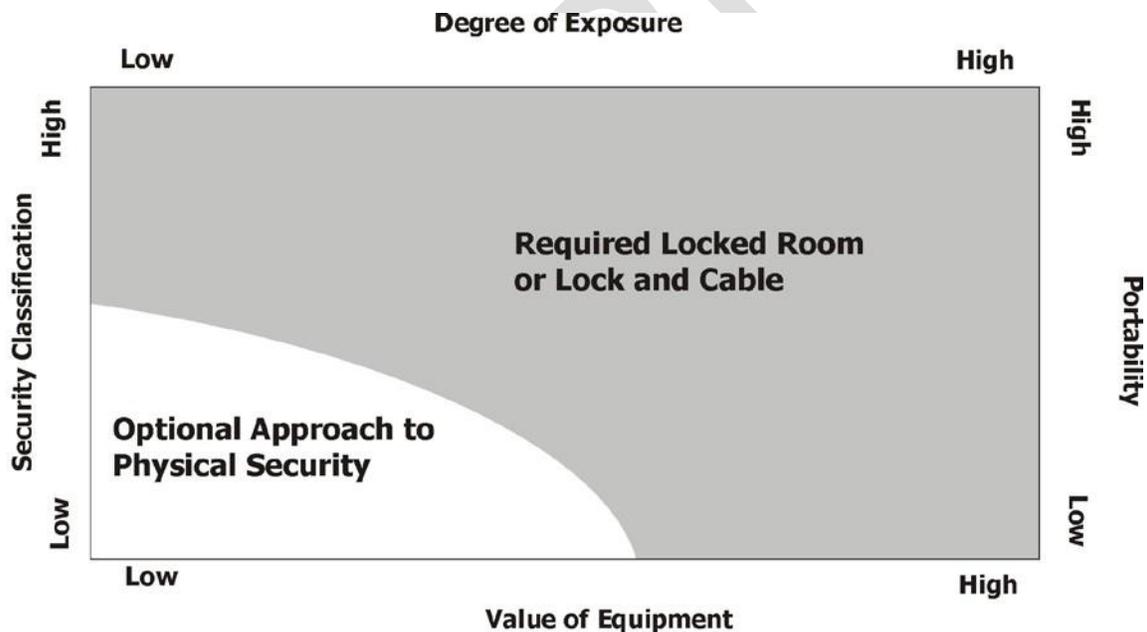
6.4 Workstation Security

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

6.4.1 Physical Security

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

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



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

6.4.2 Logical Security

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

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

7.0 Distributed Systems Environment

7.1 Overview

A number of enterprise servers provide critical application and system services. Different operating systems and configurations may be required for specific applications. This section provides information on the standards for supported systems within the Port Authority.

7.2 Microsoft Windows Servers

The standard for general-purpose application servers and File and Print Computing is IBM servers. Microsoft Windows 2008 Server (Enterprise) and 2012 Server are currently supported Operating Systems for application servers.

7.2.1 Virtual Environment

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

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

7.2.2 Windows Data Encryption

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

7.3 Unix

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

7.3.1 Unix Security

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

7.3.2 Backup

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

7.3.3 Download Scripts in the Unix/Linux Environment

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

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

7.4 z/OS

z/OS (currently release 1.5) is the IBM-supplied operating system on the IBM 2096-R07. This hardware/software supports multiple users and multiple applications. Provided on this platform for transaction-processing applications are TSO/E, ISPF, and CICS. The database is DB2, although other file structures are also supported. The Agency is dis-investing from this operating system and it will not be used to support additional applications.

7.4.1 Databases

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

7.4.2 Geographic Information System

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

7.5 Application Security

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

7.6 Server Physical Security

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

7.7 Load Balancing – Failover Architecture

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

8.0 Vendor Provided Dedicated Systems

8.1 Overview

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

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

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

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

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

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

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

8.2 Physical Security Technology Standards

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

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

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

The standard will also improve:

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

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

8.2.2 Situational Awareness Platform Software

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

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

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

8.3 Communications Infrastructure Standards

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

This standard applies but is not limited to; Layer 2 and 3 Ethernet switches, Routers, Wireless Access Points (WAP), Mobile Access Routers (MAR), GIG E (Gigabit Ethernet) switching and networking and SONET (Synchronous Optical NETWORK) equipment. Deviation from this standard requires the written consent of the CTO.

8.4 Server Infrastructure Standard

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

Technology Department has contracted discounted pricing with our service provider for its servers and hardware support. In order for the agency to take full advantage of these savings, any new Application servers or File & Print servers must be built using IBM hardware purchased by TEC. This includes turnkey and distributed systems where File & Print or Application servers are specified in the design. Any replacement File & Print or Application servers must be IBM servers. Deviation from this policy will not be

allowed without prior approval of the CTO or his designee.

9.0 Wireless Technologies

9.1 Wireless Standards

9.1.1 Purpose and Scope

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

9.1.2 General Policy

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

9.1.3 Personal Area Networks - PAN

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

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

9.1.4 Wireless Local Area Networks – WLANs

9.1.4.1 Overview

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

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

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

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

9.1.4.2 Scope

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

9.1.4.3 Principles

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

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

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

9.1.4.4 Compliance Requirements

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

9.1.4.5 Device Specifications

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

9.1.4.6 Access Point (AP) Standard

Standards Details:

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

9.1.4.7 Best Practice

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

WLAN Best Practices Add-ons:

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

Wireless Control System (WCS):

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

9.1.4.8 Portable Electronic Devices (PEDs) – Cell Phones, PDAs, messaging devices, laptops and tablets

If a device receives information via a wireless technology, and that device allows that information to be placed directly into the corporate network at the workstation level, then all perimeters and host-based security devices have been bypassed. Therefore, the following procedures apply:

- PEDs connected directly to a PA wired network via a hot sync connection to a workstation is not permitted to operate wirelessly at the same time. Wireless solutions could create 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 are required on devices and workstations that are used to synchronize/transmit data, if available. Where not available on a device, disable the synchronization capability or provide server or workstation based handheld anti-virus protection.
- PEDs are easily lost or stolen therefore approved file system/data store encryption software is required.
- PEDs need to be capable of being erased or overwritten to protect data. If the device is no longer needed and cannot be erased or overwritten, it must be physically destroyed.

9.1.4.9 Cellular and Wireless Email

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

- Must have end-to-end encryption.
- PC based redirectors are not allowed as it requires the PC to be active at all times only server based redirectors will be used.
- The use of LANS and Wireless transmitters, i.e. Bluetooth etc. by PANYNJ personnel using PANYNJ equipment is strictly prohibited

9.1.4.10 Synchronization

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

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

9.1.4.11 Responsibilities of Technology Department

- Monitor and provide oversight of all PA wireless activities, insure interoperability of wireless capabilities across the agency.
- Develop appropriate technical standards for secure wireless and handheld solutions.
- Establish a formal coordination process to ensure protection of PA information with PA information systems employing wireless technologies.
- Review and evaluate wireless technologies, products, solutions that meet PA requirements.
- Identify approved monitoring mechanisms for wireless devices to ensure compliance with policy.
- Periodically review approved wireless technology standards and procedures to ensure products and solutions remain compliant.
- Support risk management activities associated with evaluating wireless services
- Act as central coordination point and final approval authority for any exceptions to this policy.
- Define or approve acceptable wireless devices, products, services and usage.
- Provide immediate consultation to PA units.
- Adhere to wireless procedures and standards, establish procedure for reviewing and approving requests for using wireless devices to store, process, or transmit information.
- Establish procedures for periodically reviewing approved wireless devices and services to ensure that the business requirement for device/service/system is still valid and meet current PA guidance.
- Establish procedures for inventory and control of wireless devices and equipment.
- Establish procedures and implementation plans for auditing wireless connections to the network.
- Provide user training.

9.1.4.13 Responsibilities of Wireless and Handheld Device Users

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

9.2 Cellular Phone & Wireless Modem

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

9.3 Technology Mobile Device Policy

9.3.1 Introduction

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

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

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

9.3.3 Software

The current version of Apple IOS software are supported.

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

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

9.3.4 Support

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

9.3.5 Training

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

9.3.6 Acquisition

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

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

9.3.7 Personal Acquisition

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

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

9.3.8 Data Security Considerations

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

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

9.3.9 Data Backup

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

Appendices

Appendix 1 -- Business Resumption Plan Document Format

I. PURPOSE

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

II. SCOPE OF PLAN

- Planning assumptions
- Facilities and resources included in plan

III. NOMENCLATURE

- Recovery terms
- Definitions and acronyms

IV. DISASTER SEVERITY DEFINITION

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

- catastrophic
- serious
- major
- limited

V. OPERATIONS RECOVERY PROCEDURES (Procedures for recovering services)

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

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

VI. OFFICE/FACILITY BUSINESS SITE RESTORATION PROCEDURES

(Procedures for restoring physical facilities)

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

VII. BRP UPDATE PROCEDURES

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

FOR REFERENCE

Appendix 2 -- Communication Rooms/Closets Standards

SPACE

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

ENVIRONMENTAL

The following conditions must be met:

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

Appendix 3 – Standard Cabling Schemes

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

FOR RFP'S

Appendix 4 -- Unified Wiring Plan

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

LATERAL CABLE:

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

Cable specifications:

(3) Cables capable of supporting Category 5e/6 capabilities as outlined in the TIA/EIA-568-B.2 standard. Specifically:

Gauge: 24 AWG Pair

Size: 4

Insulation: Plenum, fire code rating (FEP)

Cable allocations will be as following:

Cable #1: Voice**

Cable #2: Data

Cable #3: Data

- *100.0MHz is the speed the PA wants to deliver to the desktop.
- **Cable #1 is to be split in the workstation to support 2 telephones.

Technical specs for the Cat 5e/6 cable is as follows.

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

TECHNICAL DATA--PHYSICAL			
	CMR	CMP	CM (Patch)*
Conductor diameter-in. (mm)	.020 (0.52)	020 (0.52)	024 (0.61)
Cable diameter-in. (mm)	.195 (5.0)	165 (4.2)	215 (5.5)
Nominal cable weight-lb./kft. (kg/km)	21 (31)	21 (31)	23 (34.2)
Max. installation tension-lb. (N)	25 (110)	25 (110)	25 (110)
Min. bend radius-in. (mm)	1.0 (25.4)	1.0 (25.4)	1.0 (25.4)
* Patch cables utilize stranded tinned copper conductors			

PARAMETRIC MEASUREMENTS		
	Horizontal	Patch
Mutual Capacitance	4.6 nF/100 m nom.	5.6 nF/100 m nom.
DC resistance	9.38 Ohms/100 m Max.	9.09 Ohms/100 m max.
Skew	45 ns/100 m max.	45 ns/100 m max.
Velocity of Propagation	72% nom. Non Plenum	72% nom.
Input Impedance	72% nom. Plenum	
	100 + 15% 0.7772-100 MHz	100 + 15% 0.772-100MHz
	ISO/IEC 11801	

COLOR CODE			TEMPERATURE RATING	
Pair 1	White/Blue	Blue	Installation	0 degrees C to +50 degrees C
Pair 2	White/Orange	Orange	Operation	-10 degrees C to +60 degrees C
Pair 3	White/Green	Green		
Pair 4	White/Brown	Brown		

Appendix 5 -- Telephone Closet / IDF Termination Blocks

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

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

Each workstation shall be assigned a unique station identification number.

FOR REFS

Appendix 6 -- Workstation Jacks

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

FOR REFS

Appendix 7 -- Standard Switches Inside the Department

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

Cisco 3000 series – low capacity

Cisco 4000 series – medium capacity

Cisco 5000 series – medium capacity

Cisco 6000 series – high capacity

Cisco Nexus 7000 series – high capacity

Cisco Nexus 9000 series – medium and/or high capacity

FOR RFP'S

Appendix 8 -- Workstation and Lateral Cable Identification Management

WORKSTATION AND LATERAL CABLE IDENTIFICATION/MANAGEMENT (Facility)

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

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

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

FOR REFS

Appendix 9 – Fiber Optic Specification for Network Services - PAWANET

General Scope of Work

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

Fiber Optic Terminations

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

Fiber Optic Testing

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

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

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

Appendix 10 -- Public Telephone Ordering Standards

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

General Standards

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

Process

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

FOR REFERENCE

ATTACHMENT E

CONTRACT SPECIFIC TERMS AND CONDITIONS

TABLE OF CONTENTS

1. General Agreement	2
2. Order of Precedence.....	2
3. Specific Definitions	2
4. Delivery Requirements	3
5. Delivery Schedule.....	4
6. Progress Schedule	4
7. Time is of the Essence	5
8. Bill of Sale	5
9. Title to Materials.....	5
10. Invoices	6
11. Payment.....	6
12. Equipment Warranty.....	7
13. Insurance Procured by the Contractor.....	8
14. Materials and Workmanship	10
15. Inspection and Acceptance	10
16. Errors and Omissions	11
17. Approval by the Project Manager	11
18. Changes.....	11
19. Variations in Quantity	11